Network Security Assignment 1

Evan Cruz

B00320293

[Year]

The Dyn Distributed Denial of Service (DDOS) attack was one of the largest DDoS attacks of all time. The attack happened on October 21, 2016. The attack focused on Dyn, a domain name service provider and caused connection problems for a large number of popular websites. The source of the attack was attributed to Mirai botnets. Mirai botnets are mainly made up of Internet of Things (IoT) devices. Because the IoT is becoming so popular, many of the IP addresses that helped with the attack were shown to have been odd items such as baby monitors and cameras. Both Anonymous and New World Hackers have claimed that they were responsible for the attacks, but there is no large evidence pointing toward either party causing the attack. The attack has led authorities to question the security measures put in place on IoT devices.

On October 21, 2016 at approximately 11:10 UTC there was an attack launched on a DNS provider called Dyn. This attack continued until 13:20 UTC. A second attack was launched that lasted from 15:50 UTC until 17:00 UTC. The attacks were mitigated but the impact affected a large amount of users trying to connect to various sites and services.

The attack was mainly run using Mirai botnets. Mirai is malware that infects end-point devices and turns them into bots. These bots can later be used to create a larger group of bots forming a botnet. These botnets can be used for DDoS attacks since an attack can be launched from all of the bots within the botnet at any given time. Mirai botnets mainly target new IoT devices such as cameras. It works by scanning for IoT devices and avoiding certain IP ranges such as the IP addresses of the United States department of Defence. When it finds an IoT device it gains access by simply trying factory default usernames and passwords to log into the device. The device then performs normally but slightly less efficiently. The Mirai malware can be removed by simply shutting off the device and changing the password. Since there are so many IoT devices with default factory passwords, Mirai has an extremely large number of infected devices.

The first attack there was elevated traffic in a number of regions including Western United States, South America and Asia Pacific. Dyn saw this as a coming sign of a DDoS attack and attempted to initiate their incident response protocols. During this, the attack switched from those servers to Eastern United States Servers with a high volume of TCP and UDP packets targeted at port 53. The quick and multi-point attack caused the Network and Engineering operators at Dyn to deploy other tactics to stop the attack on top of the automated tactics. These tactics included traffic shaping and rebalancing the traffic by manipulating anycast policies. The tactics were fully in place by 13:20 UTC which is when the first attack subsided.

The second main attack began at 15:50 UTC. There were other smaller attacks in between the first and second attack but they were small enough that the tactics implemented in the first attack prevented any major damage. The same attack style was launched in the second attack but on a more global scale. Dyn stopped the attack by putting in place the same tactics they had during the first attack. This allowed them to mitigate the attack at approximately 17:00 UTC, with small attacks happening until about 20:30 UTC.

The attack, like all DDoS attacks, halted legitimate users from accessing the sites that Dyn provided. Since many people did not know what was happening, many page refreshes were requested causing 10-20x normal traffic. This made it hard to distinguish between legitimate traffic and malicious traffic since so many requests were being made. By analyzing the traffic heavily, it has been determined that at least one hundred thousand malicious botnet endpoint devices were linked to the attack. Dyn also verified that much of the attack was from Mirai-based botnets. The attack resulted in an estimated 1.2 terabits per second load on the datacentres.

The Dyn attack was still being analyzed as of October 26, 2016. It was a fairly complex and severe attack that needs large amounts of attention. They also put out protective measures, which they said would be extending and scaling those measures to be more protective. They have also been in discussions with Internet infrastructure providers to try and enhance their methods and also provide their learnings from the attack. It also sparks up information about IoT security. Specifically, the attack showed that IoT devices are very vulnerable to malware or viruses since they do not quite follow the same security measures that personal computing devices do.

The main vulnerability that was taken advantage during the attack is the fact that IoT devices have weak passwords that are factory given. These passwords were then easily guessed by the Mirai malware. The simple fix for most users is to just change their passwords. One company, Xiongmai, decided to recall some of the products that were used in the attacks. However, due to the laziness of people, devices won’t be returned and passwords won’t be changed which will still leave devices vulnerable.

Dyn was hit by one of the largest DDoS attacks of all time. It was affected in a way that had not been seen on a large scale before and affected many legitimate users worldwide. Major sites like Airbnb, Netflix, and Twitter were down for long periods of time. No one has been found to be responsible for the attacks even though some groups have claimed that they launched the attacks. Since the Mirai malware code was made open-source just weeks prior to the attack, it would be very difficult to pin point who would be responsible for the attack. The Dyn DDoS attack showed that DDoS attacks are still some of the most dangerous and effective cyber-attacks. It also showed that IoT needs higher security measures since the Mirai malware breaks in solely through brute force methods. While security is improving for networks, there is still possibly endless amounts of work to be done to try and make the internet a safer, more secure area.

Burke, Samuel. *Massive Cyber Attack Turned Ordinary Devices into Weapons.* CNN Tech. <http://money.cnn.com/2016/10/22/technology/cyberattack-dyn-ddos/>

Hilton, Scott. *Dyn Analysis of Friday October 21 Attack.* Dyn.<http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>

Woolf, Nicky. *DDos Attack that Disrupted the Internet was Largest of its Kind in History, Experts Say.* The Guardian. <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>

Moffitt, Tyler. *Source Code for Mirai IoT Malware Released.* Webroot. <https://www.webroot.com/blog/2016/10/10/source-code-mirai-iot-malware-released/>

Bonderud, Douglas. *Leaked Mirai Malware Boosts IoT Insecurity Threat Level.* Security Intelligence. <https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/>