Name: Ronit Singh **CDAD-UH 1037** **Date:** 3 October, 2021

CYBERWARFARE

Week 6 Reading Summary

The article *"Understanding the Mirai Botnet"* by USENIX Security Symposium, explains and deeply analyzes the Mirai botnet attack on several high-profile companies and organizations in late 2016. It was one of the largest DDoS (Distributed Denial of Service) attacks of that time and infected nearly 600k devices by scanning and brute forcing login credentials on victim devices. IoT devices (Internet of Things) and embedded systems were its main targets due to the presence of various security flaws in them. The article goes over the details of its propagation mechanism, evolution and its after-impacts.

Mirai is the Japanese word for 'the future'. According to the article, "Mirai's reach extended across borders and legal jurisdictions, and it infected devices with little infrastructure to effectively apply security patches. This made defending against it a daunting task." (USENIX, 1094). This indicates that the attack gained its momentum primarily due to the lack of basic security system in these devices. This is because, as the article mentions, many of these devices used *default passwords and configurations* which were easy to exploit by using dictionary attacks. The Mirai botnet took advantage of the same. There is also a mention of BASHLITE, which belonged to "a DDoS malware family that infected Linux devices by brute forcing default credentials." (USENIX, 1095). The Mirai botnet belonged to the same family, but had greater features and capabilities. The article states that, "In contrast to BASHLITE, Mirai additionally employed a fast, stateless scanning module that allowed it to more efficiently identify vulnerable devices." (USENIX, 1095).

One of the main events during the attack timeline was the release of the Mirai botnet's source code to the public on hackforums.net. This was the starting point for the rise of Mirai botnet's variants that employed use of more features and attack vectors, thus improving the success rate of dictionary attacks and increasing the number of infected devices eventually. According to the article, "data suggests that consumer routers, cameras, and DVRs were the most prevalent identifiable devices." (USENIX, 1101). Moreover, "Dahua, Huawei, ZyXEL, and ZTE devices consistently remained in the Top 20." (USENIX, 1100). These were mainly the companies that manufactured these particular devices.

Although it was an attack on a huge scale, it alerted the companies and organizations and forced them to focus more on the security aspects of these devices. The article mentions many "technical and policy-based defenses for today's IoT ecosystem" (USENIX, 1106) namely security hardening practices by applying "ASLR, isolation boundaries, and principles of least privilege into their designs" (USENIX, 1106), providing automatic updates, notifications, facilitating device identification, defragmentation as well as taking note of end-of-life (lack of support from the vendor for a particular system) aspect. Moreover, by forcing the companies and organizations (that manufacture IoT devices) to comply with certain security requirements for these devices, one can comparatively mitigate much of the impact.

What surprised me?

The fact that most surprised me was that “even an unsophisticated dictionary attack could compromise hundreds of thousands of Internet-connected devices.” (USENIX, 1106) as was the case with Mirai botnet. This shows how these devices lack even the basic security infrastructure. Moreover, dictionary attacks can be performed by any novice hacker or teenager with the help of freely available powerful tools nowadays. This is a huge concern in this totally technologically dependent world.

Also, another statement mentioned in the article that concerned me was, “Researchers have found that IoT devices contain vulnerabilities from the firmware level [18, 19] up to the application level.” (USENIX, 1108). This indicates that there are security flaws present at each step which increases the chances of a successful attack against them and offers many paths or ways for the attacker to attack and succeed.

Questions?

1. How can DDoS attacks be prevented? What are the next steps that organizations take after getting attacked by DDoS/DoS?
2. Since the Mirai botnet was self-propagating, how are these malwares stopped in cases where the spread is eventually out of control?
3. How can one leverage the power of VPNs to prevent DDoS/DoS attacks?

References

Antonakakis, Manos. “Understanding the Mirai Botnet | USENIX.” USENIX, 2017, www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.