Dyn DDOS Cyberattack – a case study

Aishwarya Sreekanth
Aalto University

Prashant Sri
Aalto University

Teemu Vartiainen
Aalto University

***Abstract*—The Dyn DDoS attack was one of the biggest distributed denial of service attacks ever launched. The attack affected the availability of major internet services. It was launched by exploiting vulnerabilities in insecure Internet-of-Things devices. The attack also used a strategy of launching many different kinds of attacks at the same time by using hundreds of thousands of source devices. There are many types of defenses that could be used to mitigate against such attacks. However, many of the mitigation strategies prove to be challenging to implement. Hybrid solutions by multiple different organizations are needed to secure the internet against such attacks.**

Keywords*—*DDoS attack, Internet of things, cybersecurity

I. Introduction

The Dyn attack, which took place on 21st October of 2016, is one of the largest data breaches in history. This attack overturned a large portion of the internet in the United States and Europe and affected plenty of services. The source of the attack was the Mirai botnet. This botnet is unlike other botnets, consisting of so called Internet-of-Things (IoT) devices such as internet protocol (IP) cameras, printers, digital video recorders.

Dyn is an Internet Performance Management (IPM) company, who is believed to be a pioneer domain name system (DNS) service provider. They also offer internet infrastructure services and products such as monitoring and analytics, control, online infrastructure optimization and e-mail.

The objective of a Denial of Service (DoS) attack is to deny or disrupt authorized users from accessing a resource or service. For this malicious activity, the attacker uses one bot to flood the targeted victim or resource denying access to the authorized users. In the case of Distributed Denial of Service (DDoS) attack thousands of bots are controlled by the attacker to flood the targeted victim.

The sources from Dyn reported that the service provider experienced a Distributed Denial of Service (DDoS attack). Mitigating DDoS attacks was common to the Network Operations Center (NOC) team of Dyn. However, the NOC team could identify that this attack was unusual and bizarre.

II. The cyberattack

Per the official analysis summary from Dyn [3], the DDoS attack on their DNS infrastructure happened on 21st October 2016. Upon detailed analysis of the situation, this attack was termed to be an advanced, well planned and complex attack. And Dyn faced a series of DDoS attacks on the same day within few hours.

According to Dyn[3], Mirai botnets have contributed to a major volume of attack traffic. Mirai is a piece of malware which infects and exploits the vulnerable network devices on the Internet, preferably IoT devices. Upon successful infection, the bot gets registered to a Command and Control Server (C&C) which controls the botnet during attacks. Mirai malware exploits those network devices that authenticate using default credentials. Recently, the source code of the Mirai malware was also published in a public forum.

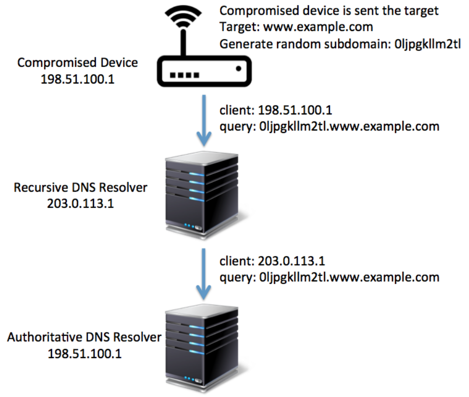
Compromised device is sent the target
Target: www.example.com
Generate random subdomain: 0ljpgkllm2tl
Compromised Device
198.51.100.1
client: 198.51.100.1
query: 0ljpgkllm2tl.www.example.com
Recursive DNS Resolver
203.0.113.1
client: 203.0.113.1
query: 0ljpgkllm2tl.www.example.com
Authoritative DNS Resolver
198.51.100.1

Fig. 1. DNS attack mechanism

A. Attack Timeline

The first attack was staged between approximately 11:10 UTC to 13:20 UTC. Initially, a huge inclination in the bandwidth consumption was witnessed at various locations of Dyn DNS infrastructure, which imitated a situation like that of a DDoS attack. The Engineering and Operations team of Dyn implemented few mitigation protocols but the attack began to target the US-East region. This abrupt large volume of data was originated from various source IP addresses and were destined for destination port 53, where the data packets were composed of TCP and UDP packets.

The next attack was carried out between 15:50 UTC and 17:00 UTC. Unlike the previous attempt, this attack was targeting almost all the available Managed Infrastructures of Dyn around the globe. Though the second attempt consisted of same set of attack vectors and protocols used during the first attack, it still managed to disrupt the functionalities of the service provider despite the deployed incident response mechanism.

B. Attack Mechanism

DNS protocol was used to perform the DDoS attack on the DNS servers of the Dyn. The attack vectors used to perform DDoS attack include recursive DNS query mechanism or DNS Waterfall Torture or authoritative DNS exhaustion attack [5][6][1]. Architecture of DNS server infrastructure consists of Recursive DNS resolver and Authoritative DNS resolver. A recursive DNS resolver receives the DNS query from the bot to resolve a 12-digit pseudo random host from the domain of the authoritative resolver. It is ensured that the recursive DNS resolver fails to resolve the DNS record of random host, so that the query gets forwarded to the authoritative resolver, as seen in figure 1. This mechanism removes the protection of caching layer from authoritative DNS resolvers [1]. The aim of this attack vector is to forward exceptionally large amount of DNS queries to the authoritative DNS resolver and exhaust the capacity of authoritative DNS resolver to resolve queries.

III. Impact

This DDoS attack affected the anycast servers of Dyn[5]. It also prevented the services for resolving legitimate DNS queries. It is estimated to have generated more than 40 to 50 times of the normal traffic volume and the expected number of involved botnets during the attack amounts to 100,000 [3]. Per a few reports, the total volume of data involved during this attack is estimated to be 1.2Tbps. A few major US websites including Paypal, Spotify, Twitter and Amazon faced connectivity issues. The various other web services of companies such as BankWest, HSBC and Ticketmaster were also affected [8]. According to Bitsight [8], approximately 8 % of the Dyn DNS customer base terminated their contract after the attack.

IV. Mitigation actions

There are three types of actions that can be used to mitigate attacks like the Dyn DDoS cyberattack: actions that a single defender can do to defend against a DDoS attack, actions that can be done for the IoT devices, and actions that can be done globally to reduce these types of attacks.

For a single defender, the most important countermeasure against these attacks is awareness. Organizations should know that these types of threats exist, and what it means. The awareness seems to be increasing. [5] A DDoS attack is very public in nature, since it attacks on the availability and tries to bring down service. Some other attacks may be stealthier and could go unnoticed, but a DDoS attack bringing down a service can hurt the reputation of an organization. When an organization wants to increase their security against DDoS attacks, several measures such as firewalls and antivirus must be used. There are also DDoS protection services, hardware or software, that work on the edge of the network filtering out these types of attacks.

The types of attacks used in the Dyn DDoS case were not anything new. However, the use of IoT devices as a massive botnet platform was. Attackers can also use them as an entry point to get into the network and then move laterally to other systems and machines. [2] Furthermore, because of the massive usefulness of these devices, organizations cannot just stop using them. Because of these reasons, organizations need to start thinking differently about these devices. IoT devices should be considered as computers part of the network like anything else. They should be monitored like any other computers, and segmented away from sensitive systems. This means disconnecting any unnecessary connections to and from these IoT devices to reduce the attack surface an attacker can use. Some researchers have even suggested actively fighting back against the botnets, by crashing the source devices or disabling the vulnerabilities remotely. [5]

To reduce these attacks globally there are a few measures. The attacks could be identified by the internet backbone operators and cut from the system before they even reach the destination. The IoT devices itself could be proactively secured against these attacks. [4] Using randomized default passwords alone could make a big difference.

V. Challenges in mitigation

There are several challenges to these mitigation strategies. The DDoS traffic may be difficult to detect or defend against, the IoT devices may have limited capabilities to support good security, and the global market does not have incentives for companies to fight these issues.

The traffic in these DDoS, especially in the Mirai worm case, looks like ordinary traffic. Since Mirai launches several types of attacks from multiple legitimate sources containing legitimate-looking traffic, it can be difficult to filter out or detect, without blocking normal legitimate traffic as well. [5] Furthermore, since the attack consists of a wide variety of different attacks on several endpoints, mitigating it would require several defenses built on top of all these endpoints. In a similar manner, the sources of the attack are distributed well, on hundreds of thousands of IoT devices, so they are difficult to filter out.

Because of the use of cloud services, it is increasingly difficult to block these attacks with hardware systems at the edge of the network, since such edge may not exist with cloud systems used in conjunction with systems on premise. The situation requires protections that are moved further upstream or into the cloud itself. The situation calls hybrid solutions that are more challenging to set up and maintain. This requires organizations to set up security strategies to cover themselves against these many types of attacks. In the end, it comes down to balancing risk against the cost. No security measure is impenetrable against all attacks, but increasing defenses works as insurance protecting against potential attacks or turning the attacker looking for targets elsewhere. [5]

There are several challenges in securing IoT devices. They usually run on minimal hardware and stripped-down operating systems, so they may not have the capabilities to run sophisticated security measures. In addition, if a vulnerability has been found, the user may not have any incentive to perform an update. Furthermore, many devices may not have update capabilities at all. Similarly, the systems that all the IoT devices are connected to may not have the capabilities to monitor all the traffic from all the devices. [2]

In the current market, all the liability from these attacks is on the victim. The cost of producing the attacks can be surprisingly small, especially since the tools like Mirai are out in the open for anyone to get and use. However, defending against the attacks, buying services and hardware, as well as dealing with the consequences, is expensive for the victim. Furthermore, there are ethical issues surrounding the defense. The attacker does not care about breaching the security of a device, but what if a defender does the same when trying to defend against the attack? It is not clear who would be responsible for the damage for such hacking back [4].

In addition, there is no market incentive for ISPs and backbone operators for preventing these kinds of attacks [7]. They do not have anyone to bill after an attack has been avoided or after preventative measures have been set up. Similarly, the IoT device manufacturers do not have much incentive to spend time and money in improving the defenses of the devices. After an IoT device has been released to the market and sold there is little incentive on maintaining the firmware or updating the security. This situation is unlikely to change unless other driving forces like government enforcement are set up. Governments could set up regulations to make sure device manufacturers are held liable after their insecure devices are used in an attack. Another possibility could be if other device manufacturers started using security as a selling point. This would start driving the sales of insecure devices down.

VI. Conclusion

The Dyn DDoS attack did not consist of any mechanisms that were groundbreaking in their nature. All the mechanisms were well known and some of them very simple. However, what was new was the way the Mirai worm combined multiple attacks into one and infected hundreds of thousands of insecure devices. This massive volume of the distributed attack was unheard of.

Mitigating such attacks proves to be challenging. Because of the large number of different kinds of attacks and the massive number of source machines, hybrid solutions are necessary from multiple stakeholders ranging from backbone providers to lawmakers to device manufacturers. Thus, until big changes in how the internet is set up and regulated happen, service providers cannot count on the issue being fixed from the outside. Instead, to prepare for these attacks each service administrator needs an in-depth defense strategy that is balanced to their own needs.

References

[1] Chris Baker. *Recent IoT-based Attacks: What Is the Impact On Managed DNS Operators?* 2016. URL: http://dyn.com/blog/recent-iot-based-attacks-what-is-the-impact-on-managed-dns-operators/.

[2] Nathaniel Gleicher. *The Big Lesson We Must Learn From The Dyn DDoS Attack*. 2016. URL: http://www.darkreading.com/endpoint/the-big-lesson-we-must-learn-from-the-dyn-ddos-attack/a/d-id/1327432.

[3] Scott Hilton. *Dyn Analysis Summary Of Friday October 21 Attack*. 2016. URL: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

[4] Kalev Leetaru. *The Dyn DDOS Attack And The Changing Balance Of Online Cyber Power*. 2016. URL: https://www.forbes.com/sites/kalevleetaru/2016/10/31/the-dyn-ddos-attack-and-the-changing-balance-of-online-cyber-power/.

[5] Steve Mansfield-Devine. "DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare". In: *Network Security* 2016.11 (2016), pp. 7–13.

[6] Radware. *DDoS Attacks on DNS Services*. 2016. URL: https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/dns-services-under-attack/.

[7] Bruce Schneier. *Lessons From the Dyn DDoS Attack*. 2016. URL: https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/.

[8] Stephanie Weagle. *Financial Impact of Mirai DDoS Attack on Dyn Revealed in New Data*. 2017. URL: https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html.