A Case study on Mirai botnets:

Dyn, OVH, KrebsOnSecurity and other organizations cyberattacks in 2016

Namruth Reddy Suryanarayana Reddy

CY5010 – Foundations of Information Assurance

03-Dec-2021

Introduction

In 2016, Dyn - one of the largest DNS service providers in USA was attacked with series of DDOS attacks[1] bringing down their servers and thereby causing major disruptions to hundreds of companies' services including the big ones such as - Twitter, Amazon, HBO and many smaller companies. This case study is about, why and how this attack was performed - technically and conceptually, what were the learnings from the attack to the cybersecurity industry and finally in retrospect - what could have been done better to prevent the attack in the first place.

Brief description of the attack

A brief description of the attack including – motivation, how it was detected, and methods used for exploitation are described in this section

The source and motivation of the attack.

Even though the Mirai botnet gained popularity for the Dyn 2016 attack, its origin was not for this attack. Before Mirai was used for DDOS on Dyn, it was developed by an undergraduate student named Paras Jha. He developed the original botnet to attack college servers during registrations and exams. It was also used to attack other Minecraft game server hosting competitors, as he was making good money hosting game servers on his own. After using the botnet on multiple occasions, Paras posted the source code online in the dark web. It was later taken by an unknown hacker group, made slightly better and used for DDOS attacks on multiple companies like - OVH, Krebs on Security, Dyn etc.

Mirai was initially not intended to take down the internet services but rather companies

---

[1] https://en.wikipedia.org/wiki/DDoS_attack_on_Dyn

like OVH, Dyn hosted specific game servers which were the actual reason for the attack. It's hard to imagine when collateral damage of an attack can causes such a huge impact. There are multiple variants of Mirai that was adapted by many hacker groups and used for various small- and large-scale attacks throughout the world.

If an undergraduate student can develop a botnet that eventually caused a major internet service disruption in US, we know how vulnerable the systems can be now of advanced threats.

How was the breach detected?

Dyn was not the first company to be affected by the Mirai botnet. Mirai was found on the internet as early as Jan 2016. But major attacks only came into picture when a surprising large scale DDOS attack on one of the largest hosting providers in the Europe -OVH. The company later confirmed that attackers were targeting their Minecraft servers. According to the telemetry logs of OVH - it was observed that there were requests as high as 1 Tbps and it was carried out using 145,000 IoT devices. Even though the exact size was not clear - this was way bigger than any other DDoS attacks in the past.

Soon after this, Brian Krebs who is an independent journalist who specializes in cybercrime was attacked using the similar botnets. He owns the website - KrebsonSecurity.com[2] which revealed that there were requests like SYN/SYNACK,GRE,HTTP as high as 650 Gbps on his servers causing major disruptions to any services from the website.

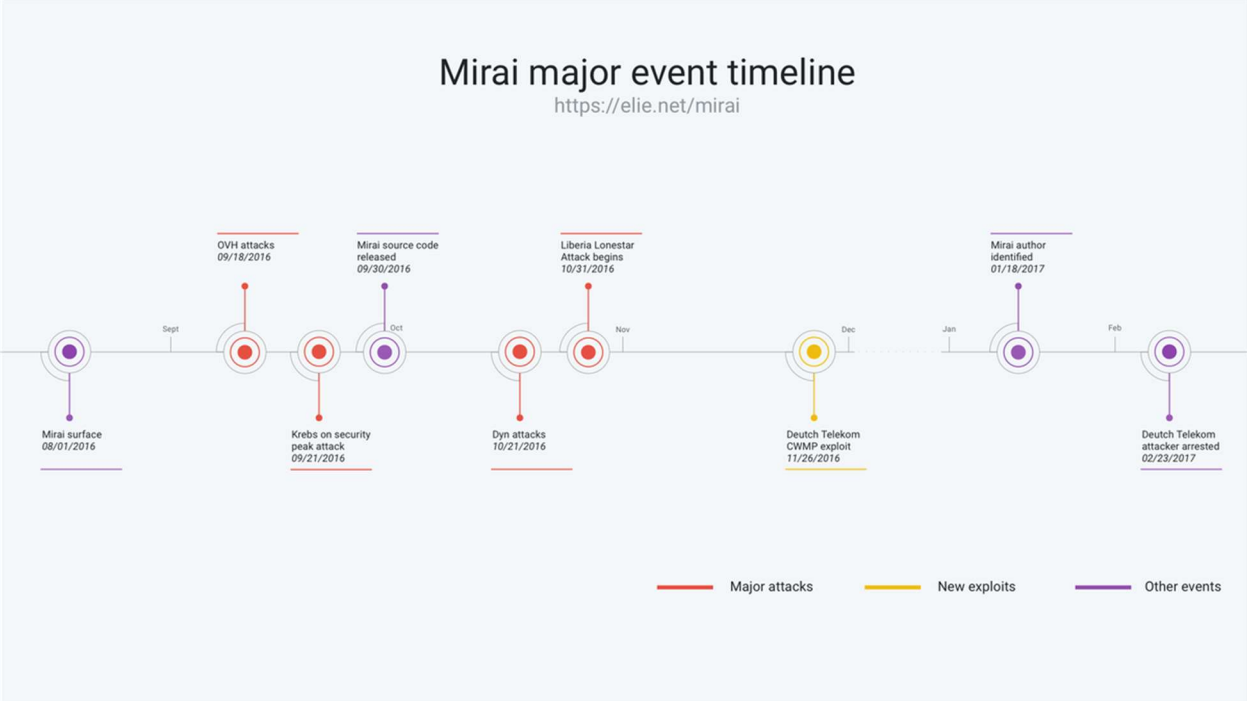
After approximately a month later - Dyn (one of the largest DNS service providers) was attacked using the same botnets. Technical details of attack on Dyn were not publicly released or they are no more available, but the scale of attack can be estimated from the details released by

---

[2] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

OVH and KrebsOnSecurity. Attack on Dyn made headlines all around the world because Dyn was the DNS provider for most of the top companies in the US as described in the introduction.

Surprisingly there were even other attacks carried out by Mirai after the Dyn attack as well. Attacks on Liberia's largest telecom operator, Deutsche Telekom - a major internet provided were also affected by Mirai. Throughout 2016, Mirai made headlines all around the world.



Cloudflare blog[3] has a great retrospective analysis of the attacks along with the timeline of various incidents. The image shown is from the same Cloudflare blog showing the various attacks that happened because of Mirai botnets. Dyn was a part of multiple other attacks that happened in 2016 because of Mirai.

---

[3] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

Amount of time between initial exploit and detection, and methods used for exploitation.

Exploit and detection were simultaneous because this was a DDOS attack and knocked the Dyn DNS servers offline. The original Mirai that was designed had 4 steps to create botnets[4]:

1. IP scanning on the internet for vulnerable IoT devices
2. Brute force the telnet login using a list of credentials
3. Cracked devices will be added as part of the botnet and they will scan for devices in their network
4. Each compromised machine will be controlled by C&C server which will instruct the bots when to attack a target

Mapping the incident's attack tactics and techniques to the MITRE ATT&CK Framework

MITRE's ATT&CK[5] framework is a concept developed by MITRE corporation to divide an entire attack into various phases so that its easier for organizations to handle cyberattacks. There are two core components in the framework: Tactics – goal of the attacker and Techniques – methods used by attackers to achieve the goal.

Mirai attack was made possible by compromising thousands of IoT devices across the internet. Mapping the tactics and techniques followed by the attacker is shown in the link below with all the techniques used by the attacker are marked in bright orange across the entire sheet.

Mirai Botnet ATT&CK mapping

[4] https://www.coursera.org/lecture/ddos-attacks-and-defense/mirai-source-code-analysis-KwxYQ

[5] https://attack.mitre.org/

Response, recovery actions and impact

It is extremely important to have an incident response plan for any organization. It is impossible to detect and mitigate all the cyberattacks in the world, therefore its only right to have a thorough plan assuming the worst case possible[6].

Response and recovery actions taken by Dyn

Dyn was able to restore the services in a couple of hours after the attack. They were attacked multiple times even after restoring the services. Dyn also released a statement saying they can't detail all the post attack recovery procedures to prevent any other attackers gaining advantage of knowing the system for future attacks.

Notifications to impacted users and authorities.

As this attack brought down some of the major websites in the US including Amazon, Quora, Airbnb and many more, Dyn released a statement about it and fixed the issue in a few hours to restore all the services.

Assessment of the breach's impact on regulations and industry, related breaches.

This attack showed the world about the weakness of IoT devices security. IoT devices security was not in the forefront because cybersecurity industry didn't expect IoT devices to cause attacks of this magnitude. This attack showed the world why IoT devices are highly insecure, and more regulations are necessary before they deployed in real-world scenarios. It was one of the key examples of how IoT devices can cause major havoc for security if they are not protected well.

What would you have done differently if you were handling post breach procedures?

As the post breach procedures were not released to the world, it's hard to say what can be changed and done better.

---

[6] https://www.cfo.com/cyber-security-technology/2017/02/lessons-learned-dyn-attack/

But having said that – Dyn still had a great incident response plan to quickly recover from the attack and restore all the services in a matter of hours.

Considering the scale of the attack and threat vector that was not seen before, they handled the incident very well and haven't seen such outages in the last 5 years after the attack.

Concluding Remarks

Mirai botnet and the cyberattacks because of it had two main implications in my opinion:

1. IoT devices security is not something that is not important anymore. It must be taken very seriously, and new regulations and security measures needs to be in place for all of them and the number of IoT devices is only going to increase in the next few years which will only make their security harder.

2. If a high school student can cause an attack of this scale, it shows us that security is still an evolving field, especially security of IoT devices and mitigation of DDOS attacks. There are a lot of attack vectors that we don't know yet and cybersecurity will always remain a process that needs to be updated regularly as new attacks emerge.

Bibliography

Antonakakis, Manos. April, Tim. Bailey, Michael. *Understanding the Mirai Botnet*. Published in 26th USENIX Security Symposium, Vancouver, BC, Canada. August 16–18, 2017

DDOS attack on Dyn - https://en.wikipedia.org/wiki/DDoS_attack_on_Dyn

Krebs On Security article on Mirai - https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Cloudflare retrospective analysis of Mirai -https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

DDOS attacks and defenses – Mirai source code analysis https://www.coursera.org/lecture/ddos-attacks-and-defense/mirai-source-code-analysis-KwxYQ

MITRE ATT&CK framework - https://attack.mitre.org/

Lesson learned from Dyn cyberattack - https://www.cfo.com/cyber-security-technology/2017/02/lessons-learned-dyn-attack/