ISSN:0975-9646

Survey on Application Layer DDoS Attacks

Anjali. M[1], B.Padmavathi[2]

Department of Computer Engineering, Pune University,

G. H. Raisoni College of Engineering and Management, Wagholi, Pune, Maharashtra, India.

Abstract- DDoS attacks are the process of making the target system non-responsive to the legitimate requests. They were focusing on network and transport layers initially. Now the application layer DDoS attacks are prominent and are most difficult to resolve online. This paper presents a comprehensive study on Botnet-based DDoS attacks on application layer, and the extended incidents of such attacks that are clearly increased recently.

Keywords— Application layer, DDoS attacks, Botnet, attacker, victim

I. INTRODUCTION

With the increase in development of internet in past few years, online attacks are also incremented. DDoS attacks are dangerous threats among them. Three main classifications of DDoS attacks are there. Bandwidth attack, Resource attack and Application layer attack. Bandwidth and resource attacks focus on Transport layer or network layer. Application-layer DDoS attacks are a bit more complicated. They are some of the most difficult attacks to mitigate against because they mimic legitimate traffic as they interact with the user interface.

The mechanism behind distributed DoS attacks is Botnets. They are the network of controlled computers. Bots are malicious programs that are written for specific purposes and they can be controlled by attackers through command and control server. Attackers or bot-masters frequently move C&C servers to avoid disruption.

Layer 3/4 DDoS attacks are volumetric attacks. Target machine is overwhelmed by a large number of packets. Malicious traffic (TCP/UDP) is used to flood the victim. Flooding continues until the victim goes offline. But there is no lasting damage once they are mitigated.

Application layer DDoS attacks concentrate on specific areas of website, making it more difficult to differentiate from normal traffic. The number of DDoS attacks that target weak spots in Web applications in addition to network services has risen during the past year and attackers are using increasingly revolutionary methods to bypass defences. Application layer DDoS attacks, specifically HTTP attacks rank first among the number of DDoS attacks for the past few years.

II. RELATED WORK

Botnet based DDoS attacks are divided into three. They are agent-handler, IRC-based, and Web-based models

A. *Agent-Handler Model*

The agent-handler model of a DDoS attack contains clients, agents and handlers. Attacker communicates with clients in the DDoS attack system. Software packages located throughout the Internet are handlers. The client uses handler packages to communicate with the agents. For conducting the attack at the appropriate time, agent software thrives in zombie system. Handlers are used for another purpose too. In-order to identify operational agents and to decide timing of attack and whether agents are to be upgraded or not, attackers communicates with agents. These all things are happening with-out the knowledge of owners and users of agent systems. Agents can communicate with one handler or with many handlers. Handler software is installed on a compromised router or network server by the attackers frequently. The term handler can be master and agent can be demons, in DDoS tools description [1].

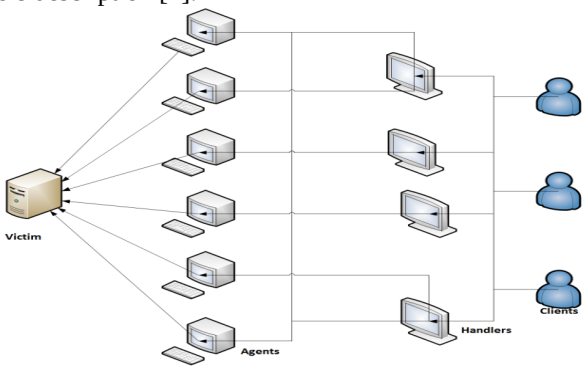

Fig. 1 Agent-handler model

B. *Internet Relay Chat (IRC) Model*

This model has similarities with Agent-Handler model. Here an IRC communication channel is used for the connection between clients and agents. Handler software's are not used. An Internet Relay Chat (IRC) channel contains IRC ports for sending commands mainly to agents. These ports are legitimate ports thus DDoS command packets are not getting tracked. IRC servers allow large volume of traffic, so attackers can easily hide their presence. IRC servers contain the list of agents and attackers do not have to search for that. Agents communicate with attackers through IRC channel to inform they are operational by sending messages. IRC connections are unencrypted. Therefore it is an attractive model for DDoS attackers [1].

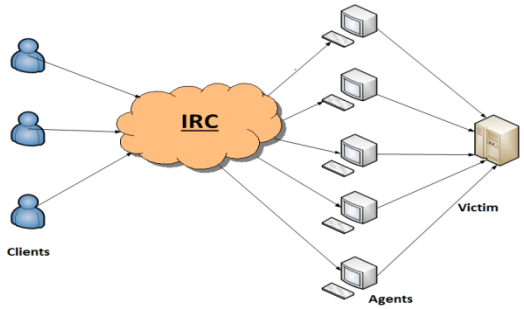

Fig. 2 Internet relay chat model

C. *Web-based Model*

For Botnet command and control (C&C), most convenient way for attacker is the IRC-based model. But for last few years web-based reporting and command has emerged .Bots has to simply report statistics to website in Web-based model. A number of bots in the Web-based model simply report statistics to a Web site, whereas in other models bots are fully configured and controlled through encrypted communications and PHP scripts and over the 80/443 port and the HTTP/HTTPS protocol.

III. PROPOSED WORK

A. Net DDoS-based Bandwidth Attacks

Net DDoS-based bandwidth attacks consume bandwidth of a network, and it takes advantage of specific IP weaknesses. Examples of such attacks are SYN and ICMP flood attacks.

1) *SYN Flood Attacks:* In SYN flood attack, vulnerability of TCP three-way handshake is utilized. In TCP 3 way handshake client sends SYN packets to the server for requesting new connection. Server acknowledges by sending SYN-ACK packet back. Client responds with ACK packet as third step, thus a connection is established. During SYN flood attacks, SYN packets are sent by the attacker with spoofed source IP addresses. Because of spoofed SYN packets are sent to the server, connection is never established. ACK packets from the client are not received in SYN flood attack. The memory stack becomes full with each half open connection. Consequently, no further requests can be processed. All services from the system are denied and it becomes offline.

2) *ICMP Flood Attacks:* In this attack, attacker sends a large number of ICMP requests to the victim and victim becomes busy by sending replies to the attacker and not able to service legitimate requests. In Smurf attack, through broadcast address attacker sends packets to all systems in a network. Attacker sends spoofed IP packets to the network with the address of victim. Victim is overwhelmed with ICMP replies from the network, and leads to denial of service of legitimate requests. Ping flood and Ping of Death are other ICMP attacks.

B. App-DDoS attacks

Application layer DDoS attack is for some specific purposes. A small number of resources are required for this attack. It is very difficult to distinguish legitimate and illegitimate traffic in Application layer DDoS attacks.

1) *HTTP Flood attacks:* HTTP flood attacks are layer 7 attacks. HTTP GET/POST requests are sent to the target server. These requests are sent through the IP address of a bot and to avoid detection they are formulated in different ways. For example to download a file from a target machine attacker sends a http request through botnet. Target machine downloads file from the hard disk, stores it in the memory, and sends back to botnet. Thus a simple http request causes consumption of resources in CPU, memory, input/output devices. Repetitive requests to download a file from same server would be suspicious. Therefore attacker gives instructions to botnet to send request to web-server. Thus it mimics legitimate traffic and it becomes difficult to distinguish between normal and attack traffic.

2) *Session Initiation Protocol (SIP) Flood attacks:* For controlling multimedia communication sessions SIP protocols are widely used [3]. VOIP has a tendency to rely on SIP. SIP INVITE packets are used to conduct flooding attacks. There are two victims in this flooding attack. They are SIP proxy server and call receiver. Resources of SIP proxy server are depleted by processing SIP INVITE packets. Thus they lack their ability of providing VOIP service. The second victim is call receiver. They are flooded with fake VOIP calls and unable to service legitimate requests.

3) *Distributed Reflector attacks:* Distributed reflector attacks hide the attack source by third parties. These third parties are reflectors. In this attack, attackers acquire control over zombies as first step. In the second step, attacker gives instructions to zombies to send attack traffic to victim via third parties. Third parties send the reply traffic as third step and thus the DDoS attack occur. The DRDoS attack occurred in February 2014 was a NTP reflection attack. Attack was appeared to be coming from OVH.com, but they were the third parties. DRDoS attack has been considered a powerful and increasingly widespread internet attack. Because of, this attack is further dispersed through third parties, and thus identification of attack source is a difficult task [4]. DRDoS attack can amplify the attack traffic, thereby attack becomes more harmful.

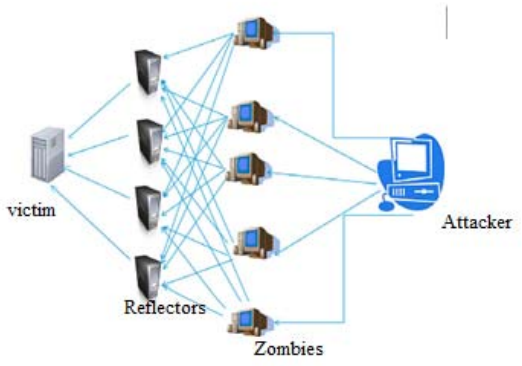

Fig. 3 Distributed Reflector Attacks

4) Domain Name System Amplification (DNS) Attacks: DNS amplification attack is an effective DRDoS attack. Different resource records and Internet domain

names are stored in a storage infrastructure called Domain Name System. DNS maps domain names with IP addresses. A requestor sends a query to the DNS server to resolve domain names. Recursive DNS server resolves queries by contacting authoritative servers if necessary. DNS query responses have large size than query requests.

C. Surprising Trends in Application Layer DDoS Attacks

IPS devices and firewalls allow HTTP or DNS traffic. These devices are not able to distinguish between normal traffic and attack traffic, thus bypasses one layer of security for the attacker.

To stop DDoS attacks online gaming companies are ready to pay a big amount of money to the attacker, such that per day revenue will be higher than a non-profitable company.

D. *The DDoS threat*

A DDoS attack directs a large number of "zombie" hosts which are compromised, against a single target. It is possible for any attacker to build a set of zombies quickly. If the number of zombies is large, the volume of DDoS attack will be high. Availability of attacking tools is another reason to make DDoS attacks wide spread. Trinoo, TFN, TFN2K [2] are some examples of tools to launch DDoS attacks. A successful DDoS attack gives widespread impact. Compromised site performance, violated SLA's, diminished company reputations, revenue loss, productivity loss etc are some impacts of DDoS attacks. DDoS attackers are using complex spoofing techniques and legitimate protocols. Thus it is very difficult to detect and defeat

.

E. Botnet Based DDoS Attacks

Application layer DDoS attacks are a major threat to Internet nowadays. It becomes more dangerous if it is botnet based. First large scale DDoS attack was reported against a university in August 1999. University network became shut down for two days. DDoS attacks occur daily. The popular websites such as Google, Twitter, and Facebook are also not able to escape from DDoS attacks. DDoS attacks against White House, FBI, DOJ, Hong Kong stock exchange are some eye-opener cases. In March 2013, a DDoS attack knocked the company Spamhaus, and it became offline. It was a DNS amplification attack [6]. 75 Gbps attack traffic was generated in this attack. To mitigate this attack, Cloud Flare announces same IP address for its 23 datacentres in one hour interval. In February 2014, 400Gbps attack traffic was generated against a company. It was a NTP DRDoS attack [5].

Revenue loss and customer loss are the main losses of Botnet based DDoS attacks. Customer loss happens because of degraded reputation. Many companies are no ready to reveal their name, if DDoS attack occur on them because of that.

IV. CONCLUSION

Botnet based DDoS attack is a serious threat to Internet. A clear picture of Application layer DDoS attacks are presented here. It is very difficult to distinguish between normal and attack traffic if it is Application layer DDoS attacks.

To detect DDoS attacks from normal traffic, an effective method should be found out as a future work.

ACKNOWLEDGEMENT

With immense pleasure, we are presenting this paper as a part of the curriculum of M.E Computer Engineering. We are very thankful to our guide, for guidance, encouragement, co-operation and timely help during the preparation phase, because of which we could complete our work.

REFERENCES

[1] Esraa Alomari, Selvakumar Manickam, B. B. Gupta, Shankar Karuppayah, Rafeef Alfaris "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art" *International Journal of Computer Applications (0975 – 8887)*, vol. 49, no.7, July 2012.

[2] Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyyaand J. K. Kalita "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions," *The Computer Journal (2013)* doi: 10.1093/comjnl/bxt031.

[3] Felipe Huici, Saverio Niccolini, Nico d'Heureuse "Protecting SIP against Very Large Flooding DoS Attacks" IEEE, Global Communications Conference, 2009.

[4] www.securityweek.com

[5] http://www.darkreading.com/attacks-and-breaches/ddos-attack-hits-400-gbit-s-breaks-record/d/d-id/1113787

[6] http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/