Wikipedia DDoS Attack

Wikipedia is the world's largest publicly accessible and editable repository of information. Currently, there are over 5 million articles hosted on Wikipedia in over 300 languages. All of this information is hosted across 6 datacenters; four of these are in the USA, one in Amsterdam, and one in Singapore. Due to the rapidly changing and highly specific demands of Wikipedia, third party services are not used to host Wikipedia's data. The primary data server used to store and serve data is hosted in Ashburn, Virginia; the remaining 5 servers act as Caching servers to deliver content to other regions quickly and accurately. The hardware that Wikipedia uses in their data centers is unknown however all of their services run on Debian/GNU Linux.

On September 6th, 2019, Wikipedia.org experienced outages starting shortly before 7 PM BST. The outages occurred in Europe and the Middle East which would imply that the Amsterdam caching server was the root server that took the brunt of the attack. This attack sent an influx of traffic that took the average page response time from 900ms to almost 3 seconds. Nothing is known about the purpose of this attack or who is behind the attack, however one valid reason was that this attack is a proof of concept for someone attempting to sell a botnet or a DDoS tool.

A Distributed Denial-of-Service attack is a brute force attack that has the intended goal of ensuring that the server under attack is too busy to fulfill any real requests made to it. A denial-of-service attack is a cyber-attack which aims to make a machine or service unavailable to its intended users by disrupting a machine's connection to the internet. This is done by an attacker sending a huge amount of requests to a server with the intent of overwhelming it. By distributing this attack across hundreds and thousands of machines, a denial-of-service attack can be used to take down larger and more resilient web services and multiple servers.

Multiple different types of denial-of-service attacks exist however the most popular of these are Smurf, Fraggle, and ACK flooding. Smurf attacks send a high volume of Internet Control Message Protocol (ICMP) which are originated by "Pinging" a server which is a request to check if a server is up. If the amount of Pings sent to a server is very large, often the server will not be able to keep up and will be too busy with attempting to reply to the "Ping" requests. Similarly, a Fraggle attack uses a huge amount of UCP requests to port 7 and port 19 since these protocols also involve a response from the destination server they behave very similar to the smurf attack method. Finally, the SYN method sends a large volume of the first part of the TCP three-way handshake, however when the destination server sends a SYN-ACK, the final part of the handshake isn't sent by the client. This works because a server will wait for a final ACK which binds the server's resources to the attack and prevents any future connections from any legitimate clients.

DDoS attacks are constantly evolving and becoming much stronger than they have been in the past. This is partly due to the increasing power of computers, however, most likely the root cause of the growth of the power of DDoS attacks is due to botnets and the increase in vulnerable IoT devices which can be used as a member of a botnet.

A few methods exist to prevent Denial of Service attacks; however, due to the wide range of possible methods that can be used to launch a Denial of Service attack, these methods will not have a perfect success rate. The most commonly used method of preventing Denial of Service attacks is rate-limiting at the network switch level. This is when a website or service only allows a set amount of requests per IP address by using a switch, however, this can be bypassed by using a botnet that is distributed among thousands of different hosts with unique IPs. Dedicated hardware can also prevent DDoS attacks by analysing packets and determines if the packet in question is dangerous and should be ignored. Wikipedia uses switches with rate limiters and application-level load balancers to attempt to deal with large volumes of traffic or DDoS attacks but due to the huge scale of this attack, these methods were not enough to protect against the website going down. As it is currently unknown which method was used to attack the servers, it is hard to say what method of prevention could have been used to keep the server from going down.

L. Deneen, “Bandwidth Management Tools, Strategies, and Issues.,” *University of Minnesota Duluth*, 2002.

Grafana. [Online]. Available: https://grafana.wikimedia.org/d/000000050/performance-metrics?refresh=5m&orgId=1&from=now-7d&to=now.

PING (ICMP) Flood DDoS Attack. [Online]. Available: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/.

D. K. Bhattacharyya and J. K. Kalita, *DDoS attacks: evolution, detection, prevention, reaction, and tolerance*. Boca Raton: Chapman & Hall/CRC, 2015.