By: Ian Hagmann, Carson Viscusi, and Thomas Roeseler

2016 DYN CORPORATION DDOS ATTACK

WHAT HAPPENED?

An unknown group launches 3 consecutive distributed denial of service attacks against the DNS provider Dyn, making major parts of the internet to become unavailable.

AUGUST 2016

The Mirai Botnet code is created, originally intended to to be used to DDoS minecraft servers.

LATE SEPTEMBER

The Mirai Botnet code leaks out onto the internet. This is the code which will then be taken to launch the attack.

OCTOBER 21ST, 2016 11:10 AM

The first DDoS attack against Dyn is launched. Internet users notice slower que times and inability to access some sites. The attack lasts until 1:20 PM.

3:50 PM UTC

The second attack is launched, which continus until 5:00 PM. All previous issues have returned along with disruption of Advanced Dyn Monitoring Services.

8:00 PM UTC

The final attack against the Dyn corporation is launched. At this point the internet as a whole in the US and Europe has been crippled. Only small independently hosted websites are accessible, but still page loading times are at a record high.

OCTOBER 21ST, 2016 10:10 UTC

Dyn announces that the Internet of Things attack is over. It takes upwards of 4 days for internet speeds to return to normal.

DECEMBER 13TH, 2017

Three men, Paras Jha, Josiah White, and Dalton Norman, enter guilty pleas with the justice department in cybercrime cases surrounding the Mirai botnet and the Dyn attacks of 2016.

2016 DYN CORPORATION

DDOS ATTACK

IMPACT

Dyn is a provider of major DNS servers. DNS servers are responsible for connecting the names of domains to actual IPs of servers hosting those domains. While the servers were down people were unable to reach websites like Amazon, Twitter, Github, and many more. Organizations spend an average of $2.5 million in recovery costs from the attack. Dyn also lost over 14,000 customers using them as a DNS provider.

HOW?

The attack was perpetrated by the Mirai Botnet. The Mirai Bonet was built on IOT devices with ARC processors that have default credentials. Mirai scanned for open Telnet ports and tried 61 default credentials on the devices it found. If it successfully logged in it would infect the device with Mirai malware. A command would be sent to port 23 on infected machines to send mass amounts of traffic to specified IPs.

MITIGATION STRATEGIES

- Network Monitoring
- Create a Response Plan (so you can respond quickly and efficiently)
- Communication Plan
- Use good cybersecurity practices
- Infrastructure should be resilient and more than just firewalls
- Data centers on different networks, data centers in different locations, servers in different data centers

2016 DYN CORPORATION

DDOS ATTACK

References:

Wikipedia contributors. (2022, December 2). Mirai (malware). In Wikipedia, The Free Encyclopedia. Retrieved 17:00, December 6, 2022, from https://en.wikipedia.org/w/index.php?title=Mirai_(malware)&oldid=1125076795

Wikipedia contributors. (2022, December 6). DDoS attacks on Dyn. In Wikipedia, The Free Encyclopedia. Retrieved 17:01, December 6, 2022, from https://en.wikipedia.org/w/index.php?title=DDoS_attacks_on_Dyn&oldid=1125866352

Hamilton, J. (2020, June 6). Update: Timeline of the massive ddos dyn attacks. CloudTweaks. Retrieved December 6, 2022, from https://cloudtweaks.com/2016/10/timeline-massive-ddos-dyn-attacks/

Fruhlinger, J. (2018, March 9). The Mirai botnet explained: How IoT devices almost brought down the internet. CSO Online. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Ragan, S. (2016, October 21). DDoS knocks down DNS, data centers across the U.S. affected. CSO Online. https://www.csoonline.com/article/3133992/ddos-knocks-down-dns-datacenters-across-the-u-s-affected.html

What is the Mirai Botnet? (n.d.). Cloudflare. https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

Woolf, N. (2016, October 26). DDoS attack that disrupted 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

Young, K. (2022, January 10). Cyber case study: The Mirai DDoS attack on Dyn. CoverLink Insurance - Ohio Insurance Agency. https://coverlink.com/case-study/mirai-ddos-attack-on-dyn/

Maria, G. (2020, December 15). *How to prevent a DDOS attack-6 strategies for small businesses*. GetApp. https://www.getapp.com/resources/how-to-prevent-a-ddos-attack/

SecurityScorecard. (2021, August 16). *10 Best Practices to Prevent DDoS Attacks*. SecurityScorecard. https://securityscorecard.com/blog/best-practices-to-prevent-ddos-attacks