Module Code: COMP4035

Module Name: Systems and Networks

Deliverable: Report – An overview of DDoS

Module Convenor: Gail Hopkins

Student ID Number: 20299113

Date of Submission: 29th October 2020

Word count: 2516

Abstract

With the development of information technology, more and more traditional industries are going to be digitalized. In addition, Cisco(2020) states that the number of devices connected in networks will be triple than the whole population by 2023. Looking around, the Internet has already become an essential part of human's life imperceptibly. Living in this age, the Internet indeed improves the quality of human's life, such as online classes, online shopping, IM(Instant Messenger), and smart city. However, in the meantime, as the Internet is growing, serval threats are also growing and becoming more diverse (Cisco, 2020). There are many different threats in the network, this report focused on DDoS, which is Distributed-Denial-of-Service attack. The report aims to give an overview of DDoS, including a definition, classification, real-world cases, possible solutions and trend prediction.

1. Introduction

With the growing quantity of the device connected on the internet, it simultaneously makes the power of the DDoS growth exponentially. Cisco(2020) points out the number of DDoS attacks will be 15.4 million by 2023 all over the world. Therefore, it is worthy to pay attention to DDoS. Figure 1 shows a simple diagram of DDoS. The attacker utilizes some hacker technologies to control lots of vulnerable devices on the internet, then use the controlled devices also called bots to access the target. Because all of the requests are from valid users, it is difficult to distinguish and separate the requests from the DDoS and the normal users. Due to the quantity of the requests are far beyond the target server's response capacity, the server will put all the new request to a waiting list or just directly deny all of them. Therefore, the service which supported by the target server becomes not available. At last, all users can not use the service.

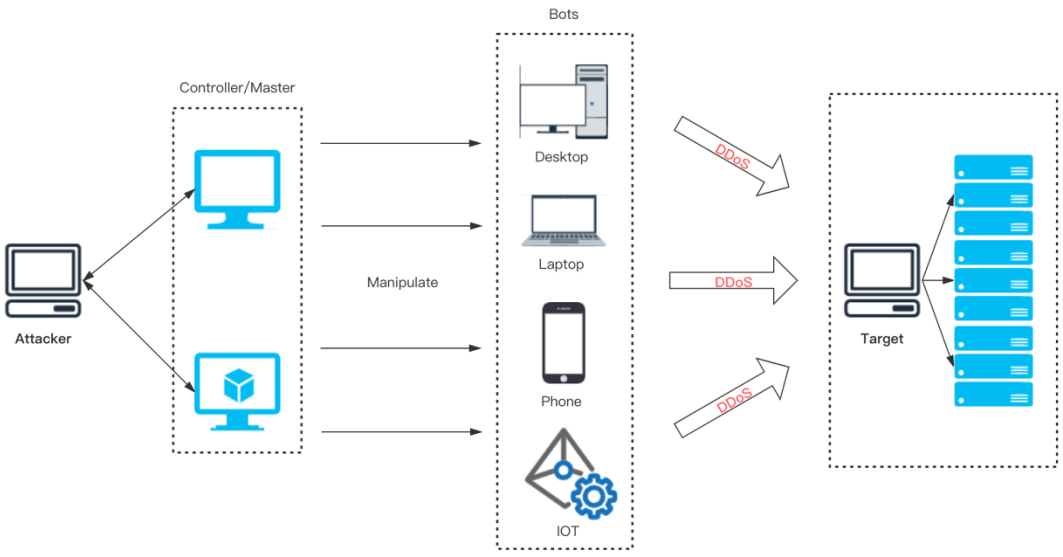

Figure 1: A simple diagram of DDoS

Types of DDOS

According to Cloudflare(2019), Esecurityplanet.com(2017) and Penta Security(2017), DDoS attack can be roughly divided into three categories, which are Volume-Based Attacks, Application Layer Attacks and Protocol Attacks. Figure 2 shows a few details of the category. Usually, the DDoS attack combined one or more types. Therefore, the real-world examples to illustrate each type of attack are only for the sake of demonstration.

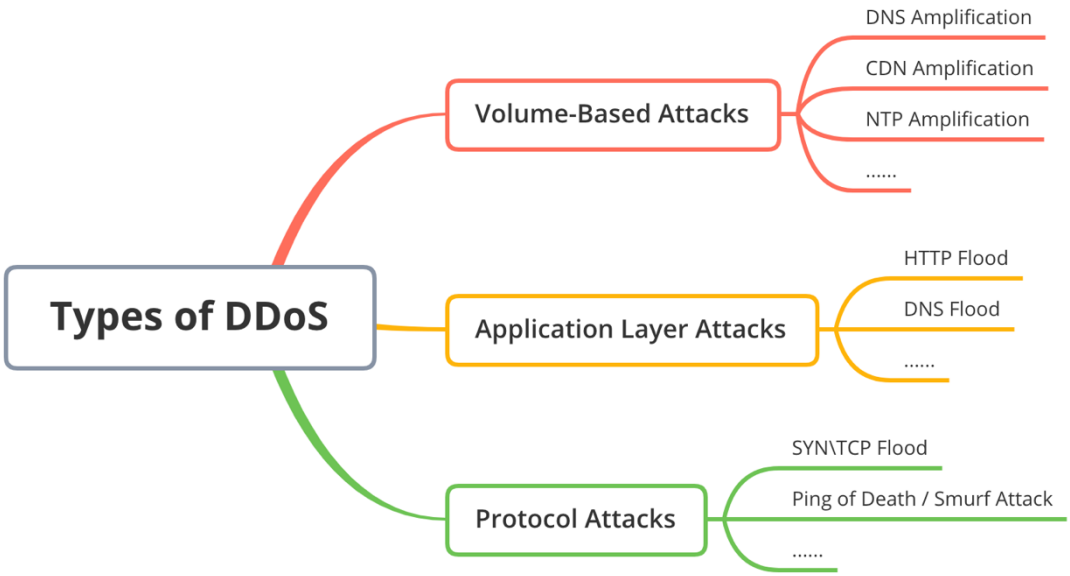

Figure 2: Types of DDoS

2. Volume-Based Attacks

Volume-Based Attack is the most common type. It is also a reflection-based attack. That means the attacker utilizes a form of amplification such as DNS and CDN to create massive congestion by consuming all available bandwidth between the target and the internet (Cloudflare, 2019). Figure 3 shows a simple sketch map of the Volume-Based Attack.

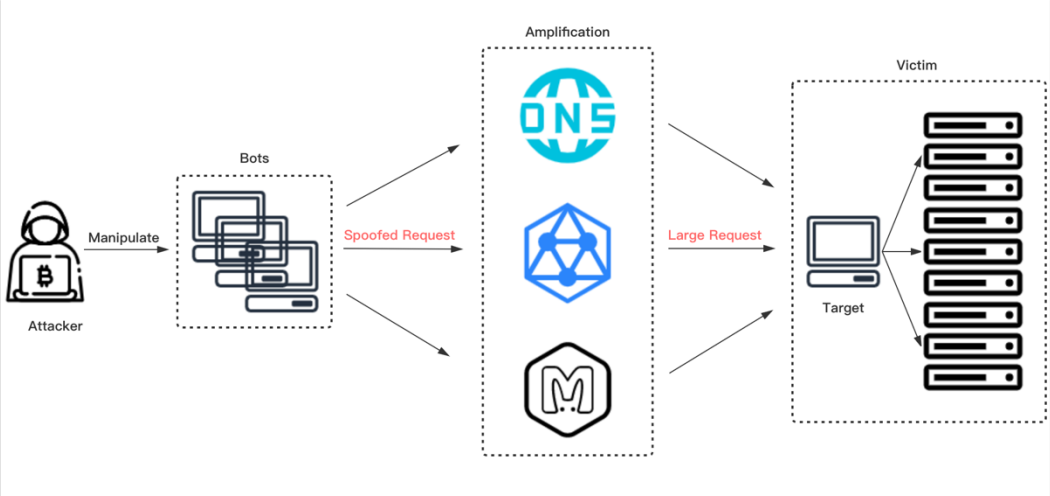

Figure 3: Volume-Based Attack

2.1. GitHub 2018 DDoS Incident

The Incident

According to Kottler(2018), Github - a code management and cooperation platform, which encountered DDoS attacks on 17:21 UTC 28/02/2018. The attack made "github.com" unavailable from 17:21 UTC and lasted 6mins to 17:26 UTC. When the status of the Github service turned abnormal, a Github's on-call engineer was notified by their network monitor system. By examining the transit-in and transit-out graph, they did a quick response to move their network traffic to Akamai, which can provide larger network capacity (Kottler, 2018). The network transit-in and transit-out can refer to figure 4. After that, "github.com" was in an intermittently unavailable until 17:30 UTC and finally back to be stable. Figure 5 shows the attack peaked at 1.35Tbps, that is 13 times more than the normal. This attack was quick, vast and low traceability. Although they claimed this attack did not affect the user's data, for an online service's availability, every second count, it indeed made a huge strike.

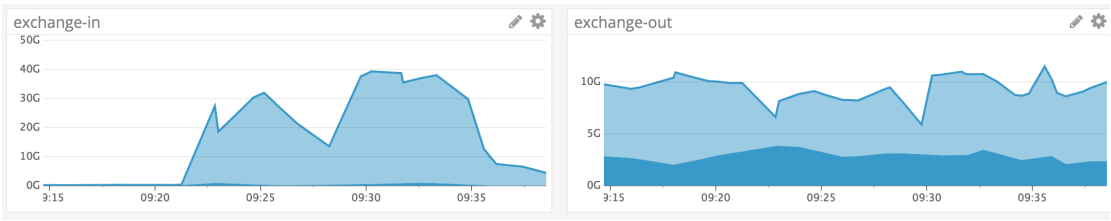

Figure 4: Network transit-in and transit-out

Source: February 28th DDoS Incident Report (Kottler, 2018)

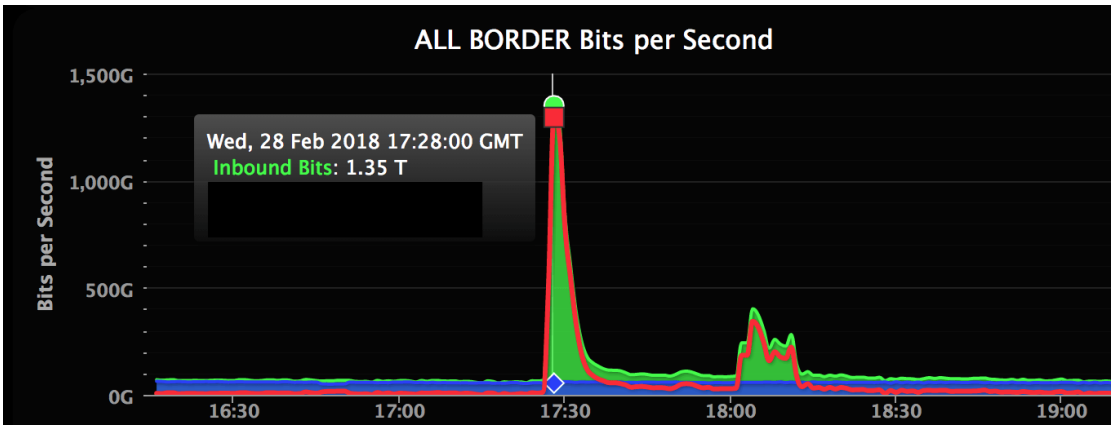

Figure 5: Attack Peak

Source: February 28th DDoS Incident Report (Kottler, 2018)

Rationale

According to Majkowski(2018), this attack based on an amplification vector - Memcached. When the option "UDP support" is enabled in Memcached, that makes the Memcached instances accessible on the public internet (Kottler, 2018). Because of this misconfiguration, the spoofed requests are able to access Memcached instances and get large responses to another address, the target address. Memcached is often used to reduce the number of requests of users by caching data (memcached.org, n.d.). Therefore, companies usually support sufficient bandwidth to Memcached instances. Due to large responses and sufficient bandwidth, the amplification factor can be up to 51,200x amplification (Majkowski, 2018). The amplification factor of

the Github DDoS attack is 51,000. Figure 6 shows Majkowski(2018) used the command-"tcpdump" to demonstrate the large response.

```
$ sudo tcpdump -ni eth0 port 11211 -t
IP 172.16.170.135.39396 > 192.168.2.1.11211: UDP, length 15
IP 192.168.2.1.11211 > 172.16.170.135.39396: UDP, length 1400
IP 192.168.2.1.11211 > 172.16.170.135.39396: UDP, length 1400
...(repeated hundreds times)...
```

Figure 6: Demonstrate a large response

Source: Memcrashed - Major amplification attacks from UDP port 11211 (Majkowski, 2018)

Solution Evaluation

About the Github DDoS incident, the on-call engineer chose to switch their network to a larger capacity network. It should be the most efficient way to mitigate the influence when the attack has happened. In addition, it can buy some time for other engineers to analyse this situation in the meantime. Then, try to take more prise reaction to prevent the same attack happened again. In such a short time, there is no enough time to do a deep analysis then reacted accurately. For a giant company, stop the losses in time ought to be a good choice.

Preventative Measure

1. Read the configuration document carefully, try to prevent the misconfiguration by careless or misunderstanding. In this case, turn off the UDP support option if don't need.
2. Put the Memcached instances in a safety network domain, if there is some special requirement, use ACL.
3. Keep the Memcached instances to be the LTS version to make sure the known bug has been fixed.

3. Application Attacks

Application Layer Attacks usually find the weakness of OSI layer 7, then exhaust the resources of the target server by establishing a large number of connections like legitimate users (Kesavan, 2016). Figure 7 displays a simple diagram of the Application Layer Attack.

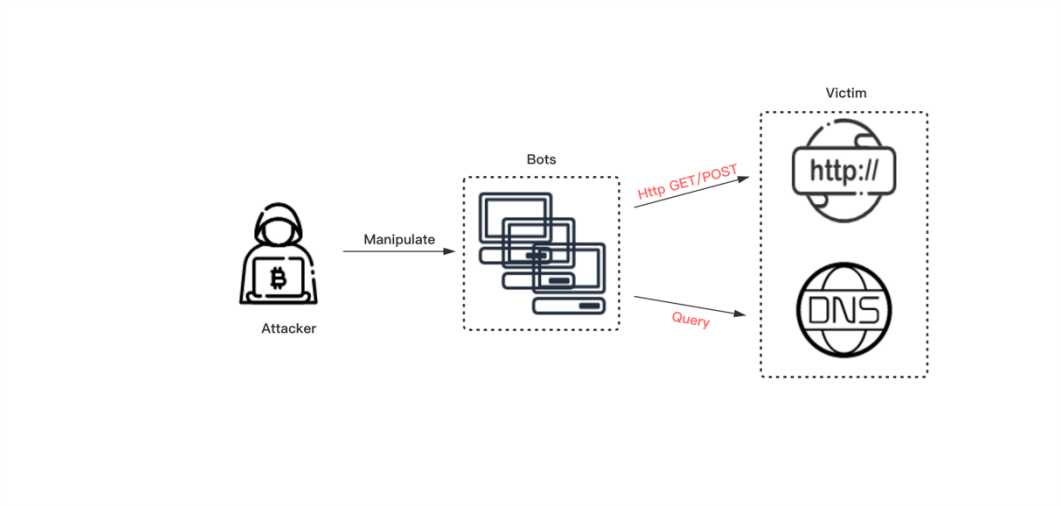

Figure 7: Application Attacks

3.1. Dyn DDoS

The Incident

According to Sreekanth, Sri and Vartiainen(n.d.) and Helmke(2019), Dyn was attacked by a series of DDoS from numerous IP address on October 21st, 2016. Dyn Inc. was an internet performance management and DNS provider. There were lots of companies that relied on Dyn's DNS, such as Twitter, Spotify and Paypal (Corero, 2017) and (Red Button, 2018).

Timeline(UTC)

- 11:10 - The first wave attack happened, the bandwidth consumption of

Dyn DNS instances arose exceptionally.

- 13:20 - Dyn team had implemented a few mitigations and restored service. The attack was resolved temporarily.
- 15:50 - A second wave attack happened, the range of bots is larger than the first wave, it was from all over the world.
- 17:00~19:00 - The attack was almost mitigated (Helmke, 2019) and (Sreekanth, Sri and Vartiainen, n.d.).

This incident struck Dyn and its customs. Because of the DDoS attack, Dyn DNS rejected all the query requests from the legitimate customs, the customs faced connectivity issues, their website or online services became unavailable. Figure 8 shows an outage map of this impact (Etherington and Conger, 2016). According to (Varghese, 2017), Dyn lost 8% of the domains on business, it is about 14500.

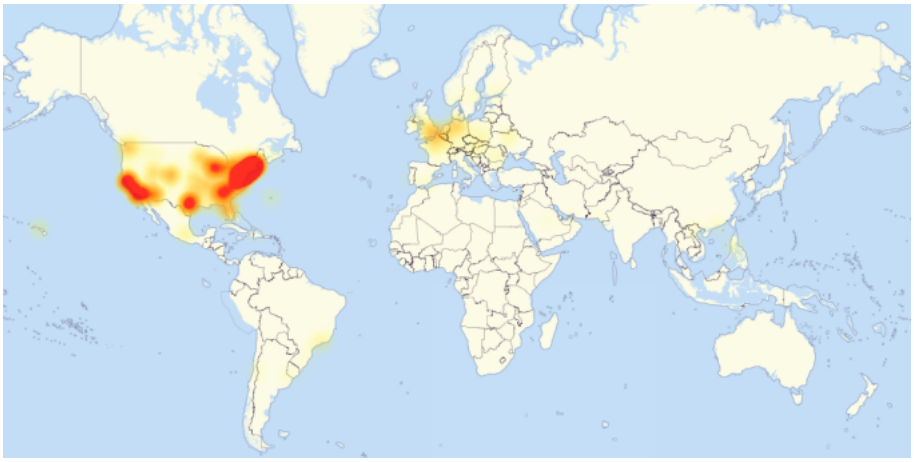

Figure 8: Outage map of this impact

Source: Large DDoS attacks cause outages at Twitter, Spotify, and other sites (Etherington and Conger, 2016)

Rationale

Firstly, the attacker used Mirai various to manipulate a mass of vulnerable IoT

devices, called bots (Schneier, 2016). Secondly, using these bots to send query requests with a random or nonexistent subdomain. It made all the recursive DNS servers were failed to resolve the information. Then, all the pressure was on the authoritative DNS. That made huge congestion even breakdown. According to Schneier (2016), the peak of this attack is up to 1.2Tbps. The rationale of this attack is exploiting the DNS query mechanism then exhaust all the resource of the authoritative DNS (Sreekanth, Sri and Vartiainen, n.d.). Figure 9 shows a diagram of this mechanism. Finally, the service was down.

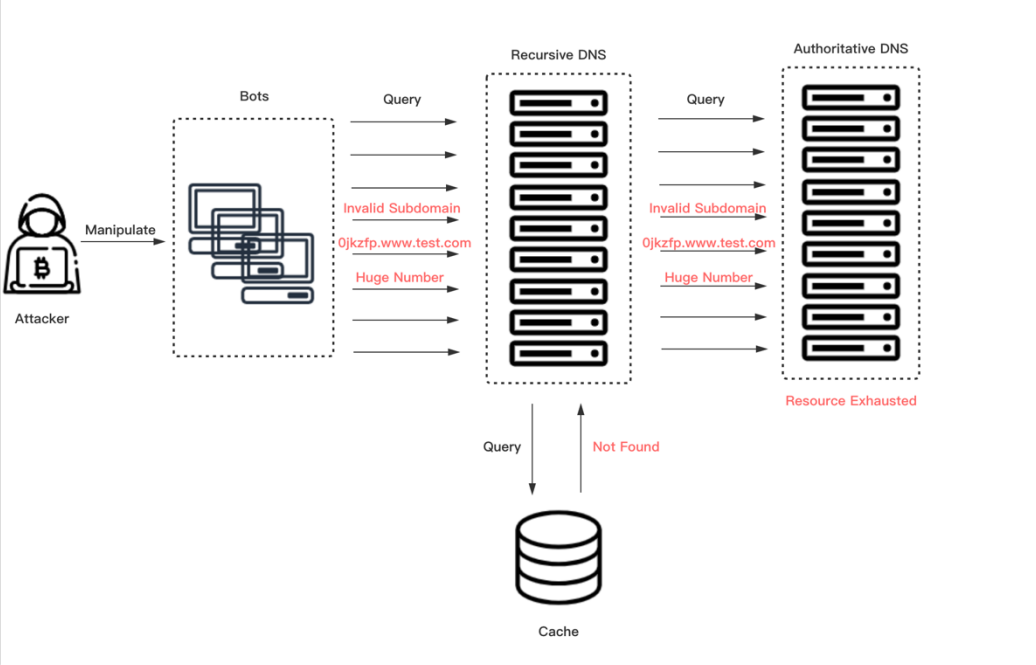

Figure 9: DNS Flood

Solution Evaluation

When the DDoS happened, Dyn implemented a serious of mitigations including: "traffic-shaping incoming traffic, rebalancing of that traffic by manipulation of anycast policies, application of internal filtering and deployment of scrubbing services" (Helmke, 2019). After the Dyn was

purchased by Oracle, the original link of Dyn's postmortem was no longer accessible-"https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/". Therefore, it is difficult to dig in some details of the react action of this attack. However, refer to the record by Helmke(2019), Dyn's solution is reasonable.

Preventative Measure

For the DNS service Provider:

1. They should have the ability to switch their DNS service route to a safety backup network environment to mitigate the impact in time.
2. They should be able to examine the attack vectors easily by the monitor system and have an emergency plan in advance.
3. They should set an attack detection system in front of the authoritative DNS.

For the Custom of the DNS server:

1. They had better prepare more than one DNS provider in advance and easy to switch.
2. They ought to ensure their monitor system is accurate enough to examine where is the problem from.

For the IoT manufacturer:

1. They should make sure their products should be set a complexed password instead of the default password when the custom begin to use them.
2. It is essential to design a health check module in the IoT device to monitor and alert the abnormal behaviour.

3.2. Wikipedia DDoS Attack

The Incident

Wikipedia is a free online knowledge repository to encourage people to cooperate voluntarily to share knowledge. According to Wikimedia Foundation(2019), Wikipedia was forced to be offline intermittently by a cyber attack. The attack happened from approximately 18:00 UTC 06/09/2019 to 2:40 UTC 07/09/2019, which lasted up to 9h (NETBLOCKS, 2019).

Timeline(UTC)

- 06/09 17:40 - The availability of HTTP server had a significant drop(40% global). The HTTP response time increased to 353ms, which is 5 times than normal. In, addition, the packet loss was up to 60%.
- In the period - Wikimedia began to insert Cloudflare as a prefix in their network structure.
- 07/09 2:40 - Wikipedia was finally back online (NETBLOCKS, 2019) and (Henthorn-Iwane, 2019).

Rationale

According to Figure 10, it shows a monitor of the availability of the HTTP server of Wikipedia. The legend "Connect" below the "Status by Phase" showed that users can not establish a TCP connection with Wikipedia, because the three-way "handshake" was unsuccessful. Therefore, from the view of the user, Wikipedia seemed like offline (Henthorn-Iwane, 2019). Similarly, the HTTP response time and packet loss raised simultaneously.

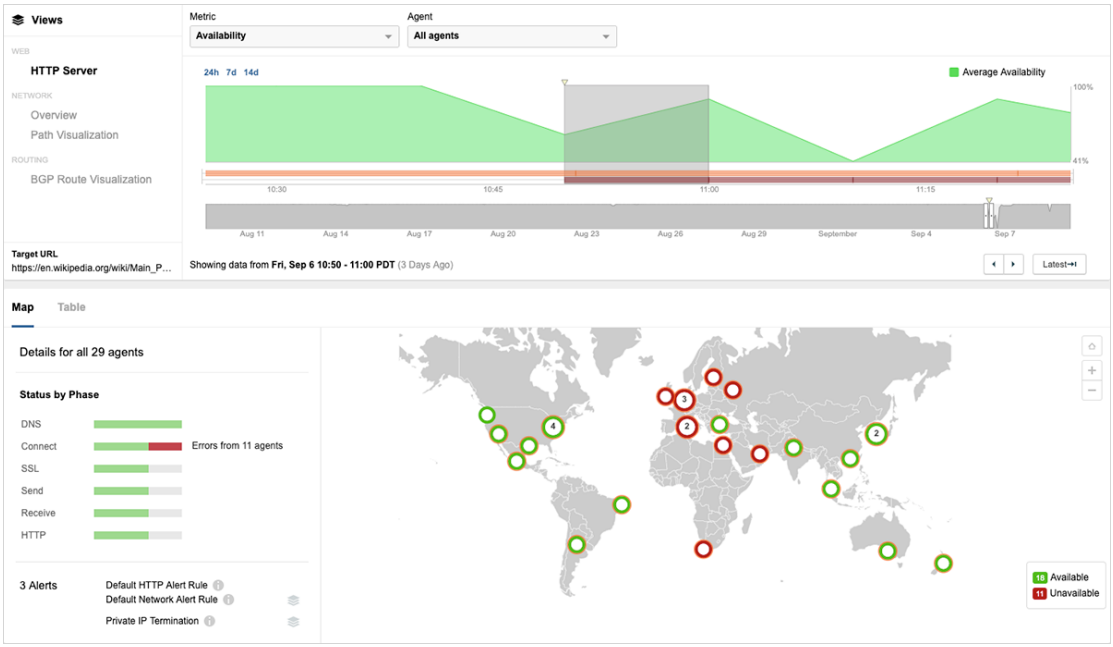

Figure 10: The Availability of the HTTP server of Wikipedia

Source: Analyzing the Wikipedia DDoS Attack (Henthorn-Iwane, 2019)

Solution Evaluation

Without no more details on how the Wikipedia SRE team handled with this attack, the main remediation step that we can know is that they asked help for a security company - Cloudflare. By restructuring the network route, Cloudflare became the front-ended part of Wikipedia (Henthorn-Iwane, 2019). In this way, the DDoS attack was mitigated at last.

Preventative Measure

1. Traffic profiling techniques: Analyse the request information, especially the Host and Method (NETSCOUT, n.d.).
2. Establishing an IP reputation database, record and category each request source IP.
3. It is essential to have a WAF as a prefix of the HTTP server.

4. Protocol Attacks

Protocol Attacks exploit a weakness in layer 3 and layer 4 of the OSI model. It aims to consume all the processing capacity of the target or the intermediaries resources such as firewall and load balancer (Penta Security, 2017). Figure 11 displays a simple diagram of the Protocol Attack.

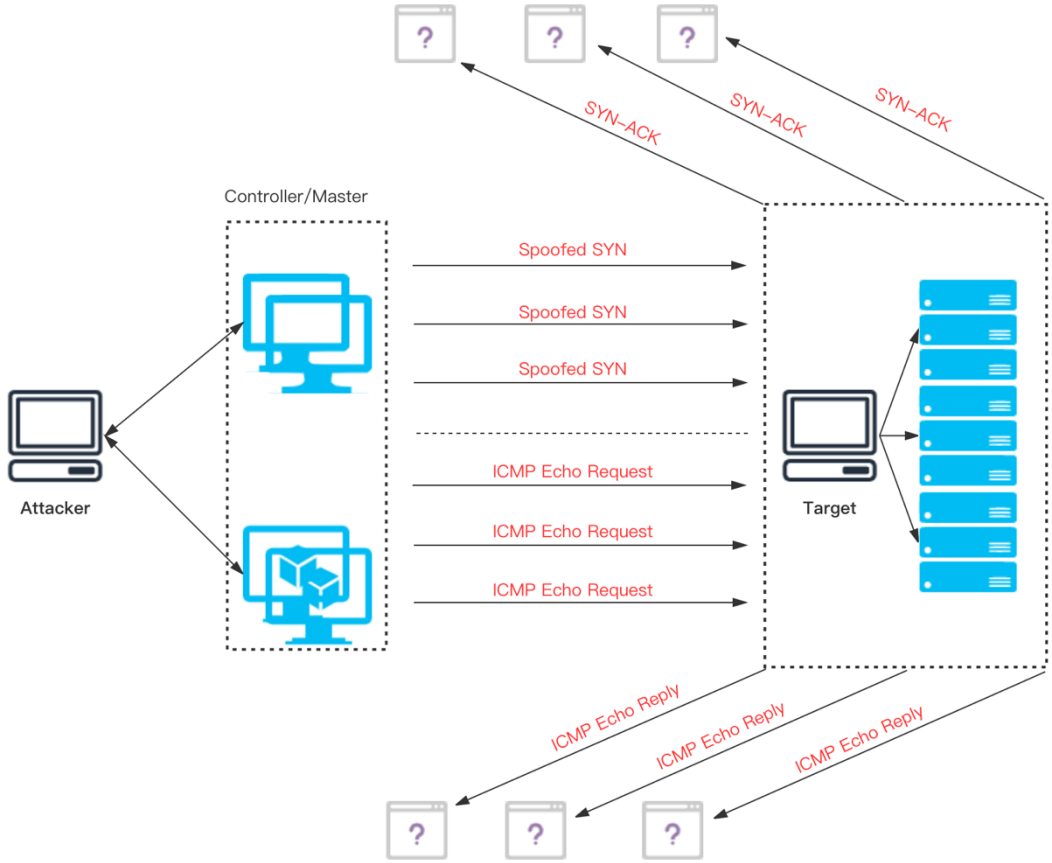

Figure 11: Protocol Attacks

4.1. Root Name Server DDoS

The Incident

The Root Name Server is a DNS service for the root zone and replies the query request by sending back the list of the authoritative name servers. There are 13 DNS root servers all over the world (enisa, 2016). According to

Lawton(2007) and Vixie, Sneeringer and Schleifer(2011), an ICMP DDoS attack was launched to the 13 DNS root name servers at 20:45 UTC 21/10/2002. This is the first time that DNS root name servers were attacked. This attack lasted approximately one hour. The Attack volume was 50 ~ 100Mbps on each root server, which was not a small number at that time (Vixie, Sneeringer and Schleifer, 2011). However, these servers were configured to block all the ICMP request. There was just a little impact.

Rationale

ICMP request can be easily launched by "ping" command in Unix. When an ICMP ECHO request is sent to a server, the server needs to reply back. That is why "ping" can be used to check whether a server is active. If the attacker manipulates thousands of devices to send ICMP request to the target, the bandwidth of the target will be exhausted. However, compared with the Volume-Based attacks, the power of ICMP flood only depends on how many bots do you have. There is no Amplification. Now, for preventing "ping of death", a server is usually set to block all the ICMP requests. Therefore, this kind of attack is more common at the dawn of the Internet.

Preventative Measure

An efficient way to prevent ICMP flood attack is to set the kernel configuration -"net.ipv4.icmp_echo_ignore_all=1" or use Iptables to drop all the ICMP requests.

5. Conclusion

This report gave an overview of the DDoS, including a rough category, a brief definition of each category and one or more significant incident in the real world to illustrate what is DDos, how far its influence, how it works and the

possible solutions to protect the target server. Actually, DDoS attacks happened all the time, the reason why people do not feel it is that almost all the service has set lots of protection to mitigate every kind of attack. When people can feel it, that will be a really worse condition. Digital Attack Map shows a live DDoS attack globally by a visualized and interactive way(Arbor Networks, n.d.). From Digital Attack Map, it reveals that most of the DDoS attack is Volume-Based Attacks. That is reasonable because this is the most efficient way to manipulate a small number of bots to cause exponential damage.

According to the "Cisco Annual Internet Report (2018–2023) White Paper", there will be 29.3 billion networked devices by 2023, up from 18.4 billion in 2018 (Cisco, 2020). Additionally, with the development of 5G technology, the performance of the network will improve simultaneously. However, the power of the DDoS will growth in the meantime. With more IoT and intelligent wearable devices join people's lives, this kind of devices all could be the potential bots (Hallman et al., 2017). Therefore, IoT manufactures are supposed to pay more attention to the security of their products in the future.

In conclusion, nothing can be perfect, so as the Internet. There are always inevitable bugs in software or service. Therefore, there is no easy way to ensure security all the time. To improve the cybersecurity, device manufactures, software companies and customs should work together to keep a healthy and safe environment on the Internet. Figure 12 illustrates more details.

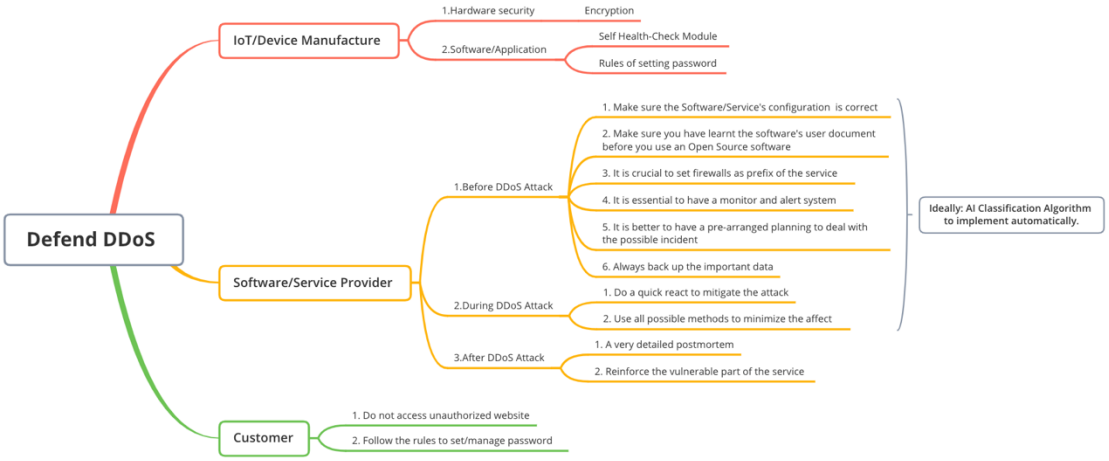

Figure 12: Defend DDoS

References

Arbor Networks (n.d.). **Digital Attack Map.** [online] www.digitalattackmap.com. Available at: https://www.digitalattackmap.com/about/ [Accessed 28 Oct. 2020].

Cisco. (2020). **Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper.** [online] Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html [Accessed 20 Oct. 2020].

Cloudflare. (2019). **Cloudflare.** [online] Available at: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/ [Accessed 23 Oct. 2020].

Corero (2017). **Financial Impact of Mirai DDoS Attack on Dyn Revealed in New Data.** [online] Corero. Available at: https://www.corero.com/blog/financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data/ [Accessed 27 Oct. 2020].

enisa (2016). **DDoS on DNS root servers.** [online] Europa.eu. Available at: https://www.enisa.europa.eu/publications/info-notes/ddos-on-dns-root-servers [Accessed 27 Oct. 2020].

Esecurityplanet.com. (2017). **Types of DDoS Attacks.** [online] Available at: https://www.esecurityplanet.com/network-security/types-of-ddos-attacks.html [Accessed 22 Oct. 2020].

Etherington, D. and Conger, K. (2016). **Large DDoS attacks cause outages**

at Twitter, Spotify, and other sites. [online] TechCrunch. Available at: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/ [Accessed 26 Oct. 2020].

Hallman, R., Bryan, J., Palavicini, G., Divita, J. and Romero-Mariona, J. (2017). IoDDoS — The Internet of Distributed Denial of Sevice Attacks - A Case Study of the Mirai Malware and IoT-Based Botnets. **Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security.**

Helmke, M. (2019). **After the Retrospective: Dyn DDoS.** [online] www.gremlin.com. Available at: https://www.gremlin.com/blog/after-the-retrospective-dyn-ddos/ [Accessed 27 Oct. 2020].

Henthorn-Iwane, A. (2019). **Analyzing the Wikipedia DDoS Attack.** [online] Internet and Cloud Intelligence Blog | ThousandEyes. Available at: https://blog.thousandeyes.com/analyzing-the-wikipedia-ddos-attack/ [Accessed 27 Oct. 2020].

Hoque, N., Bhattacharyya, D.K. and Kalita, J.K. (2015). Botnet in DDoS Attacks: Trends and Challenges. **IEEE Communications Surveys & Tutorials, 17(4), pp.2242–2270.**

Kesavan, A. (2016). **Three Common Types of DDoS Attacks?** [online] Internet and Cloud Intelligence Blog | ThousandEyes. Available at: https://blog.thousandeyes.com/three-types-ddos-attacks/.

Kottler, S. (2018). **February 28th DDoS Incident Report.** [online] The GitHub Blog. Available at: https://github.blog/2018-03-01-ddos-incident-report/ [Accessed 21 Oct. 2020].

Lawton, G. (2007). Stronger Domain Name System Thwarts Root-Server Attacks. **Computer**, 40(5), pp.14–17.

Majkowski, M. (2018). **Memcrashed - Major amplification attacks from UDP port 11211.** The Cloudflare Blog. Available at: https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/ [Accessed 26 Oct. 2020].

memcached.org. (n.d.). **memcached - a distributed memory object caching system.** [online] Available at: https://memcached.org/ [Accessed 27 Oct. 2020].

NETBLOCKS (2019). **Wikipedia disrupted globally in apparent denial of service attack.** [online] NetBlocks. Available at: https://netblocks.org/reports/wikipedia-disrupted-globally-in-apparent-denial-of-service-attack-RyjoqY8g [Accessed 27 Oct. 2020].

NETSCOUT (n.d.). **What is an HTTP Flooding Attack?** [online] NETSCOUT. Available at: https://www.netscout.com/what-is-ddos/http-flood-attacks [Accessed 27 Oct. 2020].

Penta Security (2017). **Types of DDoS Attacks: Explanation for the Non-Tech-Savvy.** [online] Penta Security Systems Inc. Available at: https://www.pentasecurity.com/blog/ddos-attacks-types-explanation/ [Accessed 26 Oct. 2020].

Red Button (2018). **Dyn DDoS Attack | Red Button.** [online] Red Button. Available at: https://www.red-button.net/blog/dyn-dyndns-ddos-attack/ [Accessed 27 Oct. 2020].

Schneier, B. (2016). **Lessons From the Dyn DDoS Attack.** [online] Security Intelligence. Available at: https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/ [Accessed 27 Oct. 2020].

Sreekanth, A., Sri, P. and Vartiainen, T. (n.d.). **Dyn DDOS Cyberattack -a case study.** [online] Available at: https://mycourses.aalto.fi/pluginfile.php/457047/mod_folder/content/0/Cyber%20Ghosts.pdf?forcedownload=1 [Accessed 22 Oct. 2020].

Varghese, S. (2017). **iTWire - DDoS attack on Dyn costly for company: claim.** [online] www.itwire.com. Available at: https://www.itwire.com/security/76717-ddos-attack-on-dyn-costly-for-company-claim.html [Accessed 27 Oct. 2020].

Vixie, P., Sneeringer, G. and Schleifer, M. (2011**). 21 Oct 2002 Root Server Denial of Service Attack - Report | Internet Systems Consortium.** [online] web.archive.org. Available at: https://web.archive.org/web/20110302164416/http://www.isc.org/f-root-denial-of-service-21-oct-2002 [Accessed 26 Oct. 2020].

Wikimedia Foundation (2019). **Malicious attack on Wikipedia—What we know, and what we're doing.** [online] Wikimedia Foundation. Available at: https://wikimediafoundation.org/news/2019/09/07/malicious-attack-on-wikipedia-what-we-know-and-what-were-doing/ [Accessed 27 Oct. 2020].