RESEARCH ARTICLE OPEN ACCESS

A Study of Distributed Denial of service Flooding Attacks by Preventive & Defense mechanisms

S.Srileka*, G.Sophia Reena**
**(Department of Computer Science, PSGR Krishnammal college for women, Coimbatore*
Email: srileka206@gmail.com)
*** (Department of Information Technology, PSGR Krishnammal college for women, Coimbatore*
Email: sophiareena@psgrkc.ac.in)

ABSTRACT
Distributed denial-of-service attack, or DDoS attack, is an attempt to overwhelm a website or online service with traffic from multiple sources in order to render it unavailable to users. DDoS attacks are one of the biggest concerns for security professionals. DDoS flooding attacks attempts to disrupt legitimate users access to services. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies (i.e., Botnets). This paper is about the overview of the DDOS attack, the various types of these attacks, the Preventive measures and the Defense mechanisms for these attacks. The Preventive measure is about the general mechanisms to be done to prevent the entry of DDos attack. The Defense mechanism defines the techniques to protect the network and server.
Keywords: DDos Attack, DDos Attack types, Defense Mechanisms, Prevention

---

Date of Submission: 26-10-2017 Date of acceptance: 07-11-2017

I. INTRODUCTION

A DDoS attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet. Unlike a Denial of Service (DoS) attack, in which one computer and one internet connection is used to flood targeted resource with packets, a DDoS attack uses many computers and many Internet connections, often distributed globally in what is referred to as a botnet. Many DDoS attacks succeed not due to the skill or resources at the command of the attackers, but because of lack of preparation on the defender's side. Security managers, adept at handling threats like intrusion, web application exploitations, and worms.

In the fig 1 the process is shown in which the attackers attack a server by sending malicious traffic of data requests to a targeted server and makes the server to overload with traffic and thus it makes the resources and information unavailable to the legitimate users.

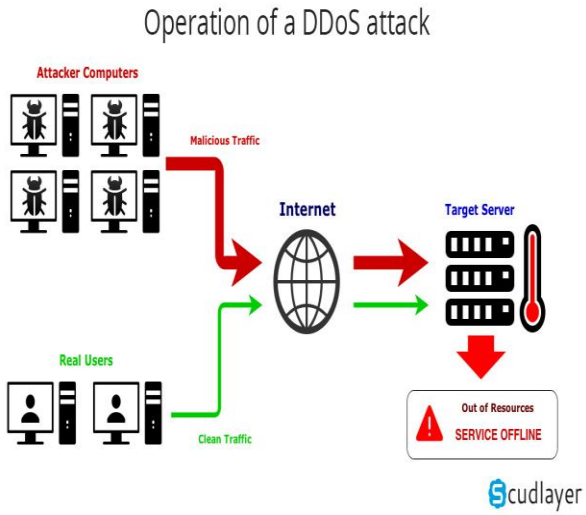

***Fig 1** Distributed denial of service attack process to disrupt services*

Today DDOS attack has become a major threat for network security all over the world. They can easily be launched by any people with the basic knowledge of the network security. They are most cheaper and efficient method for network attacking which can shutdown the company network by cram-full as of with requests and thus affects network availability. A DDoS attack is carried out in following phases**,** the attacker first recruits multiple agent machines. This process is usually performed automatically through scanning of remote machines,

looking for security holes that will enable subversion. The discovered vulnerability is then exploited to break into recruited machines and infect them with the attack code. The exploit/infect phase is frequently automated, and the infected machines can be used for further recruitment of new agents. Another recruit/exploit/infect strategy consists of distributing attack software under disguise of a useful application (these software copies are called Trojans). This distribution can be performed, for instance, by sending E-mail messages with infected attachments. Subverted agent machines are used to send the attack packets. Attackers often hide the identity of subverted machines during the attack through spoofing of the source address field in attack packets.

II. DDOS ATTACKS TYPES

The DDos attack is differentiated by various types by the ways in which the attacks are implemented in a particular network or a website or a server etc. The various types of DDos attacks are defined as follows,

Flooding or Volumetric Attack Flooding attack as the name implies, sends a large amount of traffic to a network to make the network to overflow with the traffic. This has the capability of crashing the network so that the legitimate users cannot access their network

User Datagram Protocol (UDP) attacks The UDP is an attack where an attacker sends a large number of UDP packets to random ports on a remote host. UDP floods accounted for approximately 75 percent of DDoS attacks in the last quarter of 2015, according to the Versign DDoS Trends Report.

Protocol attacks (sometimes also called state-exhaustion attacks) The Protocol attacks target a weakness in how a protocol operates. The SYN flood is a Protocol attack which targets the three-way handshake mechanism in TCP.

Application Level Attacks Application level attacks target areas that have more vulnerability. Rather than attempt to overwhelm the entire server, an attacker will focus their attack on one – or a few – applications. Web-based email apps, WordPress, Joomla, and forum software are good examples of application specific targets.

Unintentional DDos Unintended distributed denial of service happens when a spike in web traffic causes a server not to be able to handle all of the incoming requests. The more traffic that occurs, the more resources are used. This causes pages to timeout when loading and eventually the server will fail to respond and go offline.

Multi-Vector Attacks Multi-vector attacks are the most complex forms of distributed denial of service (DDoS) attack. Instead of utilizing a single method, a combination of tools and strategies are used to overwhelm the target and take it offline. Often times, multi-vector attacks will target specific applications on the target server, as well as, flood the target with a large volume of malicious traffic. These types of DDoS attacks are the most difficult to mitigate because the attack come in different forms and targets different resources simultaneously.

Degradation of Service Attack The purpose of this attack is to slow server response times. A DDoS attacker seeks to take a website or server offline. That is not the case in a degradation of service attack. The goal here is to slow response time to a level that essentially makes the website unusable for most people. Zombie computers are leveraged to flood a target machine with malicious traffic that will cause performance and page-loading issues. These types of attacks are difficult to detect because the goal is not to take the website offline, but to degrade performance. They are often confused with simply an increase in website traffic.

Slowloris Slowloris is DDoS attack software that enables a single computer to take down a web server. Due the simple yet elegant nature of this attack, it requires minimal bandwidth to implement and affects the target server's web server only, with almost no side effects on other services and ports. Over the years, Slowloris has been credited with a number of high-profile server takedowns

Diversion or Ransom Attack In this attack vector the attacker commences a DDoS act against victim server to distract the security team and incident responders while the attacker uses different methods to penetrate the network. There are two popular variants of this attack, One popular variant of this attack is to flood the victim's servers constantly until they pay a ransom (normally in untraceable bitcoin).A second variant of this attack is to divert the incident response team with a large-scale DDoS attack while implanting malware or Trojans on the network designed to steal data, information or PII, or exploit a known vulnerability.

III. DDOS PREVENTION MEASURES

If a website goes down due to an overload of website traffic, then it is probably a victim of the notorious distributed denial of service (DDoS) attack. DDoS attacks have become a nightmare for companies with an active online presence. The Prevention of DDos attack is the best way to stop DDos attack. Most of the prevention mechanisms aim to fix security vulnerabilities (e.g., insecure protocols, weak authentication schemes, and vulnerable computer systems) that can be exploited to launch DDoS attacks. There are some general prevention mechanisms that should be employed in servers, hosts, and intermediate networks. Some of these general prevention mechanisms are as follows:

i)Security mechanisms for system and Protocol security like preventing illegitimate access, removing bugs, updating installed protocols, installing software patches, removing unused software,
ii) Resource allocation & accounting Provides resources to counter DDoS attack and control users access based on their privileges and behaviors**.**
iii) Reconfiguration mechanisms alter the topology of either the victim network to add more resources to tolerate the DDoS attack (e.g., resource replication services)
iv)All of the end hosts are encouraged to install improved Intrusion Detection & Prevention Systems (IDPSs) to prevent them from being compromised by the adversaries.

Today, businesses need to tighten their seat belts to work and land safely in the highly advanced internet world. Some of the unique ways to prevent from the DDoS attacks are as follows,

Monitor Traffic Levels

A DDoS attack main aim is to bring a huge amount of traffic to a website, which spikes the traffic beyond the imagination. Therefore, it is best to analyze if there is an abnormal traffic increase in the website. If the number of visitors per minute increases to unusual number of visitors then it means there is a presence of DDos attack. Staying alert, monitoring the traffic and setting threshold limits when traffic goes beyond a certain level will help in DDoS protection.

Remote Black Holing

The UDP traffic can be filtered with the remote black holing which stop undesirable traffic to enter a protected network. These remote black holes are areas where the traffic is forwarded and then dropped. And, when an attack is detected it drops all the traffic based on the IP address and the destination.

Extra Bandwidth

It makes sense to have more bandwidth than it plausibly need because overprovisioning the bandwidth provides extra time to identify and deal with the attack. It also enables the server to accommodate unprecedented spikes in traffic and to some extent lowers the intensity of the attack.

Proxy Protection

Proxy protection provides an extra layer of DDoS protection for any website and keeps the website safe from complex cyber threats. The Proxy protection hides the real IP from hackers and sends proxy traffic through their mitigation network. Remote proxy protection increases the security and performance of HTTP applications.

Pay Attention to Connected Devices

Special attention must be given to the connected devices to prevent DDos attack. For stronger DDoS protection, the passwords should be changed on the devices regularly, switching off the devices when not in use and verifying every device before connecting is essential.

Intrusion Detection System and Intrusion Prevention System [1]

IDS also known as The Intrusion detection system is the piece of installed software or a physical appliance to monitor and detect unwanted traffic on a network or a device. The intrusion detection monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Some of intrusion detection methodologies are Signature based detection and Anomaly based detection, In signature based detection, observed events are compared against the pre-defined signatures in order to identify possible unwanted traffic. In Anomaly based detection the considered normal activity is compared with the observed events to identify significant deviations.

IPS also known as the Intrusion Prevention System is a device that is not only for detecting malicious activities, but the preventive actions are also taken to secure the host or the network. Firewalls and IPS are control devices. They sit in line between two networks and control the traffic going through them. The IPS accepts all the requests except those whose contents seem to be malicious and threatening to the system.

IV. DDOS DEFENSE MECHANISMS

The ultimate goal of any DDoS defense mechanism is to detect them as soon as possible and stop them as near as possible to their sources. The defense mechanism is based on these four categories Source based mechanism, Destination based mechanism, Network based mechanism and Hybrid based mechanism. It is shown in following fig 2

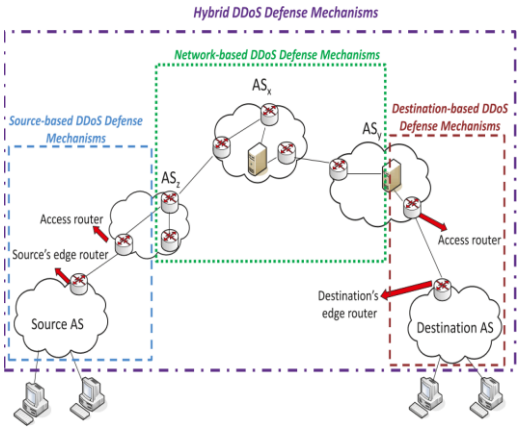

Fig 2 *Defense mechanisms*

4.1 Source Based defense mechanism

Source-based mechanisms are deployed near the sources of the attack to prevent the generation of DDos flooding attack from the network customers. These mechanisms can take place either at the edge routers of the source's local network or at the access routers of an Autonomous System (AS) that connects to the sources edge routers. Various source-based mechanisms have been designed to defend against DDoS flooding attacks at the source. The Various source-based mechanisms to defend against DDoS flooding attacks are Ingress/Egress6 filtering at the sources' edge routers, D-WARD, Multi-Level Tree for Online Packet Statistics (MULTOPS) [2], and Tabulated Online Packet Statistics (TOPS).

4.2 Destination-based mechanisms

In the destination-based defense mechanisms, the detection and mitigation is done at the victim which is also the attack destination. Some of the major destination-based DDoS defense mechanisms are IP Traceback mechanisms, Packet marking, Hop-count filtering, Management Information Base, Packet dropping based on the level of congestion mechanisms. These mechanisms can closely observe the victim, model its behavior and detect any anomalies.

4.3 Network-based mechanisms

These mechanisms are deployed inside networks and mainly on the routers of the ASs Detecting attack traffic and creating a proper response to stop it at intermediate networks is an ideal goal of this category of defense mechanisms. Some of the main network-based DDoS defense mechanisms are Route-based packet filtering [3] and Detecting & filtering malicious routers

4.4 Hybrid (Distributed) mechanisms

There is no strong cooperation among the deployment points in the source, destination and network based mechanisms. Furthermore, the source, destination and hybrid based mechanisms are centralized in which the detection and mitigation is mostly done centrally. As opposed to centralized defense mechanisms, hybrid defense mechanisms are deployed at multiple locations such as source, destination or intermediate networks and there is usually cooperation among the deployment points. Some of the hybrid DDoS defense mechanisms are Hybrid packet marking, throttling/filtering mechanisms, Aggregate-based Congestion Control (ACC)**[**4] and Track[5]

V. CONCLUSION

Recent industry study showed that some 75% of IT decision makers have suffered at least one DDoS in the past 12 months, and 31% reported service disruption as a result of these attacks. As more and more commercial and governmental organizations are discovering the hard way, DDoS is a threat that cannot be ignored. Distributed denial-of-service (DDoS) attacks remain a major security problem, the mitigation is very hard especially when it comes to highly distributed botnet-based attacks. The early discovery of these attacks, which is challenging but it is necessary to protect the end-users as well as the expensive network infrastructure resources. Various defense mechanisms have been discovered which acts as a protection guard for these DDos attacks. Although there are various defense and mitigation techniques for these attacks, the Prevention measures which are done at the earlier stage can prevent our network, server and websites from these DDos attacks.

REFERENCES

[1] International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 Volume 4 Issue 2 May 2013 *Intrusion detection system and Intrusion prevention system: a comparative study* Nilotpal Chakraborty School of Future Studies & Planning, Devi Ahilya University, Indore, India

[2] T. M. Gil, and M. Poleto, *MULTOPS: a data-structure for bandwidth attack detection*, in Proc. of 10th Usenix Security Symposium, Washington, DC, pp. 2338, August 1317, 2001.

[3] K. Park, and H. Lee, *On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets*, in Proc. ACM SIGCOMM, August 2001.

[4] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, *Controlling high bandwidth aggregates in the network*, presented at Computer Communication Review, pp.62-73, 2002

[5] R. Chen, J. M. Park, and R. Marchany, *TRACK: A novel approach for defending against distributed denial-of-service attacks*, Dept. of Electrical and Computer Engineering, Virginia Tech, Feb. 2006.

S.Srileka. " A Study of Distributed Denial of service Flooding Attacks by Preventive & Defense mechanisms." International Journal of Engineering Research and Applications (IJERA) , vol. 7, no. 11, 2017, pp. 69–72.