IJCSC International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 239-241

Analysis of Botnet Behavior Using Queuing Theory

Shruti Singh[1] & Manasi Gyanchandani[2]

[1-2]Department of Computer Science & Engineering, MANIT, Bhopal, India
Email: [1]sshruti.0939@gmail.com, [2]manasi_gyanchandani@yahoo.co.in

ABSTRACT

With the rapid development of information technology, internet has affect the people in all aspects such as public utilities, telecommunication, financial transaction and defense system, all depends on information technology and their security. By using latest technology and internet, attackers may perform malicious activities. Botnet is the most serious emerging threat. Botnet performs various kinds of malicious activities and one of them is DDoS. DDoS degrades the performance of a network disconnects the host and performs bandwidth depletion and resource depletion attack. This paper gives a brief detail of Botnet, DDoS attack and analysis of bot behavior.
Keywords: DoS, DDoS, Botnet.

1. INTRODUCTION

Botnets are the network compromised machines under the control of a human operator. Using botnet attacker can perform various attacks like distributed denial of service (DDoS), email spamming, key logging, click fraud etc. A Denial of Service (DoS) attack is an attack is used preventing legitimate users from using a specified network resource such as a website, web service, or computer system. A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems.

2. DOS AND DDOS ATTACK

2.1. DoS Attack

DoS attack is a type of attack on a network. A DoS Attack is an attempt to make a computer resource or service unavailable to its legitimate users [1]. RFC 4732 defines DoS attack.

2.1.1. Types of DoS attack

1. *UDP Flooding:* UDP flooding is host based DoS attack. This attack can be initialized by sending large number of UDP packets to the random port on the victim system. If large number of UDP packet is delivered to the random ports on victim system, the victim system will go down.
2. *TCP SYN Flooding:* TCP SYN is also known as SYN flooding. This attack uses 3 way handshakes that initialize a new TCP connection. If attackers rapidly send SYN segments without spoofing their IP source address, this is called a direct attack. Another attack is spoofing attack. In this attack attacker uses IP address spoofing [2].
3. *Ping of Death:* The Ping of Death uses a ping system utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang, or reboot when they receive such a maliciously crafted packet.
4. *Smurf Attack:* In Smurf Attack, attacker generates large amount of traffic on a victim computer. Attacker sends a packet as a direct broadcast to a subnet of a network. All the system in the subnet sends the reply of this broadcast. Attacker uses spoofed IP address. By spoofing the source IP address of the packet, all the responses will get sent to the spoofed IP address. Thus attacker floods a victim. This attack is an example of amplification attack [7].

2.2. DDoS Attack

DDoS attack is used to perform overloading in a network or system, so that an authorized user cannot use the service. Using this attack, attacker can neither crack authentication of a system nor can gain unauthorized access to a system but this attack is used to degrade the performance of a network.

The main difference between DDoS and DoS attack is that DoS attack utilizes one source or system where as DDoS attack uses large number of compromised systems or sources which are trying to attack on a single or small number of target systems. DDoS attack starts when a copy of malicious software (Trojans, virus or worms) gets

installed on large number of systems. This malicious software is called "Bot"[3]. The term "Bot" is used to describe an automated process. The word Bot has been derived from the word "Robot". Robot is a Czech word which means "worker"[4]. The compromised bots are controlled by a single entity known as "Botmaster". Botmaster acts as a bot controller and other bots form a "zombie army" or "botnet"[5].

2.2.1. Goal of DDoS Attack

In Distributed Denial of Service, attacker attempts to flood a network, interrupts the connection between two machines, prevents a particular legitimate user from accessing a resource and thus disrupts the service of system [6].

In botnet, botmaster first send malicious code to cause initial infection. Initially infected system, are called secondary victim. These bots again send malicious code to other systems in network and these compromised systems also works as bot.

Botmaster instructs these compromised bots to attack the services by killing a target resource. This target resource acts as a primary victim.

If the size of the botnet is adequately large, DDoS attack through botnet can be better synchronized.

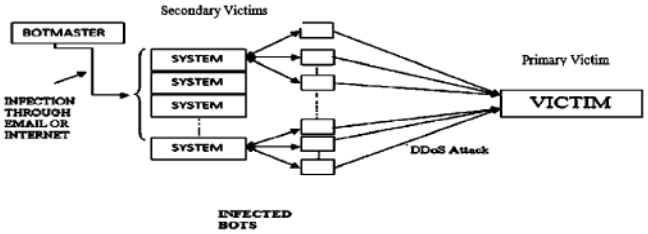

Fig. 1: DDoS Attack Through Botnet

Fig.1 shows how a botmaster send a malicious code through email or internet or by using exploit scanning/ autorooting and infects a large number of computers with in a network, to perform DDoS attack.

There are two main types of DDoS attack: bandwidth depletion and resource depletion as shown in figure 2[7]. Bandwidth depletion attack is used to prevent legitimate traffic from reaching the target. This attack commonly includes UDP flood attack, ICMP flood attack, and reflection attack. Resource depletion attacker tries to deplete resource on the victim computer. This attack includes TCP SYN attacks, PUSH and ACK attacks, teardrop, and recursive HTTP attacks.

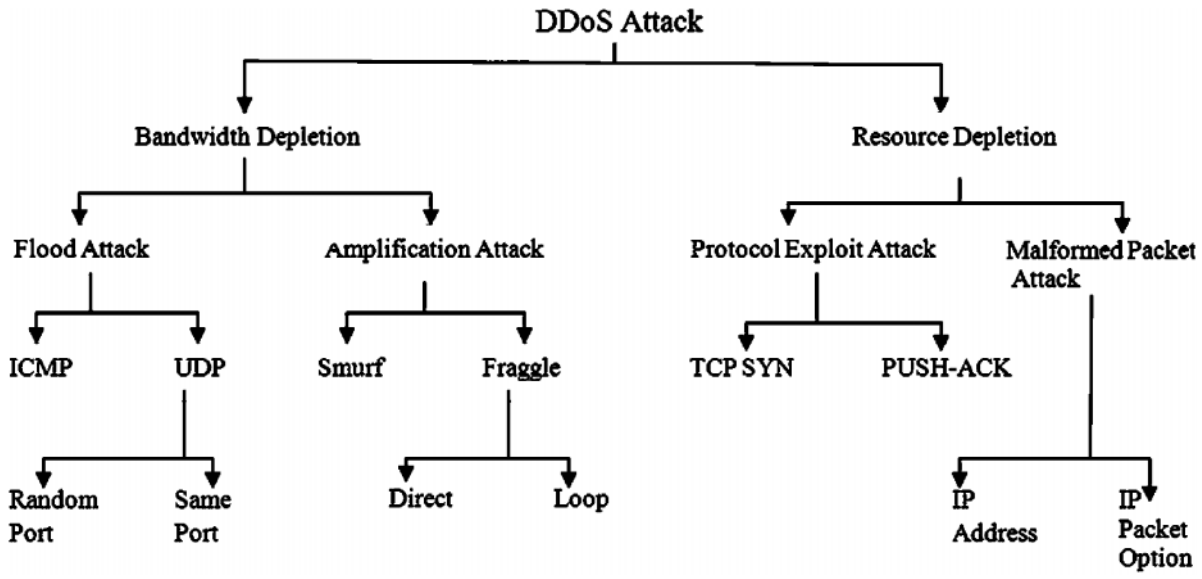

Fig. 2: DDoS Attack Variants

3. IMPLEMENTATION WORK

We simulate a Botnet network. Simulation is in NS2. We simulate the entire network with a scenario given in table 1. The system consists of 17 nodes. In this botnet one node work as botmaster, six nodes work as bot, one node is the server node, three nodes are victim nodes and remaining six nodes are normal nodes. For DDoS attack, we have used UDP flooding in simulation and applied queuing theory to evaluate the performance of network.

Table 1
Simulation Scenario

Number of nodes	17
Bot nodes	6
Victim nodes	3
Server nodes	1
Normal nodes	6
Botmaster	1

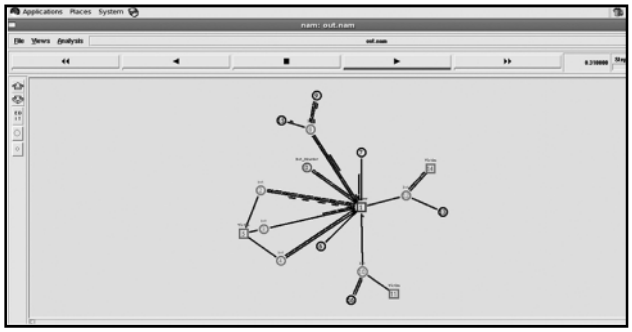

Fig. 3: Screen Shot of the Simulation

The figure 3 shows the screen shot of the above mentioned simulation scenario. We have applied queuing theory to determine the packet drop rate as a result of DDoS attack. Earlier the original line of constant bit rate (CBR) was 2MB. When the bot infected systems performs UDP flooding on the other system of the network, it has been observed that the performance get degraded by 1.5, 1.3, 1.2, 1.4 MB. The degradation in the performance for the above mentioned scenario can be analyzed by the graph shown in figure 4.

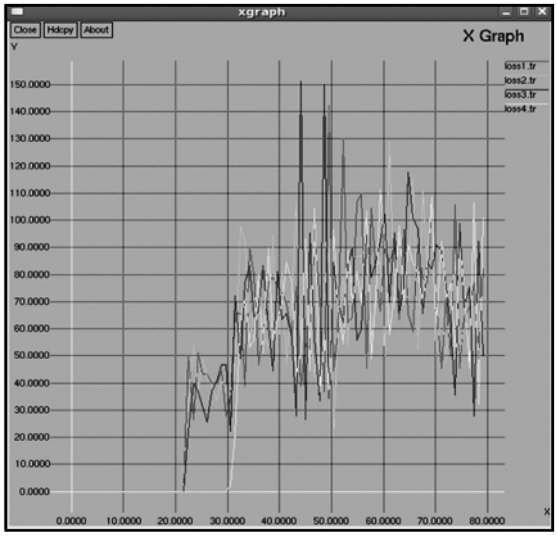

Fig. 4: Packet Drop Rate of Node 1, 2, 3 and 4

4. CONCLUSION

Most of the attack and fraudulent activities on the internet are carried by malware. Malware includes virus, worms, trojan, spyware and in recent times botnets. Flooding based attacks are the very serious threat to the network. Distributed Denial of Service (DDoS) attacks have become a large problem for users of computer systems connected to the Internet. Mainly, Internet servers which are providing vital services in the network must be protected from these types of attacks. In future, queuing theory can be applied to determine round trip time and various other performance parameters. By applying, queuing theory in our botnet simulation, we have measured the rate of packet drop of the infected nodes in the botnet.

REFERENCES

[1] Hang Chau, Network Security – Defense Against DoS/ DDoS Attacks.

[2] Wesley M. Eddy, Verizon Federal, "Defenses Against TCP SYN Flooding Attack", *The Internet Protocol Journal*, **9**, No. 4, December 2006.

[3] F. Lau, S. H. et al., "Distributed Denial of Service Attacks," *2000 IEEE Int. Conf. on Systems, Man, and Cybernetics*, Nashville, TN, October 2000.

[4] B. Saha and A, Gairola, "Botnet: An overview," *CERT-In WhitePaperCIWP-2005-05*, 2005.

[5] E. Cooke, F. Jahanian, and D. McPherson, "The Zombie Roundup: Understanding, Detecting and Disrupting Botnets", *In Proceedings of the Steps to Reducing Unwanted Traffic on the Internet (SRUTI 2005 Workshop)*, Cambridge, MA, July 2005.

[6] CERT Coordination Center, "Denial of Service Attacks," http://www.cert.org/homeusers/ddos.html.

[7] Stephen M. Specht, Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures", *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems*, pp. 543-550, September 2004.