DDOS Protection by Dividing and Limiting

Harshil Shah
Computer Science
hri Bhagubai Mafatlal
Polytechnic,
Mumbai

Priyansh Shah
Computer Science
Shri Bhagubai Mafatlal
Polytechnic,
Mumbai

Swapna Naik
Computer Science
Shri Bhagubai Mafatlal
Polytechnic,
Mumbai

ABSTRACT

DDOS attacks have increased lately to an extent where large companies have lost millions. They pose a large threat to internet security. This paper explains DOS and DDOS attacks and their types as well as two computer softwares – LOIC and DDOSIM - to launch DDOS attacks and the history of the well-known botnets and DDOS attacks. A solution for DDOS protection at application layer is also proposed. It explores the combination of various tools and techniques like ingress filtering, IP address blacklist checker and dividing the server as a measure to limit the attacks.

General Terms

DDOS protection, dividing and limiting, types of DOS attacks, types of DDOS attacks.

Keywords

DOS, DDOS, ingress filtering, dividing, IP blacklist, LOIC, DDOSIM, botnet.

1. INTRODUCTION

This paper explains main types of DOS and DDOS attacks along with history of DDOS attacks and a brief study on the botnet and its types. We also explain our solution to the DDOS attacks. Section 2 explains DOS attacks along with its types. Section 3 describes DDOS attacks and botnet. Section 4 describes two DOS/DDOS softwares – LOIC and DDOSIM. Section 5 describes history of DDOS attacks and some of the well-known botnets. Section 6 describes our solution towards DDOS attacks.

2. DENIAL OF SERVICE (DOS)

DOS is an older technique compared to DDOS. In a DOS attack, the user or the organization is denied the services they normally expect. DOS/DDOS attack does not usually result in theft of information or security loss. But a DOS/DDOS attack can cost a particular person/company a great deal of money and time. The usual method to carry out a DOS attack is - take the case of a network which is going to be a victim of the DOS attack. The network has a bandwidth of 100 Mbps i.e. it cannot handle traffic more than 100 Mbps. The attacker sends a huge number, tons even, of legitimate looking packets. So in order to flood the network, the attacker should have a bandwidth higher than 100 Mbps. This will cause the network to exhaust its capacity, thereby resulting in shutting down of system or unusually slowing down and thus denying service to its legitimate users.

2.1 Types of DOS Attacks

1) *Bandwidth flood*: This involves sending a lot of traffic that eventually overwhelms the network. Usually the attacker sends multiple requests, for instance ping requests (at least 10000 requests per second) to the target and considerably lowers the target speed [8].

2) *Service Request flood*: It is more precise than just sending a bunch of network traffic. During the attack, a large volume of specific service requests like DNS queries, TCP connection requests, HTTP requests are sent to the target. Initiated service requests do not necessarily have to be met with; they just have to consume resources [8].

3) *ICMP flood*: Processing and responding to an ICMP request consumes CPU resources. In an ICMP flood, the attacker sends multiple ICMP requests without waiting for response. At a certain point the server's ability to serve these requests is impaired thereby blocking legitimate requests [8].

4) *SYN flood*: In an SYN flood, the three-way handshake method of TCP/IP network is manipulated. Sending a lot of SYN packets and leaving them half open and then continuing to send them is the norm. The target tries to service all of these half open SYN requests. This results in the target waiting for 75 sec to purge all the half open requests. [A SYN request should be open for 75 sec before purge.] One of the techniques to leave this SYN requests half open is - the attacker usually spoofs his IP address and sends an SYN request to the target. The target replies with a confirmation packet to the spoofed IP address, but the spoofed IP address won't send an acknowledgement to the target as it never sent an SYN request in the first place, thus resulting in the request being half open. Now tens of thousands of SYN requests pending for 75 seconds are going to either shut down or fail the system.

5) *Slow Loris attack*: The attacker tries to make many connections to the target web server and hold them open for as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. Periodically it will send HTTP headers, adding to but never completing the request. Affected servers will keep these connections open, filling their maximum concurrent connection pool and eventually denying additional connection attempts from legitimate clients.

6) *NTP amplified attack*: An NTP server responds to a command called mon_list (monitor list) where the server returns a list of IP addresses of up to last 600 machines that the NTP server has interacted with. This response is much bigger than the request sent making it ideal for an amplified attack. The request packet is 234 bytes long. The response is split across 10 packets totaling 4460 bytes i.e. an amplification factor of 19x. The attacker usually forges his IP address to that of target's IP address

and sends multiple requests to an NTP server. The target is overwhelmed with the packets received from NTP server

2.2 Limitations of DOS Attacks

The IP address of the attacker is easily compromised. Great bandwidth and computational power is required to make an effective attack. Modern routers are smart. They can sense the traffic pattern and may realise that a specific client is sending too many packets compared to the other clients, thus blocking his IP address and preventing the attack. Hence the attack may last only for a short period of time. In order to overcome these drawbacks, "Distributed Denial of Service" attacks are used currently.

3. DISTRIBUTED DENIAL OF SERVICE (DDOS)

Unlike a DOS attack where only a single internet connection is used to carry out the attacks, a DDOS attack occurs when multiple systems flood the bandwidth or resources of a targeted system. The advantage of DDOS attack is that processing power as well as bandwidth of multiple computers is used to attack a target server which makes it hard to locate the attacker (sometimes the attacker doesn't even take part in carrying out the attacks) and making the attack more severe. This also makes it hard for the server to differentiate between legitimate and illegitimate traffic.

3.1 Botnet – The Best Medium to Carry Out DDOS Attacks

Botnet (network of bots) is basically a network of computers that are infected by single virus. Attacker who spreads this virus across the network can control several functions of the infected computers according to the type of virus. The infected computers are generally referred to as bots. These bots are spread across the network in a zombie manner where the attacker infects one computer and the infected computer infects others and so on. Botnets pose a very large threat to internet security. A botnet can be used for several malpractices like stealing personal information, carrying out DDOS attacks, etc. The computers (victims) in a botnet are unaware of the fact that they're being used to carry out DDOS attacks. You can identify if your computer is being used as a bot only when your internet speed decreases or by using an anti-virus software. These anti-virus softwares cross-check known virus signatures against your PC files and detect it accordingly. However, if the bots are custom made, it's hard to detect the virus. The attacker basically sends a small virus across network. The virus can spread by using various methods such as click baits, spam mails, software crack files and a more recent method where virus is encrypted in the header of an image. These bots are generally triggered to carry out an attack when the attacker instructs them [9].

3.2 Types of Botnets

1) *C&C type*: Bots in C&C type use command and control server to communicate and carry out the attacks accordingly. These bots communicate through Internet Relay Chat on a C&C channel. The attacker sets up C&C server on his own machine or in some cases even infected computers are used as C&C servers. These bots generally remain hidden until the attacker forwards the instruction. The attacker joins the C&C server first thus having the privileges to control the whole botnet. In order to take down a C&C botnet, usually C&C servers are located and taken down thus breaking the communication. Taking down the C&C server doesn't mean taking down the bots, the bots can be again used after setting a new C&C server of the same configuration.

2) *P2P type*: In a peer-2-peer botnet command and control servers are not used. Instead the computers are randomly organised where one computer gives commands to one or more computers and in turn the computers receiving commands forward the commands to others. The bots generally maintain a list of trusted/infected computers. One of the recent methods includes using a twitter account to instruct the bots to carry out an attack. The bots are configured in such a way that they check a certain twitter account/page to check for instructions at certain intervals. The attacker tweets the instructions which triggers the bots to carry out the attacks. However, latency can be a problem in P2P botnet as by the time the command passes along the chain, the bots carry out attacks without waiting for command to pass through whole botnet, which creates a difference between two attacks carried by two different bots. P2P botnet attacks are the most difficult to stop.

4. DOS/DDOS SOFTWARES

1) *Low Orbit Ion Canon*: LOIC is an open-source software developed to carry out DOS attacks on a system so as to check/test the stress of network. It's been written in C Sharp. LOIC performs a DOS/DDOS (when multiple users join simultaneously) by flooding the server with TCP/UDP packets. LOIC has a URL/IP field where you enter the URL/IP of the server you want to attack. The LOIC uses port 80 as default port to attack the server. The software can implement its attack in the form of multiple HTTP requests or ICMP/SYN flood technique where it sends multiple packets or opens multiple connections to target simultaneously. One can also increase the speed/frequency of attack. The frequency of the attack depends on bandwidth and processing power of the computer. The "IMMA CHARGING MAH LAZEER" button is the button to start the attacks. The software will start slowing down the server after a certain point [3].

2) *DDOSIM*: DDOSIM is a layer-7 DDOS simulator just like LOIC but instead of single PC, it is used in lab environment. It is used to test the amount of load a server can handle. DDOSIM creates a zombie army with random IP addresses which open connections with server. After establishing the connection DDOSIM starts its attacks on the server [4].

5. HISTORY OF HIGH SCALE DDOS ATTACKS

One of the most recent high scale DDOS attacks was observed in Mumbai where the local ISPs were targeted with a magnitude of 200 gigabytes per second. This resulted in shutting down of these ISPs for 4-5 days [6]. As a matter of fact, India is one of the biggest hot-bed for DDOS attackers due to lack of people's awareness in cyber security. Cyber security expert L. S. Subramanian quoted, "Because of tight security budgets and lack of awareness of end users to secure their PC, they are vulnerable to malware and turn themselves into a botnet node. [7]"

Some of the famous botnet include - The MEGA-D botnet detected in 2008 and bought down in 2009. Before it was taken down it was successful in infecting 500k computers worldwide responsible for 32% of spam at that time. ZeroAccess was a botnet controlling 1.9 million computers around the world. It generated fake clicks on advertising yielding revenue for each clicks to the advertisement. One of the biggest P2P botnet named Storm controlled over 1 million to 50 million computers. It was known for enabling share price fraud and identity theft. Many such botnets have been detected and dismantled. However, there are many botnets still alive [2].

6. LIMITING APPLICATION LAYER DDOS ATTACK THROUGH DIVIDING AND LIMITING

In the different types of attacks discussed above, most of them take place at network layer i.e. they overwhelm the bandwidth of network and make it slow for legitimate traffic to reach the target. However, network layer attacks can be prevented by pattern sensing of traffic and blocking the attacker.

Unlike network layer attacks, application layer based attacks are much harder to stop. Application layer based DDOS attack involves exhausting the resources. This can be achieved in certain ways. One of the ways is to send multiple HTTP requests to the server which consumes a lot of server processing power. Thus most of processor time is allocated to illegitimate traffic resulting in denying of service to legitimate traffic. If botnet is used to carry out such attacks it becomes much harder for the server to differentiate between legitimate and illegitimate traffic [1].

In the attacks some of the points are common such as – attacker spoofs his IP address, sending illegitimate/malicious traffic. Our approach includes combination of ingress filtering at firewall, monitoring the traffic via IP address blacklist checker, dividing the server into segments to increase security and limiting processing power that can be used by each client.

6.1 Ingress Filtering

It's a technique used to authenticate whether the traffic has actually originated from the source it claims to be. Source IP address that are commonly blocked by ingress filtering are:-

1. IP address already in use in an internal network. This stops the attacker from taking advantage of poorly written firewall.
2. IP address that is private.
3. IP addresses that are multicast.
4. Service or management network IP address.

Thus, using ingress filtering at firewall will discard spoofed packets reducing the possibility of DDOS attacks [5].

6.2 IP Address Blacklist Checker

This is done by using the DNSBL list. A DNSBL (domain name system black list) is a list which maintains the IP address of systems that have a history of sending spam. This list is based on the Internet Domain Name System which converts complicated IP address into simple names which makes it easier to read, use and search. This list can be used by the administrator to crosscheck with the IP addresses to flag/reject suspected packets.

6.3 Dividing and Limiting

Dividing the server into several segments and forcing security constraints at each segment will gradually decrease the possibility of application layer DDOS attacks. In case a malicious packet succeeds in entering the server it will affect that particular segment and not the whole server. Also monitoring the traffic at each segments and exchanging information with each and every segments will improve overall efficiency of system to identify illegitimate traffic. Additionally, limiting the processor time to each and every server process will reduce the ability of application layer DDOS attacks to exhaust the processing power.

7. CONCLUSION

In this paper a new concept of limiting DDOS attacks was introduced. However, DDOS attack still poses a very large threat to cyber security. With the improvements in technology (4G/LTE) or networking speed, the frequency of DDOS attacks is going to increase as well. With increasing nodes in botnet it will make it harder to mitigate a large scale DDOS attack. Thus awareness about internet security is required. Proper security measures are needed to be taken at ISP side (egress filtering) as well server side such as using firewalls, proxies, etc. to minimize the effect of this attacks. The future scope of this paper is limited as this solution does not nullify the DDOS attacks.

8. REFERENCES

[1] Ukasz Apiecionek, Wojciech Makowski. "Firewall rule with token bucket as a DDOS tool", in Proc. IEEE, 2015, pp. 32-35.

[2] Karl Thomas. "Nine bad botnets and the damage they did."Internet:http://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/, 25 feb 2015.

[3] Deepankar Varma. "LOIC (Low Orbit Ion Canon) – DOS attacking tool." Internet: http://resources.infosecinstitute.com/loic-dos-attacking-tool/, 20 dec 2011.

[4] Groove group's blog. "Application layer DDOS simulatorddosimv.02."Internet:https://thegrovegroup.wordpress.com/2010/12/18/application-layer-ddos-simulator-ddosim-v0-2/, 19 dec 2010.

[5] Mathew Haughn. "Ingress filtering." Internet: http://whatis.techtarget.com/definition/ingress-filtering, june 2015.

[6] Asheeta Regidi. "Internet service providers in Mumbai targeted in DDOS attack." Internet: http://tech.firstpost.co m/news-analysis/internet-service-providers-in-mumbai-targeted-in-ddos-attack-326708.html, 25 jul 2016.

[7] Geetha Nandikotkur. "India launches most DDOS attack."Internet:http://www.bankinfosecurity.in/india-launches-most-ddos-attacks-a-7512, 31 oct 2014.

[8] PluralsightIT. "Ethical hacking – Types of DOS attacks."Internet:https://www.youtube.com/watch?v=7VMvo0-qLl0, 15 may 2012.

[9] JackTutorials. "Explained! #1 – What is Botnet." Internet: https://www.youtube.com/watch?v=ahynBPv58n8, 10 may 2015.