Mirai Botnet: Exposing the Cyber Insecurity of IoT Devices

Kinda AL CHAHID
University of Bordeaux
Master's Degree in Computer Science - Communicating autonomous mobile systems - 2017/2018
Imen HENTATI
University of Bordeaux
Master's Degree in Computer Science - Software Engineering - 2017/2018

Index Terms—Mirai, Botnet, Malware, Security, DDos, IoT, Telnet, TCP, IP, DNS . . .

1 Introduction

With the emergence of IoT[1] devices, a big dilemma took place for manufacturers between speed and security. In 2020, it is predicted that 26 billion objects will be connected [6] and with it, many potential threats.
Mirai is one of the most dangerous attacks that was able to control thousands of botnets[2] to perform a Distributed Denial of service [3] attack[4].

In this article, we summarize the USENIX article [1] about Mirai botnet. We explain the different stages of Mirai's attack and the reasons of its efficiency. We discuss the ways we can improve Internet security based on how Mirai botnet exploited the (fragile) IoT ecosystem with massive DDoS attacks. Finally, we talk about the impact of Mirai and the related work of the article.

2 Context

Mirai isn't the first attack targeting IoT devices weakness. The **Carna botnet** [12] appeared earlier in 2013, infecting approximately 420,000 devices especially routers. As Mirai processes, Carna uses default passwords from a static dictionary to check the device's credentials. If they aren't in the dictionary, it leaves it behind which makes the attack more efficient and fast-processing. It was originally used to map the internet access for over 24h.

BASHLITE [13], on the other hand, was the first to launch *distributed denial-of-service* attacks. It was famous for its infections with bruteforce algorithms to detect vulnerable IP[5] addresses, then go through a dictionary of common username/password combination and relying on TCP[6] connections.

Mirai works a little differently, using a random generation of IP addresses based on a range of IP excluding the US Postal Service, the Department of Defense, the Internet Assigned Numbers Authority (IANA) and IP ranges belonging to Hewlett-Packard and General Electric.

3 Contribution

Mirai is a malware[7] that compromises Linux devices, turning them into remotely-controlled "zombies" that can be used as part of a distributed DDoS attack.

It first appeared in September 2016 when it launched its first attack disabling Krebs on Security with a big mass of distributed DDos attacks. Mirai primarily targets Internet of Things (IoT) devices such as printers, DVRs[8] and CCTV cameras[9]. The Mirai botnet has been used in some of the largest known DDoS attacks. This includes the huge take down of Dyn DNS services[10] causing the unavailability of so many websites to millions of users in Europe and North America.
In this section, we will go through the major facts about Mirai according to the Usenix article [1].

1. "Internet of things" - small objects connected to the internet (e.g., printers, smart home gadget...)
2. A "botnet" is a Iot device that runs a program used by a hacker.
3. "Denial of service" - DoS - occurs when a service (website, server, etc...), has too much information to analyze. To protect itself, it cuts off all its services, causing its unavailability. It's very difficult to avoid this attack since it's hard to say if it's an attack or normal massive connections.
4. "Distributed denial-of-service" - DDoS - is an attack performed by different devices connecting to the target website preventing server resources from being able to handle any requests of malicious or benign intent. The owners of these botnets aren't aware of the infection having place.
5. Internet protocol - a unique address for eath device
6. "Transmission Control Protocol" - communication protocol used to connect a device to internet
7. "Malware" - short for malicious software, an unwanted software used by hacker
8. "Digital Video Recorder
9. Closed-circuit Television Camera - used as private surveillance camera
10. "Domain Name System" - used to convert IP addresses into named services like "www.google.fr" and conversely

3.1 Mirai operation

In the section, we will look further on how Mirai works [4] to infect devices and turn them into so-called *zombies*.

There are four entities that take part of the operation:

- The Victim : An internet service targeted for a DDos attack.
- A C2 Domain : Each botnet has a C&C[11] server which is a computer that communicate with the botnet by the IRC[12] protocol, configured to connect to with the indication of their victim [8].
- The hacker.
- The first Botnet: an IoT device that became a botnet controlled by a C2 Domain.
- The botnets "army" or cluster: an agglomeration of botnet controlled by the same C2 Domain.

In the operation, we find two big modules: *replication* and *attack* that we will go through in figures 1 and 3 respectively.

Replication module

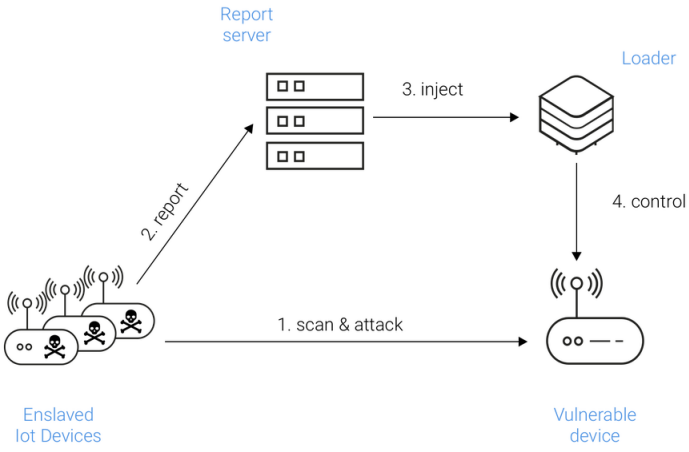

Fig. 1. Replication module: Mirai bots scan the IPv4 address space for devices that run on Telnet[15] or SSH[16], and attempt to log in using a hardcoded dictionary of IoT credentials. Once successful, the bot sends the victim IP address and associated credentials to a report server, which asynchronously triggers a loader to infect the device. [4]

The attack begins with a scan of a selected range of IP addresses with telnet TCP port (1). In a normal behaviour like shown in figure 2, a computer is secured thanks to a local network protected by a private IP. Once it's connected to the internet, the residential gateway changes this IP to a public IP. For an attacker, it's hard to see the local network from outside the residential gateway. However, this is not applicable for IoT devices because these devices constantly need to be reachable and manageable, in other words throught a public IP exposed to attackers.

For the targeted IP address, the algorithm will try a combination of ten login/passwords out of 64 registered in a dictionary then make a report of which one worked on a distant server (2).

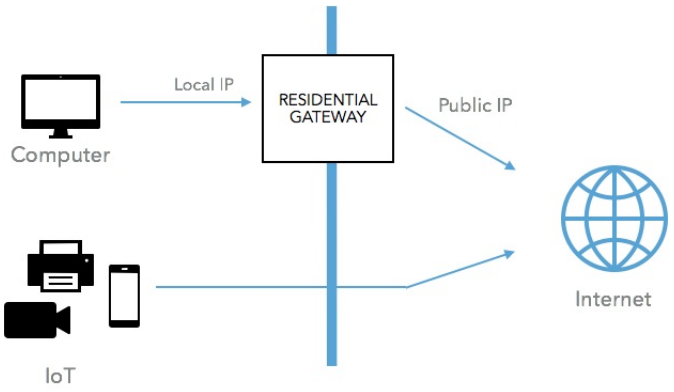

Fig. 2. Once a device connects to internet, the residential gateway transform it's local IP to public IP and opposite called Network Translated Addresses or NAT. However, an Iot needs a constant connection online, whitch means a public IP visible online

Once in control of the device, the material architecture (MIPS 32-bit, ARM 32-bit, and x86 32-bit) is detected (3) and Mirai starts downloading the malware according to the architecture. The device is now infected and therefore becomes a botnet. Once becoming a "zombie" it infect all device inside the local network if the device inside it has a telnet port for example.

Attack module

The newly made 'zombie' works on detecting and infecting the rest of the IoT devices connected to the same network.

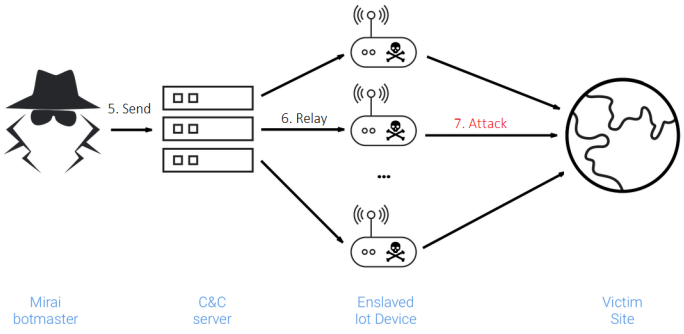

Fig. 3. Attack module: Infected hosts scan for additional victims and accept DDoS commands from a command and control (C2) server. [4]

If the attacker sends an order (5) on a "Command and control" (C2 Domain), the C2 will propagate the order to its related botnet (6). In figure 4, we show some possible orders a botnet might receive.

11. Command and Control
12. Internet Relay Chat

```
#define ATK_VEC_UDP        0  /* Straight up UDP flood */
#define ATK_VEC_VSE        1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS        2  /* DNS water torture */
#define ATK_VEC_SYN        3  /* SYN flood with options */
#define ATK_VEC_ACK        4  /* ACK flood */
#define ATK_VEC_STOMP      5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP      6  /* GRE IP flood */
#define ATK_VEC_GREETH     7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY      8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN  9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP       10 /* HTTP layer 7 flood */
```

Fig. 4. Sample of orders that the C2 Domain sends to a botnet [9]

The order is composed of selected IP that the device has to connect to (7) which can cause a DDoS of 1To/s (equivalent to a download of a movie in hight definition per seconde). The biggest threat of Mirai is that, even though a botnet has a limited bandwidth (because of the region/location of the device or its limited capacity), it's the number of IoT infections that causes such damage.

3.2 Methodology

To detect and understand Mirai's pattern, the authors used different techniques to analyze the network and look through the infected areas. The most important methods are cited down below.

- IP scanning: using tools like Censys [10] that scans all IPv4 devices accessible online.
- Honeypots: an online device disconnected from local network but accessible online. Used to understand how the attack is performed.
- Active and Passive DNS: unlike active DNS, passive DNS records every attempt and archives it for further analysis. [14]
- analyze DDoS attack traces with the results of every DDoS that targeted Krebs Security between 2012 and 2016 [1].

3.3 The Victims

From figure 5, each victim was targeted from one cluster. Here, we will talk about a sample of victims of Mirai.

The first Mirai victim was *Krebs on Security* inside the cluster 1.
Another cluster attacked six IP addresses [2], four were linked to *Dyn*, a DNS Server. The other two were *Sony Playstation*'s server. The author explained how those four IP were also linked to Playstation server after looking further into the Dyn response. However, Dyn was a collateral victim, in fact it couldn't stand the amount of data sent by Mirai and had also a DDos (very likely unintendedly). As a result, many websites hosted by Dyn including Twitter, Netflix, CNN and many others in Europe and the US were brought down by the malware.

This attack combined with others on Valve server and Xbox server were part of cluster 6.

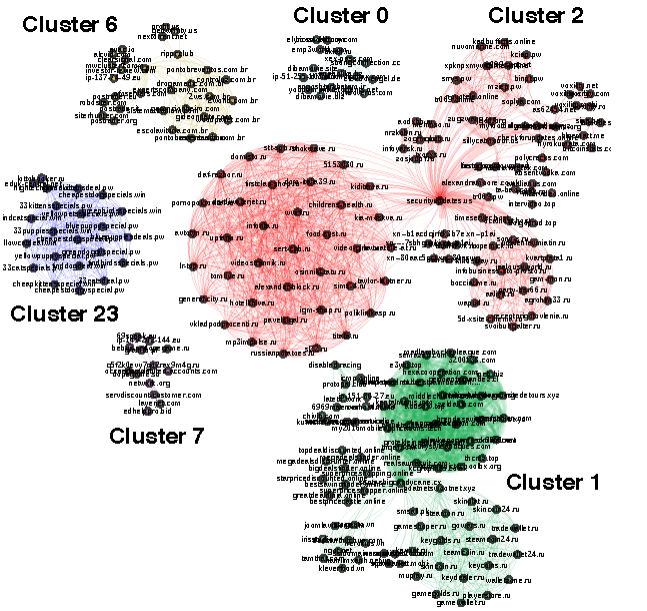

Fig. 5. C2 Domain visualisation : Each cluster contains a certain amount of botnet. Each one has it's own target. [1]

4 Discussion

Mirai code leaked

On september 30, 2017 Mirai code was revealed [5] to the world through a hackers forum by Anna-sempai, Mirai's known author. Whith the code, many people started testing the code and building botnets for their own motives. It made identifying the original attacks significantly harder.

Reaper Botnet

A new IoT malware emerged based on Mirai since its appearance in 2016: Reaper Botnet [11]. The major difference between both malwares is that Reaper does not aim credentials as Mirai does, but targets security vulnerabilities in IoT devices.
Reaper might not be the last malware targeting IoT, as long as security measures have not been taken.

IPv6, the new standard for IP

Since the emergence of connected devices, the number of available IP[17] decreased significantly. To prevent absence of new addresses, the NAT [18] technique was invented to remap addresses into others. This added another layer of protection to the local network.
Another type of IP was created: IPv6 which brought almost unlimited addresses. However, IPv6 does not use NAT, which means that the additional layer of protection is not present, making the local network unprotected and exposed to hackers. IPv6 should be the next standard of IP [7].

17. The original form of IP is called IPv4.
18. "Network Addresses Translation" - cf figure 2

Recommendations

The "Internet of things" must simply become "the Internet" [3]. We deem that the manufacturers of IoT devices must acknowledge the vulnerabilities in their systems to raise the security level of their devices. It is nowadays preferable to create new protocols based on cryptography and reinforced security based mostly on the possibility of changing passwords of the device which is not possible on every connected object.

Another good way to prevent such attacks based on simple algorithms is to inform buyers that their smart watches, cameras and even their connected toothbrushes are not secure. One way to avoid malware infections is by teaching simple security measures like changing default passwords (which would significantly reduce the impact of Mirai-like malwares).

5 Related Work

In a recent research of the BGP[19] [15], analysis of blackholing usage show that Mirai is responsible for an increase of the level of blackholing activity that lasted for months. There are additionally two spikes correlating with the "Krebs on Security" and "Liberias Internet infrastructure" attacks which are clearly victims of Mirai.

The USENIX article inspired many others to discuss cyber security inside the IoT world.
One presents an End-to-End view of IoT security and privacy [16] with protocol solutions against attacks like Mirai. It points out new IoT weaknesses through a vulnerability analysis of the Edimax IP camera system.

Another one [17], which is the most recent article inspired by malwares like Mirai, raises the alarms againt manufacturers of IoT. It points out the fragility of IoT devices and explains how Mirai is only a harbinger of more widespread and crippling attacks in the future, which leads us to the next section.

5.1 Articles in the future

We expect more articles to see the light about cyber insecurity, refering to Mirai as the biggest and most dangerous attack and yet that could have been avoided with simple precautions. We might also hear about new malwares following the path of Mirai and potentially finding new breaches in the security systems.

6 Conclusion

This article points out the lack of security of the IoT system through an evaluation of the Mirai botnet.

And yet, ways exist to decrease the number of such attacks and perhaps eradicate them.

If people learned simple ways to protect themselves, the situation would drastically change, closing the door for any hack attempts based on default configuration.
We live in a era that evolves constantly, every minute of every day. Considering the fact that very basic objects are now connected to the internet like simple toothbrushes, people should reconsider the usefulness of such "smart" objects given the threats they are exposing themselves to.

19. Border Gateway Protocol

References

[1] Manos Antonakakis and Tim April and Michael Bailey and Matt Bernhard and Elie Bursztein and Jaime Cochran and Zakir Durumeric and J. Alex Halderman and Luca Invernizzi and Michalis Kallitsis and Deepak Kumar and Chaz Lever and Zane Ma and Joshua Mason and Damian Menscher and Chad Seaman and Nick Sullivan and Kurt Thomas and Yi Zhou, *Understanding the Mirai Botnet, USENIX Security Symposium*, 2017

[2] USENIX Security 17 - Understanding the Mirai Botnet- Conference: *https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis*

[3] Alan Paller, Ed Skoudis, Michael Assante, Johannes Ullrich, RSA Conference: The seven most dangerous new attack techniques and what's coming next. *https://www.rsaconference.com/events/us17/agenda/sessions/7582-the-seven-most-dangerous-new-attack-techniques-and, 2017*

[4] Elie Bursztein, *Inside Mirai the infamous IoT Botnet: A Retrospective Analysis*, dec 2017

[5] US-CERT. 2016. Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets. "https://goo.gl/SYA8JW", nov 2016.

[6] Gitta Rohling: Facts and Forecasts: Billions of Things, Trillions of Dollars *https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/internet-of-things-facts-and-forecasts.html*

[7] Google *http://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption*

[8] Sentryo: Le botnet IoT Mirai : une menace cl en main rendue publique *https://www.sentryo.net/fr/botnet-iot-mirai-menace-cle-en-main-rendue-publique/*

[9] Anna Senpai: Code source of Mirai *https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/attack.h*

[10] Censys : *https://censys.io/*

[11] Andy Greenberg: The Reaper IoT Botnet Has Already Infected a Million Networks *https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/*

[12] Christian Stcker and Judith Horchert: Mapping the Internet A Hacker's Secret Internet Census *http://www.spiegel.de/international/world/hacker-measures-the-internet-illegally-with-carna-botnet-a-890413.html*

[13] Tom Spring: BASHLITE Family Of Malware Infects 1 Million IoT Devices *https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/*

[14] Benjamin Roussey: What is Passive DNS? *http://techgenix.com/what-passive-dns/*

[15] Vasileios Giotsas and Georgios Smaragdakis and Christoph Dietzel and Philipp Richter and Anja Feldmann and Arthur Berger, *Inferring BGP Blackholing Activity in the Internet*, 2017

[16] Zhen Ling and Kaizheng Liu and Yiling Xu and Yier Jin and Xinwen Fu, *An End-to-End View of IoT Security and Privacy*, 2017

[17] Theophilus Benson, Balakrishnan Chandrasekaran, Sounding the Bell for Improving Internet (of Things) Security, 2017