International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET207450

A Study of DDOS (Distributed-denial-of- service) Attacks and Its Preventions

Bhawna Tripathi, Dr. Devesh Katiyar, Gaurav Goel
Dr. Shakuntala Mishra National Rehabilitation University, Mohaan Road, Lucknow, Uttar Pradesh, India

Article Info
Volume 7 Issue 4
Page Number : 176-181
Publication Issue :
July-August-2020

Article History
Accepted : 01 Aug 2020
Published : 05 Aug 2020

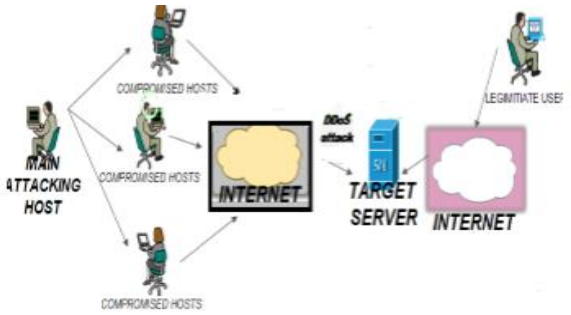
ABSTRACT

The data security is one of the most important themes in the information World. Cloud Computing is a grooving technology and implemented by many companies, but there are many issues and one of them is DDOS. .The DDOS attack is one of the most Threatening attacks in today's world. This paper introduces about the major problem occur in the security which is known as DDOS attacks The study of this research is to find out the various techniques to prevent these attacks along with their modification techniques and to find out any possible solution.

Keywords : Information, Ddos , Cloud Computing, Techniques, Preventions

I. INTRODUCTION

DDOS stand for Distributed Denial of service. It is a form of Cyber Attack , Distributed denial-of-service is one kind of the most highlighted and most important attacks of today's Cyber world. a distributed denial of service (DDOS) attack is a cruel challenge to make an online service unavailable to users , usually by temporarily interfering or suspending the service of its hosting service, that can be targets critical system to Distrupt network package or connectivity that cause a denial of service for users of the targeted resources. The Architecture consists of main attacker's host and three co-operated hosts to launch the coordinate attack through the internet by sending a large number of requests through the network. The network of the target server gets busy and then it will not respond to its legitimate users and will not able to provide services to the other actual hosts.



Architecture of DDOS attacks.

The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of -service attack.

Cloud Computing has become one of the most challenging service of Internet, it has gaining Incredible fame for past few years , but it is under the severe threats is Distributed denial of Service(DDOS) .It introduces an huge threat to current Internet community . Attack uses multiple machines operating together to attack a network or site, and these attacks cause so much extra network

traffic that it is difficult for legitimate traffic to reach your site while blocking the forged attacking packets. Attacker may use your computer to attack another computer, by taking advantage of security exposures or weaknesses, an attacker could take control of your computer.

He or she could then force your computer to send huge amounts of data to a web site or send spam to particular email addresses

Difference between (DOS) and DDOS Attack

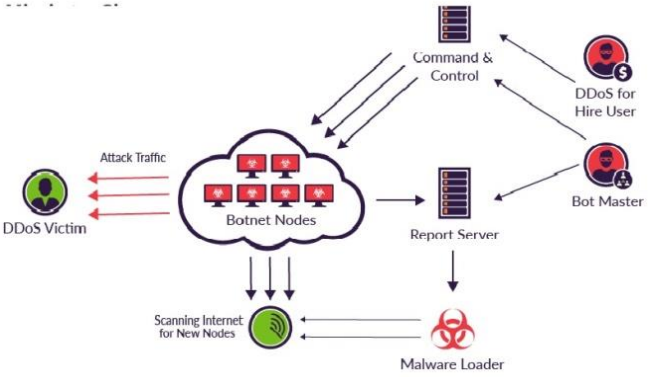
A DOS attack is parallel to a DDOS attack, except they take very different forms. DOS attacks exist in one of two broad classes, Denial-of-Service (DOS) and Distributed Denial-of-Service (DDOS). DOS attacks are executed by a single attacker and their goal is to make an application, service or machine inaccessible. This is done by either flooding it with more requests than it can handle or otherwise consuming resources or processing in such a way that authentic requests cannot be handled. Within DOS, there are two primary categories:

1. Application attacks - Also, sometimes called 'Layer 7 attacks', they involve putting operation strain on the software serving the requests in such a way that it cannot handle additional requests.
2. Network attacks - These attacks generally aim to saturate a bandwidth by overwhelming a server using brute force or by flooding with malformed requests. These types of attacks are rare nowadays due to the basic firewall configuration and the ability of servers to handle traffic from a single malicious client.

DDOS attacks are denial-of-service attacks in which more than one attacking machines participate. DDOS attacks can also be perpetrated by large groups of active users using simple tools like in the DDOS attack by the Anonymous hacker group. The hacker group had used a free internet tool called Low Orbit Ion Canon (LOIC) to conduct online attacks against computer systems.

BOTNETS

A botnet refers to a group of computers which have been infected by malware and have come under the control of a malicious actor. The term botnet is a portmanteau from the words robot and network and each infected device is called a bot. Botnets can be designed to accomplish illegal or malicious tasks including sending spam, stealing data, fraudulently clicking on ads or distributed denial-of-service (DDOS) attacks.



While some malware, such, will have a direct impact on the owner of the device, DDOS botnet malware can have different levels of visibility; some malware is designed to take total control of a device, while other malware runs silently as a background process while waiting silently for instructions from the attacker or "bot herder."

Self-propagating botnets recruit additional bots through a variety of different channels. Pathways for infection include the exploitation of website vulnerabilities, Trojan horse malware, and cracking weak authentication to gain remote access. Once access has been obtained, all of these methods for infection result in the installation of malware on the target device, allowing remote control by the operator of the botnet. Once a device is infected, it may attempt to self-propagate the botnet malware by recruiting other hardware devices in the surrounding network.

While it's infeasible to pinpoint the exact numbers of bots in a particular botnet, estimations for total number of bots in a sophisticated botnet have ranged in size from a few thousand to greater than a million.

II. TYPES OF ATTACK

DDOS attack can be divided into three parts-

1) Volume based attack-

The most common DDOS attack overwhelms a machine's network bandwidth by flooding it with false data requests on every open port the device has available. Because the bot floods ports with data, the machine continually has to deal with checking the malicious data requests and has no room to accept legitimate traffic. UDP floods and ICMP floods comprise the two primary forms of volumetric attacks.

UDP stands for User Datagram Protocol and refers to the simple transmission of data without checking its integrity. The UDP format lends itself well to fast data transmission, which unfortunately makes it a prime tool for attackers.

ICMP stands for Internet Control Message Protocol, referring to network devices that communicate with one another. An attack focused on ICMP relies on attacking nodes sending false error requests to the target. The target has to deal with these requests and cannot respond to real ones, similar to how a UDP attack works.

2) Protocol Attacks –

A protocol attack focuses on destructive connection tables in network areas that deal directly with verifying connections. By sending successively slow pings, deliberately malformed pings, and partial packets, the attacking computer can cause memory buffers in the target to overload and potentially crash the system. A protocol attack can also target firewalls. This is why a firewall alone will not stop denial of service attacks.

One of the most common protocol attacks is the SYN flood, which makes use of the three-way handshake process for establishing a TCP/IP connection. Typically, the client sends a SYN (synchronize) packet, receives a SYN-ACK (synchronize-acknowledge), and sends an ACK in return before establishing a connection. During an attack, the client only sends SYN packets, causing the server to send a SYN-ACK and wait for the final phase that never occurs. This, in turn, ties up network resources.

Often, would-be hackers combine these three types of approaches to attack a target on multiple fronts, completely overwhelming its defences until stronger and more thorough count measures can be deployed.

3) Application Layer Attacks

The application layer is the topmost layer of the OSI network model and the one closest to the user's interaction with the system. Attacks that make use of the application layer focus primarily on direct Web traffic. Potential avenues include HTTP, HTTPS, DNS, or SMTP .Application-layer attacks are not as easy to catch because they typically make use of a smaller number of machines, sometimes even a single one. Therefore, the server can be tricked into treating the attack as nothing more than a higher volume of legitimate traffic.

Preventions and Defence against DDOS Attacks-

These attacks target data, applications, and infrastructure simultaneously to increase the chances of success. To fight them, you need a battle plan, as well as reliable DDOS prevention and mitigation solutions. You need an integrated security strategy that protects all infrastructure levels.

1. Develop a Denial of Service Response Plan.

Develop a DDOS prevention plan based on a thorough security assessment. Unlike smaller companies, larger businesses may require complex infrastructure and involving multiple teams in DDOS planning. When DDOS hits, there is no time to think about the best steps to take. They need to be defined in advance to enable prompt reactions and avoid any impacts. Developing an incident response plan is the critical first step toward comprehensive Defence strategy. Depending on the infrastructure, a DDOS response plan can get quite exhaustive. The first step you take when a malicious attack happens can define how it will end. Make sure your data center is prepared, and your team is aware of their responsibilities. That way, you can minimize the impact on your business and save yourself months of recovery.

The key elements remain the same for any company, and they include:

- **Systems checklist.** Develop a full list of assets you should implement to ensure advanced threat identification, assessment, and filtering tools, as well as security-enhanced hardware and software-level protection, is in place.
- **Form a response team**. Define responsibilities for key team members to ensure organized reaction to the attack as it happens.
- **Define notification and escalation procedures**. Make sure your team members know exactly whom to contact in case of the attack.
- **Include the list of internal and external contacts** that should be informed about the attack. You should also develop communication strategies with your customers, cloud service provider, and any security vendors.

2. Secure Your Network Infrastructure.

Mitigating network security threats can only be achieved with multi-level protection strategies in place. This includes advance intrusion prevention and threat management systems, which combine firewalls, VPN, anti-spam, content filtering, load balancing, and other layers of DDOS defense techniques. Together they enable constant and consistent network protection to prevent a DDOS attack from happening. This includes everything from identifying possible traffic inconsistencies with the highest level of precision in blocking the attack.

Most of the standard network equipment comes with limited DDOS mitigation options, so you may want to outsource some of the additional services. With cloud-based solutions, you can access advanced mitigation and protection resources on a pay-per-use basis. This is an excellent option for small and medium-sized businesses that may want to keep their security budgets within projected limits. In addition to this, you should also make sure your systems are up-to-date. Out dated systems are usually the ones with most ambiguities . Denial of Service attackers find holes. By regularly patching your infrastructure and installing new software versions, you can close more doors to the attackers.

Given the complexity of DDOS attacks, there's hardly a way to defend against them without appropriate systems to identify anomalies in traffic and provide instant response. Backed by secure infrastructure and a battle-plan, such systems can minimize the threat. More than that, they can bring the needed peace of mind and confidence to everyone from a system admin to CEO.

3. Practice Basic Network Security

The most basic countermeasure to **preventing DDOS attacks** is to allow as little user error as possible. Engaging in strong security practices can keep business networks from being compromised. Secure

practices include complex passwords that change on a regular basis, anti-phishing methods, and secure firewalls that allow little outside traffic. These measures alone will not stop DDOS, but they serve as a critical security foundation.

4. Maintain Strong Network Architecture

Focusing on a secure network architecture is vital to security. Business should create redundant network resources; if one server is attacked, the others can handle the extra network traffic. When possible, servers should be located in different places geographically. Spread-out resources are more difficult for attackers to target.

5. Leverage the Cloud

Outsourcing **DDOS prevention** to cloud-based service providers offers several advantages. First, the cloud has far more bandwidth, and resources than a private network likely does. With the increased magnitude of DDOS attacks, relying solely on on-premises hardware is likely to fail.

Second, the nature of the cloud means it is a diffuse resource. Cloud-based apps can absorb harmful or malicious traffic before it ever reaches its intended destination. Third, cloud-based services are operated by software engineers whose job consists of monitoring the Web for the latest DDOS tactics. Deciding on the right environment for data and applications will differ between companies and industries. Hybrid environments can be convenient for achieving the right balance between security and flexibility, especially with vendors providing tailor-made solutions.

6. Understand the Warning Signs

Some symptoms of a DDOS attack include network slowdown, spotty connectivity on a company intranet, or intermittent website shutdowns. No network is perfect, but if a lack of performance seems to be prolonged or more severe than usual, the network likely is experiencing a DDOS and the company should take action.

7. Consider DDOS-as-a-Service

DDOS-as-a-Service provides improved flexibility for environments that combine in-house and third party resources, or cloud and dedicated server hosting.

At the same time, it ensures that all the security infrastructure components meet the highest security standards and compliance requirements. The key benefit of this model is the ability of tailor-made security architecture for the needs of a particular company, making the high-level DDOS protection available to businesses of any size.

Recent Attack

DDOS attacks are not only on the rise—they're also bigger and more devastating than ever before. the progression of the largest and most famous distributed denial of service attacks that have occurred -

2020 February — Amazon Web Services (AWS) reported that they observed and mitigated a 2.3 tbps UDP reflection vector DDOS attack. Not only is this the largest DDOS attack that AWS reports ever facing, but it's also thought to be the largest DDOS attack in history on record in terms of bit rate.

2019 April — Imperva reports one of their clients was able to thwart a DDOS attack that peaked at 580 million packets per second. To date, this is considered the largest DDOS attack by packet volume to date.

January — Another Imperva client sustained a 500 million packets per second DDOS attack.

1) **2018 March —** NETSCOUT reported that its global traffic and DDOS threat detection system confirmed a 1.7 Tbps memcached

reflection/amplification attack on an unnamed U.S.-based service provider.

February — The GitHub DDOS attack inundated the company with 1.35 Tbps of data (129.6 million PPS) — the largest DDOS attack on record as of that time — via memcaching. This means that the attackers spoofed GitHub's IP address to send small inquiries to several Memcached servers to trigger a major response in the form of a 50x data response.

2) **2017 October** — The Czech statistical office websites relating to the Czech Republic's parliamentary elections — volby.cz and volbyhned.cz — failed temporarily due to DDOS attacks during the vote count.

June — Throughout the second half of the year, video game software developer Square Enix's Final Fantasy XIV online role-playing game (RPG) sustained intermittent DDOS attacks via botnets. The attacks spanned the summer and another set of attacks occurred during the fall.

3) **2016 October** — The Dyn DDOS attack, which measured in at 1.2 Tbps and was considered the largest DDOS attack at the time, brought down much of the internet across the U.S. and Europe. Using the Mirai botnet, the attack targeted dyn , a company that controls much of the domain name system (DNS) infrastructure of the internet.

September — French web host OVH experienced a DDOS attack measuring in at nearly 1 Tbps. The attackers used a botnet of hacked IoT devices (CCTV cameras and personal video recorders) to launch their attack.

III. CONCLUSION AND FUTURE WORK

DDOS attack has now become the number one threat to Internet in present scenarios. There is millions of dollars loss to the companies suffering from these attacks. The major challenge is to differentiate between the legitimate traffic and attack traffic. Since most of the attackers uses the legitimate attack models differentiating between the two becomes a trivial task. We know there is no one to govern over the Internet. The security of Internet is highly dependent on others. Internet needs to be more secure and Users needs to be more aware about Internet security So to deploy a defense mechanism only at the victim's side alone is not going to solve this problem. We need to deploy defense techniques at every level, whether its edge router, core routers, ISP levels, etc. Moreover our effort should be more on dealing with these attacks before the actual damage has happened.

IV. REFERENCES

[1]. David K. Y. Yau, Member, IEEE and John C. S. (2005) 'Defending Against Distributed Denial-of-Service Attacks With Max-Min Fair Server-Centric Router Throttles'.

[2]. Tasnuva Mahjabin1, Yang Xiao1, Guang Sun2 and Wangdong Jiang2 'A survey of distributed denial-of-service attack, prevention, and mitigation techniques

[3]. https://www.imperva.com/learn/application-security/ddos-attacks/

[4]. https://blog.eccouncil.org/types-of-ddos-attacks-and-their-prevention-and-mitigation-strategy/

[5]. https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-attack/

[6]. https://www.thesslstore.com/blog/largest-ddos-attack-in-history

Cite this article as :

Bhawna Tripathi, Dr. Devesh Katiyar, Gaurav Goel, "A Study of DDOS (Distributed-denial-of- service) Attacks and Its Preventions", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 4, pp. 176-181, July-August 2020. Available at doi : https://doi.org/10.32628/IJSRSET207450
Journal URL : http://ijsrset.com/IJSRSET207450