International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2015): 3.791

Distributed Denial of Service Attack

Shruti Sharma[1], Shreya Garg[2], Ayushi Karodiya[3], Himanshu Gupta[4]

[1, 2]Ujjain Engineering College, Sanwer Road 456010, Ujjain, India

[3]Chameli Devi Group of Institutes, Khandwa Road 452020, Indore, India

[4]JECRC University, Ramchandrapura Vidhani Village Jaipur, India

Abstract: ***Distributed Denial of Services attacks are a growing threat to Internet. DDOS attack methods are evolving and becoming more refined and target specific day by day. These attacks can quickly incapacitate a targeted business, costing victims thousands, if not millions, of dollars in lost revenue and productivity. This paper discuss about DDOS attack types, tools along with the traditional methods used for its prevention. Further, we described about the problems associated with defensive methods and how it could be improved. We have also given an insight of the recent DDOS attack on internet traffic management company Dyn and also the recent changes in DDOS attack.***

Keywords: DDOS, packets, server, host

1. Introduction

One day when you are sitting in your office trying to access the web server, you realized that your Web server becomes inaccessible. When you inspect, you realize that a flood of packets is rushing into your network. You have just become one of the hundreds of thousands of victims of a denial-of-service attack, a pervasive and growing threat to the Internet. The denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the interruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Denial-Of-Service (DOS) is an attack targeted at depriving legitimate users from online services. When this attack comes from a single host or network node, then it is simply referred to as a Denial of Service attack but when the attack comes from multitude of compromised system then that attack is called Distributed Denial of Service (DDOS).

2. Distributed Denial of Service Attack

DDOS is more dangerous and poses more threats as compare to DOS. Although, major DDOS attacks are difficult to create, minor DDOS attacks are easy to make. This is due to the wide variety of DDOS attack. It may do it by attacking the TCP/IP protocol, it may do it by attacking server resources, or it could be as simple as too many users demanding too much bandwidth simultaneously. Presently, the attack methods and tools have become more refined, effective, and more difficult to trace to the real attackers, while defense technologies have been unable to withstand large-scale attacks.

3. Different Types of DDOS Attack

One way to classify DDOS attacks is in terms of the type of resource that is consumed i.e. the resource consumed is either an internal host resource on the target system or data transmission capacity in the local network to which the target is attacked.

3.1 SYN Flood Attack

It is a type of Distributed Denial of Service (DDOS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. Essentially, with SYN flood DDOS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address. The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port. The malicious client either does not send the expected ACK, or—if the IP address is spoofed—never receives the SYN-ACK in the first place. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet for some time.

3.2 Distributed ICMP Attack

It is an attack that consumes data transmission resources. The following steps are involved:

1) The attacker takes control of multiple hosts over the Internet, instructing them to send ICMP ECHO packets3 with the target's spoofed IP address to a group of hosts that act as reflectors, as described subsequently.
2) Nodes at the bounce site receive multiple spoofed requests and respond by sending echo reply packets to the target site.
3) The target's router is flooded with packets from the bounce site, leaving no data transmission capacity for legitimate traffic.

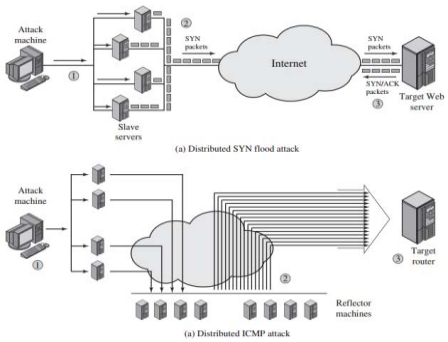

Figure 1: Types of DDOS Attack

Another way to classify DDOS attacks is as either direct or reflector DDOS attacks.

In a **direct DDOS** attack the attacker is able to implant zombie software on a number of sites distributed throughout the Internet. Often, the DDOS attack involves two levels of zombie machines: master zombies and slave zombies. The hosts of both machines have been infected with malicious code. The attacker coordinates and triggers the master zombies, which in turn coordinate and trigger the slave zombies. The use of two levels of zombies makes it more difficult to trace the attack back to its source and provides for a more resilient network of attackers.

A **reflector DDOS** attack adds another layer of machines. In this type of attack, the slave zombies construct packets requiring a response that contains the target's IP address as the source IP address in the packet's IP header. These packets are sent to uninfected machines known as reflectors. The uninfected machines respond with packets directed at the target machine. A reflector DDOS attack can easily involve more machines and more traffic than a direct DDOS attack and hence be more damaging.

4. DDOS Attack Tools

1) **Low Orbit Ion Cannon (LOIC):** It is flooding tool that produces excessive volumes of TCP, UDP, or HTTP traffic to subject server to a heavy network load.
2) **High Orbit Ion Cannon (HOIC):** It is a cross platform script for sending HTTP POST and GET requests wrapped in an easy to use GUI. It was used to target the U.S Department of Justice.
3) **hping:** It is a command line utility used to send large volumes of TCP traffic to a target while spoofing the source IP addresses.
4) **Slowloris :** It uses a very slow HTTP requests by sending HTTP headers to the target site in tiny chunks as slowly as possible which makes the server to wait for the headers to arrive and thus creating DOS.
5) **R.U.D.Y:** RUDY achieves DOS by using long form field HHTP POST submission. It causes the application to await the nonstop posts in order to do processing.
6) **#Refref:** It is based on vulnerabilities in SQL database software that allow for injection attacks. It forces the server to use a special SQL function that causes non -stop execution of few lines of codes that consumes server's resource causing DOS.
7) **Botnets:** Botnets are large collection of compromised computers, often called "zombies", infected with malware that allows an attacker to control them.

5. Recent Havoc created by DDOS on Websites

Just few days ago on 21st October DDOS attack crippled servers across U.S East Coast around 11 a.m affecting hundreds of websites including the New York Times, Reddit, Twitter, Spotify and eBay making them unreachable for parts of the day. The attack came from "tens of millions" of addresses on machines that had been infected with malicious software code. The code—known as Mirai—takes advantage of a weakness in internet-connected devices and forms them into a collection of attacking machines, called a "botnet". Other sites temporarily disrupted by the attacks included PayPal Holdings Inc., Shopify,Airbnb, Kayak and GitHub, a service used by programmers and major technology firms to create software. The Mirai botnet that formed the backbone of this attack is thought to be made up of several hundred thousand devices, but criminals are able to make their attacks appear to come from an even larger number of devices, using a technique called "source spoofing". The thorough investigation to find other sources of traffic for attack is still in progress. Continuing the trend from 2015, the most common DDoS attack types in Q1 2016 were UDP floods (DNS, NTP, SSDP and SNMP), making up 62 percent of total attacks in the quarter.

6. Defense against DDOS

In general, there are three lines of defense against DDOS attacks

- **Attack prevention and preemption (before the attack):** These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients. Techniques include enforcing policies for resource consumption and providing backup resources available on demand. In addition, prevention mechanisms modify systems and protocols on the Internet to reduce the possibility of DDoS attacks. On one side host may be securely protected from master and agent implants. There are indeed known signatures and scanning procedures to detect them. Another is to monitor network traffic known attack messages sent between attackers and masters. On the active side, cyber informants and cyber spies can be employed to intercept attack plans.
- **Attack detection and filtering (during the attack):** These mechanisms attempt to detect the attack as it begins and respond immediately. This minimizes the impact of the attack on the target. Detection involves looking for suspicious patterns of behavior. Response involves filtering out packets likely to be part of the attack. The detection part is responsible for identifying the ddos attacks or attack packets. The filtering part is responsible for classifying those packets and then dropping them.
- **Attack source traceback and identification (during and after the attack):** This is an attempt to identify the source of the attack as a first step in preventing future attacks. There are two approaches for traceback. One is for router to record information about packets they have seen for

later traceback requests. Another is for router to send additional information about the packets they have seen to the packet's destinations via either the packets or another channel. However, this method typically does not yield results fast enough, if at all, to mitigate an ongoing attack.

7. Problems in DDOS mitigation and an urgent need to improve it

DDOS attacks are complex problem to solve. First, there are no common characteristics of DDOS streams that can be used for their detection. Furthermore, the distributed nature of DDOS attacks makes them extremely difficult to combat or trace back. Moreover, the automated tools that make the deployment of a DDOS attack possible can be easily downloaded. Attackers may also use IP spoofing in order to hide their true identity, and this makes the traceback of DDOS attacks even more difficult. Finally, there is no sufficient security level on all machines in the Internet, while there are persistent security holes in Internet hosts.

The conventional understanding of DDOS is one that involves volume and capacity. But, there's a much more sophisticated kind of attack starting to become more common – and that's application layer attacks. You don't need as much volume, and it's extremely hard to detect.

DDOS attackers are now expending quite a lot of effort to spoof legitimate sessions. They'll do a fair amount of reconnaissance on their target, identify where the weakness or vulnerabilities are – say, a login page. And they know that if they run 20, or 50 or maybe 100 concurrent sessions of that login, it'll lock up the backend database, rendering the site down.

Presently, in the mitigation industry, a lot of companies are offering platforms that can deal with the traditional interpretation of DDOS, but the industries must be prepared to deal with the more urbane and more targeted kind of attacks. The strategy right now is less preventing on an attack, and more on how quickly can you respond? They need to analyze, parse, and create a quick, customized rule set that's very granular and can be applied to specific parts of the website – an element, or a UI for instance

8. Conclusion

DDOS attacks are combative and constantly evolving. In the past two to three years, these attacks have undergone significant technological improvements that make them exponentially more powerful and threat full than previous attacks. In addition, the availability of "rent-a-bots" makes it easier for hackers to launch these attacks, and the increasingly criminalized nature of these attacks, which makes them more dangerous. The current defensive mechanism as discussed in this paper is inadequate and there exist many vulnerable areas in the internet that are susceptible to DDOS attacks. There is an exigent need of building a powerful and combative defense mechanism to protect the entire internet form DDOS attacks

References

[1] Patrikakis, C.; Masikos, M.; and Zouraraki, O. "Distributed Denial of Service Attacks." The Internet Protocol Journal, December 2004.
[2] Chang, R. "Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial." IEEE Communications Magazine, October 2002
[3] CERT Coordination Center."Denial of Service Attacks." June 2001. http://www.cert.org/ tech_tips/denial_of_service.html
[4] http://www.wsj.com/articles/how-denial-of-service-attacks-wreak-havoc-on-websites-1477076597
[5] http://www.itproportal.com/2014/02/04/the-future-of-ddos-and-how-to-stay-ahead-of-attacks/
[6] https://security.radware.com/ddos-knowledge-center/ddos-attack-types/common-ddos-attack-tools/
[7] http://projects.laas.fr/METROSEC/Security_and_DoS.pdf
[8] https://www.incapsula.com/ddos/attack-glossary/syn-flood.html
[9] William Stallings, "Cryptography and Network Security: Principles and Practice" Pearson