Mirai Botnet Awareness

Rishabh Balse

May 2021

1 Introduction

Mirai is a worm-like family of malware that infects IoT devices. It has affected hundreds of thousands of IoT devices since it first emerged in 2016. Mirai scans the devices that run on the ARC processor which runs over the Linux operating system. If the default username and password combo are never changed, Mirai can simply log into the device and infect it. Mirai is mutating, which means it keeps on giving birth to different variants. Botnets are dangerous as they have the potential to impact virtually every person whether or not they use IoT devices or even the Internet. To curb this spread you will have to do your part.

2 How Did We Get Here?

Attackers are trying to rile up as many machines as possible, to generate the largest attack possible

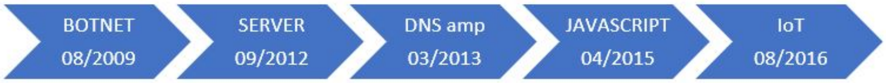


Figure 1: Botnet Trends

- In 2009 on the anniversary of Russo-Georgian War, a botnet was used to target all the social media accounts of a Georgian activist. This attack took down Twitter and made Facebook slow. This attack was also focused on Google and generated 600,000 queries per second. This was done by compromising home machines.
- In 2012, attackers realized its more impactful to compromise servers instead of home machines and created BroBot to attack the many different banks in the US. This attack was around 125 Gbps.

- In 2013, somebody realized it was not necessary to even compromise machines, all they must do is to get machines to send them the much-needed Bandwidth which could be used for DDOS. This helped generate the Spamhaus Attack which measured at a whooping 300 Gbps.
- Users inside or outside China trying to use Chinese websites fell victim to the China's Great Firewall which tracked the users and ran JavaScript on their machines to make them a part of their Botnet attacks. In 2015, they carried out one such attack on Github.
- In this present day, there are tonnes of IoT devices that have default root passwords and very weak security. What Mirai Botnet does is exploit these weakly secured devices, make them a part of their large attacking army and create a huge inconvenience by using their bandwidth to perform a massive scale DDoS attacks on their victims.

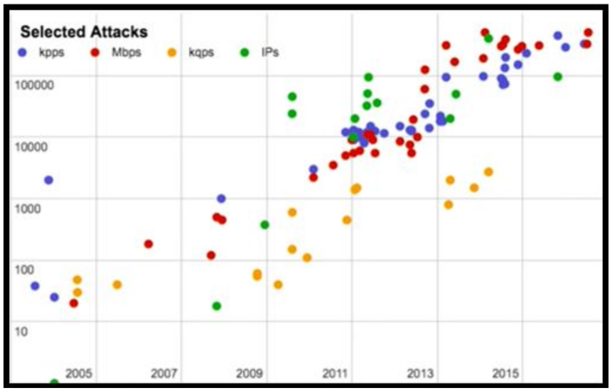


Figure 2: Attack Intensity Over Time

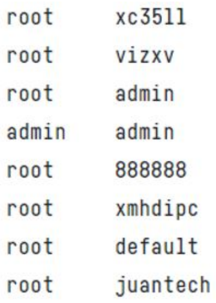
3 Source Code Analysis

Analysing the source code helps us understand the mindsets of the hackers behind the code.
Mirai is built for two core purposes:

- Locate and compromise IoT devices to further grow the botnet.
- Launch DDoS attacks based on instructions received from a remote command and control server.

3.1 IP Scanning and Password Cracking

To fulfil its recruitment function, Mirai performs wide-ranging scans of IP addresses. The purpose of these scans is to locate under-secured IoT devices that could be remotely accessed via easily guessable login credentials—usually factory default usernames and passwords (e.g., admin/admin). Mirai uses a brute force technique for guessing passwords a.k.a. dictionary attacks.



```
root     xc3511
root     vizxv
root     admin
admin    admin
root     888888
root     xmhdipc
root     default
root     juantech
```

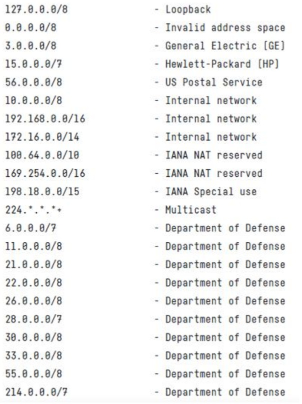
Figure 3: Portion of Attacker's Guess List

3.2 GRE IP/ETH Flood

Mirai uses a kind of special attack that floods their victim's GRE (Generic Routing Encapsulation) Tunnel protocol.

3.3 "Don't Mess With" List

One of the most interesting things revealed by the code was a hard-coded list of IPs Mirai bots are programmed to avoid when performing their IP scans. This list, which you can find below, includes the US Postal Service, the Department of Defence, the Internet Assigned Numbers Authority (IANA) and IP ranges belonging to Hewlett-Packard and General Electric.

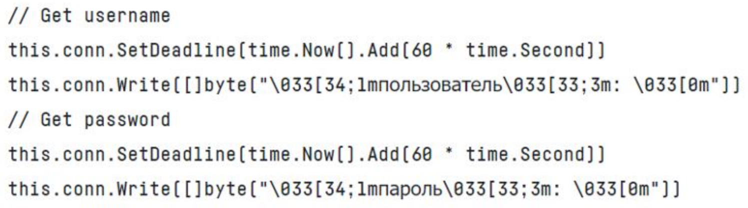


```
127.0.0.0/8              - Loopback
0.0.0.0/8                - Invalid address space
3.0.0.0/8                - General Electric [GE]
15.0.0.0/7               - Hewlett-Packard [HP]
56.0.0.0/8               - US Postal Service
10.0.0.0/8               - Internal network
192.168.0.0/16           - Internal network
172.16.0.0/14            - Internal network
100.64.0.0/10            - IANA NAT reserved
169.254.0.0/16           - IANA NAT reserved
198.18.0.0/15            - IANA Special use
224.*.*.*+               - Multicast
6.0.0.0/7                - Department of Defense
11.0.0.0/8               - Department of Defense
21.0.0.0/8               - Department of Defense
22.0.0.0/8               - Department of Defense
26.0.0.0/8               - Department of Defense
28.0.0.0/7               - Department of Defense
30.0.0.0/8               - Department of Defense
33.0.0.0/8               - Department of Defense
55.0.0.0/8               - Department of Defense
214.0.0.0/7              - Department of Defense
```

Figure 4: Mirai's Don't Mess-With list

3.4 Origin Speculation

Lastly, it's worth noting that Mirai's code holds traces of Russian-language strings despite its English C&C interface. Here, for instance, Russian is used to describe the "username" and "password" login fields:



```
// Get username
this.conn.SetDeadline(time.Now().Add(60 * time.Second))
this.conn.Write([]byte("\033[34;1mпользователь\033[33;3m: \033[0m"))
// Get password
this.conn.SetDeadline(time.Now().Add(60 * time.Second))
this.conn.Write([]byte("\033[34;1mпароль\033[33;3m: \033[0m"))
```

Figure 5: Traces of Russian Text

This opens the door for speculation about the code's origin, serving as a clue that Mirai was developed by Russian hackers or—at least—a group of hackers, some of whom were of Russian origin.

4 Why Should i Care?

You might probably be wondering, why should I even care? For my devices are safe and attacker doesn't want to use Mirai to personally harm me. Well, you are correct, to an extent. But as human beings and social creatures, our focus must shift from a personalized perspective to a collective well-being.

Try to imagining in a few years and with an advent of 5G technology, doctors might be performing a surgery using robotic tools from one part of the country to the other, and suddenly the instruments are hampered by thousands and millions of Botnets. If suppose you come to know, that one of your devices have been part of this disruptive wave, won't you feel tiny bit guilty?

You yourself won't become a victim of a DDOS. For all it may concern, the attackers care about you, in a different way. These attackers don't want to attack you head on but want to use you to attack someone else. But you can't depend on any government to stop attacks coming from your homes, you can. So, its best we don't hide behind ignorance, bad guys prey on ignorant people.

ASK YOURSELVES THESE QUESTIONS BEFORE BUYING A 'SMART' DEVICE:

- If I can access that IOT device from my smart phone, what is stopping someone else from doing the same?
- What's the process for updates if somebody finds a security vulnerability in my device?

- What is the native language of your support staff? Last thing you need is a language barrier during crisis.

Only spend your money when you get solid answers to these questions.

5 Possible Solutions Against Mirai

- Stop using default/generic passwords for your smart devices.
- Put all your smart devices behind a credible firewall.
    - You should be aware of the log traffic in and out.
    - It should show you data rates in and out.
    - It should have diagnostic tools you can use for troubleshooting.
- Upgrade your knowledge. Attend seminars, read latest news articles and expand your domain knowledge. You should be aware what kind of attack is prevalent today. One prominent website to get all the current happenings around and about the hacking world is Krebs on Security. (https://krebsonsecurity.com)

6 Conclusion

The next-gen botnet malware, the 'Mirai Attack', is already here. It has the power to take control of your Smart devices, generate a large scale botnet army and use their bandwidth for a massive DDoS attack. Secure your IOT devices. Don't be ignorant. Take responsibility, make amends and share your knowledge with others.
'Care and Share to be Prepared'.