Department of Information Engineering and Computer Science

Master degree in Computer Science - Cyber Security

FINAL REPORT

IoT MALWARE: MIRAI

Group 4

Luigi Dell'Eva, Riccardo Germenia, Ion Andy Ditu

Academic year 2023/2024

Contents

1 Introduction

1.1 DDoS

1.2 Botnet

A botnet is a network of internet-connected devices, such as computers, smartphones or IoT devices, whose security has been compromised and control has been taken over by a third party. Botnets were initially designed for legitimate purposes, such as automating repetitive tasks or managing chatrooms. However, their ability to execute code within other computers led to their misuse for malicious activities, such as stealing passwords, tracking user keystrokes, and launching attacks against unsuspecting devices. [2] They are one of the most common types of **network-based attacks** today due to their use of large, coordinated groups of hosts. These groups are created by infecting vulnerable hosts, turning them into "*zombies*" or **bots**, which can then be controlled remotely. When a collection of bots is managed by a **Command and Control** (CNC) infrastructure, it forms a botnet. Botnets help in obscuring the identity of the attacking host by providing a layer of indirection, separating the attacking host from its victim through zombie hosts, and separating the attack itself from the botnet assembly by an arbitrary amount of time. [4] The method of controlling bots varies based on the architecture of the botnet's command and control mechanisms, which can be **Internet Relay Chat** (IRC), **HTTP**, **DNS**, or **P2P-based**.

1.3 Mirai

Mirai is a malware that targets **IoT devices**, such as routers, cameras and others, by exploiting their default credentials. Once a device is compromised by Mirai, it becomes part of a botnet that can be used to launch **DDoS attacks**, however, this do not compromise the device's functionality except for occasional increased bandwidth usage. It is capable of running on various CPU architectures, including MIPS, ARM, and PPC. It uses a dictionary attack with a set of 62 entries to gain control of vulnerable devices. The infected devices are reported to a control server to become part of a large-scale Agent-Handler botnet. [1]

The botnet was first created by a guy named Paras Jha, who used it to launch multiple DDoS attacks against Minecraft servers. This was to extort money from the server owners, who would pay him to gain "protection" from the attacks. Then it was also used to attack Rutgers University, where he was a student. After these events, he joined forces with other two individuals, Josiah White and Dalton Norman, to further develop the malware, which later became known as Mirai. The malware was first discovered by MalwareMustDie, a non-profit security research group, in August 2016. In the late september of the same year, it gained public attention after being used in a DDoS attack against the Krebs On Security website, reaching 620 Gbps. Following this, it was employed in an attack on the French hosting company OVH, which peaked at 1 Tbps. After these attacks, Anna-senpai, which seems to be the online nickname of Paras Jha, released the source code of Mirai on HackForums[1]. This led to the proliferation of Mirai-based botnets and some time later caused the Dyn DDoS attack, which took down several high-profile websites, such as GitHub, Twitter, Reddit, and Netflix. Dyn estimated that up to 100,000 malicious endpoints were involved in the attack. [3]

1.3.1 Mirai architecture

The architecture of Mirai is illustraded in Figure 1.1 and is based on a **centrlized** model. The botnet is composed of four main components:

- **CNC server**: the central component of the botnet, it is used by the admin / users to control the bots and to send commands to them.

[1] Original post: `https://hackforums.net/showthread.php?tid=5420472`

- **Bots**: the infected devices that are part of the botnet and are used to launch DDoS attacks. Other than waiting for commands to perform attacks, each bot performs some tasks:
  - **Scanner**: perform active scanning of the internet for vulnerable devices, once found it reports them to the report server. When a device is found it tries to remotely access by using a dictionary based attack with a set of 62 entries. If the attack is successful, the bot will send the vilnerability to the reporting server.
  - **Killer**: tries to kill other malware running on the device.
  - **Masking**: once the malware is running, it deletes itself from the device to go unnoticed.
- **Reporting server**: its role is to receive the vulnerablity (IP, port and potential username and password) found by the bots and forward them to the loader.
- **Loader server**: it is in charge of loading the malware on the reported devices.

To summarize, Mirai uses a spreading model named "Real Time Loading", which is based on the following steps: Bots → Reporting server → Loader server → Bots. [1] More information on how the components works with some code snippets can be found in Chapter 2.

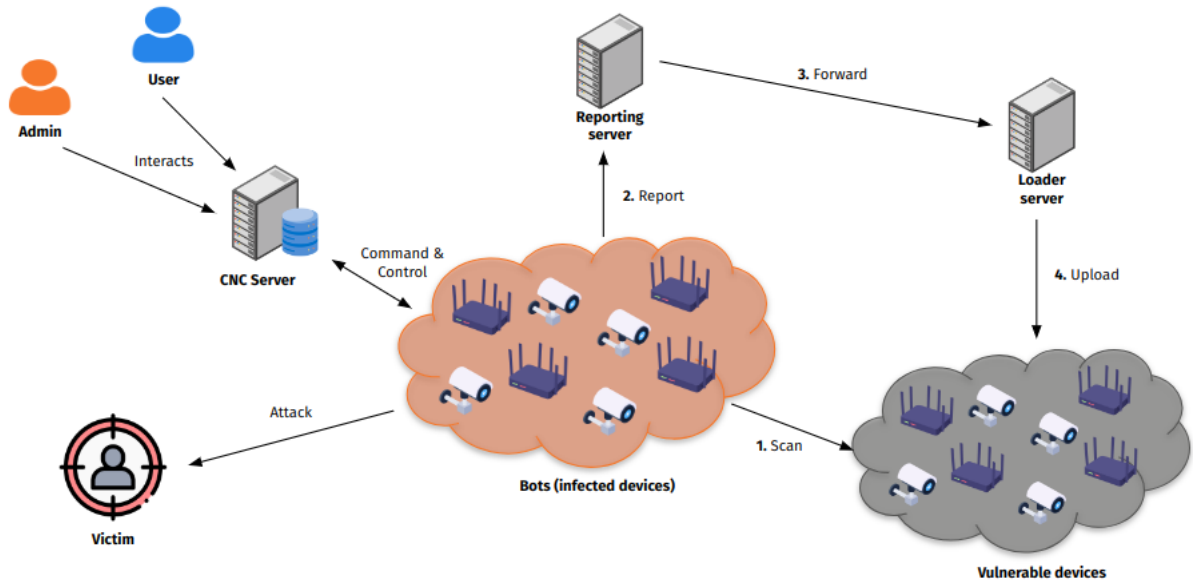

Figure 1.1: Mirai architecture

2 Mirai static analysis

3 Traffic analysis

4 IoT Malware Laboratory

5 Other malware

5.1 Hajime

5.2 Goldoon

5.3 BotenaGo

5.4 Malware comparison

6 Conclusion

Bibliography

[1] Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi. Ddos-capable iot malwares: Comparative analysis and mirai investigation. *Security and Communication Networks*, 2018:1–30, 2018.

[2] Fortinet. Botnet. `https://www.fortinet.com/resources/cyberglossary/what-is-botnet`. Accessed: 2024-05-27.

[3] Hamdija Sinanović and Sasa Mrdovic. Analysis of mirai malicious software. In *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–5, 2017.

[4] W Timothy Strayer, David Lapsely, Robert Walsh, and Carl Livadas. Botnet detection based on network behavior. *Botnet Detection: Countering the Largest Security Threat*, pages 1–24, 2008.