IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 11, November 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 11, November 2020 ||

Study on Distributed Denial-of-Service (DDoS) Attacks, Their Causes, Effects & Preventions.

Ankita Tiwari, Varun Herlekar

Department of Computer Engineering, Government College of Engineering, Yavatmal, Maharashtra, India

ABSTRACT:A distributed denial-of-service (DDoS) attack is a venomous attempt to unsettle the normal traffic of a targeted server or website by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. The primary way a DDoS is accomplished is through a network of remotely controlled, hacked computers, or bots. These are often referred to as "zombie computers." They form what is known as a "botnet" or network of bots. This paper summarizes the complete idea of DDoS, its Causes, Effects, and all preventive measures we should take to prevent an attack.

KEYWORDS: DDoS Attack, HTTP Flood, Layer Attack, CLDAP, DNS, IP, Amplification, UDP, ICMP, Distributed Denial of Service attack.

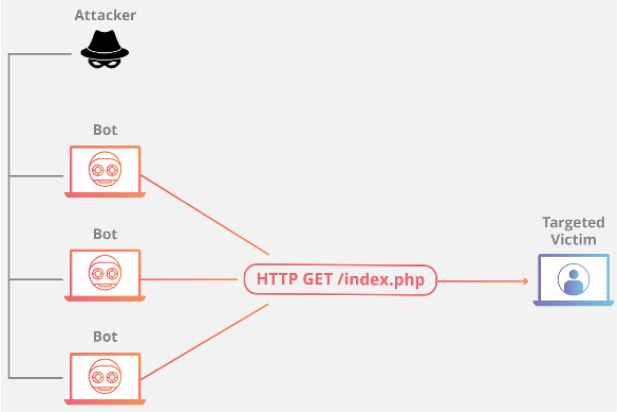
I. INTRODUCTION

Distributed Denial of services is a cyber-attack in which the culprit seeks to make a server, computer, website, or any other resources unavailable by flooding or crashing the website with too much traffic that causes the denial of services for users of targeted resources. A DDoS attack is one of the most powerful weapons on the internet. The flood of incoming messages, connection requests, or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems. This effectively makes it impossible to stop the attack simply by blocking a single source. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail, and activism can motivate these attacks. In certain situations, often ones related to poor coding, missing patches, or generally unstable systems, even legitimate requests to target systems can result in DDoS-like results.

II. TYPES OF DDOS ATTACKS

1.Application layer attack

These attacks are performed to exhaust the target's resources to create a denial-of-service. These attacks target the layer where web pages are generated on the server and delivered in response to HTTP requests. It can be expensive for the target server to respond to, as the server often loads multiple files and runs database queries to create a web page.

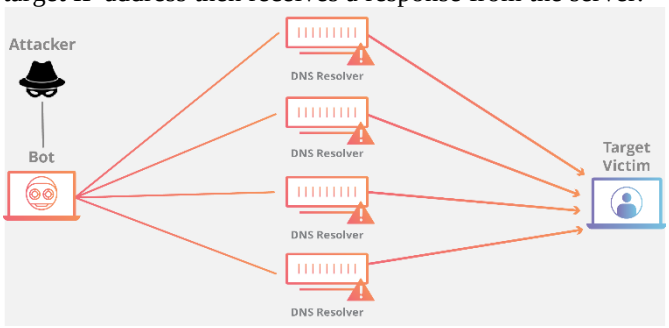


| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 11, November 2020 ||

2.HTTP Flood
This attack is similar to pressing refresh in a web browser over and over on many different computers at once, large numbers of HTTP requests flood the server, resulting in denial-of-service. There are 2 types of HTTP Flood Attack, Simpler implementations may access one URL with the same range of attacking IP addresses, referrers, and user agents. Complex versions may use a large number of attacking IP addresses, and target random URLs using random referrers and user agents.

3.DNS Amplification
This category of attacks attempts to create overcrowding by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet. With very little effort, a long response is generated and sent to the victim. By making a request to an open DNS server with a spoofed IP address (the IP address of the victim), the target IP address then receives a response from the server.



4.UDP Flood
A UDP flood, by definition, is any DDoS attack that floods a target with User Datagram Protocol (UDP) packets. The goal of the attack is to flood random ports on a remote host. This causes the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP 'Destination Unreachable' packet. This process saps host resources, which can ultimately lead to inaccessibility.

5.ICMP (Ping) Flood
Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting in a significant overall system slowdown.

III. DDOS PROCEDURE

A Number of tools exist that can be adapted to launch DDoS attacks, or are explicitly designed for that purpose. The tools with the stated purpose of helping security researchers and network engineers perform stress tests against their own networks, but which can also be used to perform genuine attacks. Some are specialized and only focus on a particular layer of the OSI model, while others are designed to allow for multiple attack vectors.
Here are some categories of tools used:

•Low and slow attack tools:
Designed to send small amounts of data across multiple connections in order to keep ports on a targeted server open as long as possible, these tools continue to take up the server's resources until it is unable to maintain additional connections.

•Application layer (L7) attack tools:
These tools target layer 7 of the OSI model, where Internet-based requests such as HTTP occur. Using an HTTP flood attack to overwhelm a target with HTTP GET and POST requests, a malicious actor can launch attack traffic that is difficult to distinguish from normal requests made by actual visitors.

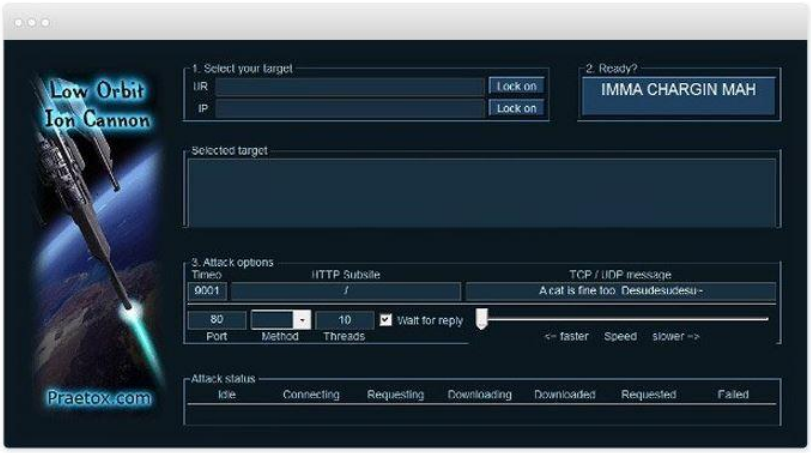
| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 11, November 2020 ||

•Protocol and transport layer (L3/L4) attack tools:
These tools utilize protocols like UDP to send large volumes of traffic to a targeted server, such as during a UDP flood.

Some commonly used tools:

- Low Orbit Ion Cannon (LOIC)
- High Orbit Ion Cannon (HOIC)
- Slowloris
- R. U. D. Y (R-U-Dead-Yet)



The LOIC application interface.

IV. EFFECTS & PREVENTIONS

DDoS attack might have many effects; it totally depends on the type of attack it is. Some of those has been discussed below:

- Website Lay-off: Effect of website lay-off is that your website is overwhelmed and becomes unavailable. This means if you have any of your business will not be available after website lay-off. It also impacts on your reputation as a website owner. And if you don't fix the site quickly, it can affect your SEO as if Google crawls your site and finds it out of action, you will lose rank.

- Website Vulnerability: Website Vulnerability is a type of weakness or misconfiguration in a web application code. It allows an attacker to gain some level of control on a website and possibly the hosting server. Some examples of website vulnerability are SQL Injection Vulnerabilities (SQLi), Cross-Site Scripting (XSS), File Inclusion (LFI/RFI), Cross-Site Request Forgery (CSRF) and Command Injection.

- Hosting and Server Issue: Many hosting companies these days offer DDoS protected servers with the option to purchase the level of protection you need. Ultimately, this type of protection is your best line of defence against a DDoS attack on your dedicated server

- Loss of Money and Time: Repairing a website that has been subject to a DDoS attack takes time. It can also take money. If you don't know what's happened to your site and haven't prepared for the possibility of an attack, you could end up having to rebuild your site from scratch (I've seen sites where this has happened).

Here are some ways, using which DDoS attacks can be prevented:

I. Purchase More Bandwidth: The first step you have to take, for the prevention of a DDoS attack and make your infrastructure DDoS resistant, is to make sure that you have sufficient bandwidth to handle any spikes in traffic that could be caused due to malicious activity.

II. Securing Network Infrastructure: There are several large providers that specialize in scaling infrastructure to respond to attacks. Mitigating network security threats can only be achieved with multi-level protection

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 11, November 2020 ||

strategies in place. This includes advanced intrusion prevention and threat management systems, which combine firewalls, VPN, anti-spam, content filtering, load balancing, and other layers of DDoS defence techniques.

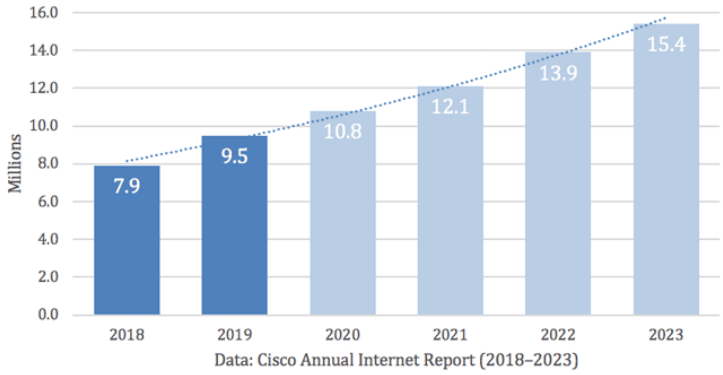
III. Transparent Mitigation: Hackers could be launching the Dodos to make your users lose access to your site. When your site is under attack, you must use a mitigation technology to enable people to continue using it without making it unavailable and without making them see splash screens and outdated cached content.

IV. Deploy Anti Dodos software and hardware module: Along with having your server protected by network firewalls and other specialized web application firewalls, you must use load balancers. You can also add software modules to another web server software for DDoS prevention.

And many precautions can be taken to stay protected from DDoS attacks.

V. CASE STUDIES

The first known Distributed Denial of Service attack occurred in 1996 when Panix, now one of the oldest internet service providers, was knocked offline for several days by a SYN flood, a technique that has become a classic DDoS attack. Over the next few years DDoS attacks became common and Cisco predicts that the total number of DDoS attacks will double from the 7.9 million seen in 2018 to something over 15 million by 2023.



A. Google Attack – 2017

Google's Threat Analysis Group (TAG) posted a blog update discussing how the threats and threat actors are changing their tactics due to the 2020 U.S. election. Google Security Reliability Engineering team measured a record-breaking UDP amplification attack sourced out of several Chinese ISPs. Launched from three Chinese ISPs, the attack on thousands of Google's IP addresses lasted for six months and peaked at 2.5 Tbps. The attacker used several networks to spoof, exposed CLDAP, DNS, and SMTP servers, which would then send large responses to google.

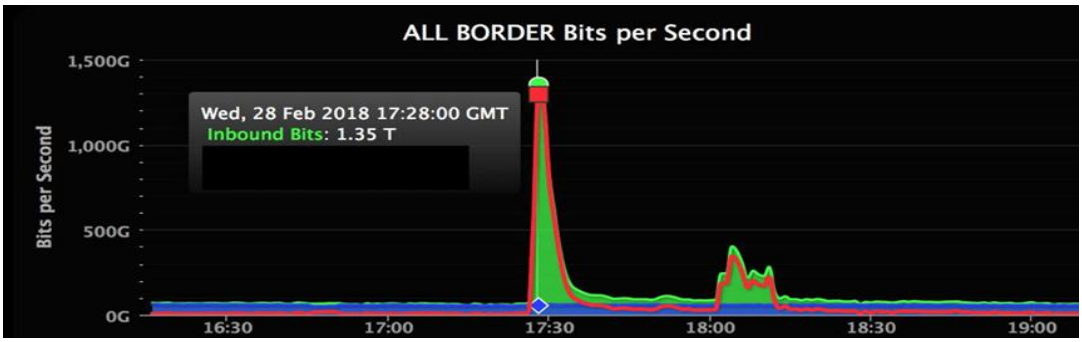
B. Github Attack – 2018

GitHub, a platform for software developers was hit with a DDoS attack that clocked in at 1.35 terabits per second and lasted for roughly 20 minutes. The traffic was traced back to over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints.

The following chart shows just how much of a difference there was between normal traffic levels and those of the attack:

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 11, November 2020 ||



C. AWS Attack – 2020

Amazon Web Services, was hit by a gigantic DDoS attack in February 2020. This was the most extreme recent DDoS attack ever and it targeted an unidentified AWS customer using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) Reflection. This technique relies on vulnerable third-party CLDAP servers and amplifies the amount of data sent to the victim's IP address by 56 to 70 times. The attack lasted for three days and peaked at an astounding 2.3 terabytes per second. While the disruption caused by the AWS DDoS Attack was far less severe than it could have been, the sheer scale of the attack.

VI. CONCLUSION

DDoS attacks have been proven to be an effective way to unsettle web services. Despite advances in mitigation and prevention techniques, DDoS attacks will remain a constant threat to organizations large and small. A good place to start is a mindset of privacy and security, starting with encrypted email and following good online security/privacy practices. This diminishes the chance your devices turn into a bot that contribute to DDOS attacks. In this paper we have gone through the DDoS overview with its types, how attack is done, it's effects and preventions and we had also gone through case study. We have highlighted the DDoS details part and visualize the security aspects and complete case study.

REFRENCES

1. https://thecyberagents.com
2. https://anticybercrime.org
3. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
4. https://thehackernews.com/2018/03/biggest-ddos-attack-github.html
5. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
6. https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details