Schemes For Detecting DDoS Attacks

Rohit Lodha 2015A7PS0040P
f2015040@pilani.bits-pilani.ac.in

Abstract

Distributed Denial of Service (DDoS) is an attempt to flood the bandwidth or resources of a targeted system making it unavailable by overwhelming it with traffic from multiple compromised systems. Since the incoming traffic originates from many different sources, it is almost impossible to stop the attack simply by blocking a single source.

With the exponential rise of Internet-based e-business and e-commerce, the disruption caused by DDoS attacks is more
critical than ever before. The attacker's single purpose is to reduce or eliminate the availability of a service provided over the Internet to its authentic users. This is accomplished either by exploiting the vulnerabilities in the software or network protocols, or by draining the consumable resources like bandwidth, computational time and memory of the victim. The first kind of attacks can be bypassed by patching-up outdated software and updating the host systems once in awhile. The latter kind is much more difficult to defend.

As reported by Arbor Networks, more than 2000 DDoS attacks are observed daily. Anyone can buy a week-long DDoS attack for $150 on the black market. Of all downtime incidents, one-third are attributed to DDoS attacks. Therefore, how to guard against these attacks and protect the access of genuine users has attracted attention from both industries and academia.

This paper aims to explore various defence mechanism and novel schemes to detect any type of DDoS attacks including preventive, reactive and source-tracking mechanisms, how are they applied, what are their limitations and how encryption mechanism can enhance the speed of detection.

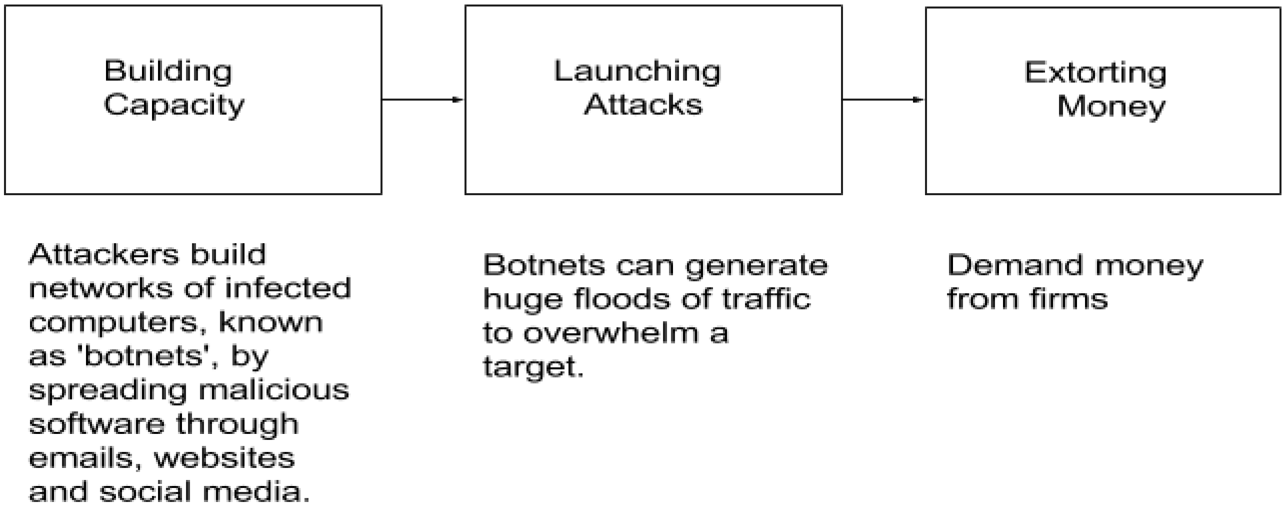
SYNOPSYS

Distributed Denial of Service (DDoS) is a type of DOS attack where multiple compromised systems(botnets), often infected with a Trojan, are used to target a single system to make an online service unavailable by overwhelming it with traffic. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

We can think of the DDoS attack as an analogy to a group of people crowding the entry door or gate to a mall, and not letting legitimate parties, who want to shop, enter into the mall, disrupting normal operations.

In today's world, the Internet is an essential part of our everyday life. Many important and crucial services like banking, shopping, transport, health, and communication are partly or completely dependent on the Internet. According to recent sources, the number of hosts connected to the internet is almost 400 million and there are currently more than 1 billion users of the Internet. Thus, any disruption in the operation of the Internet can be very inconvenient for most of us. The Internet was originally designed for openness and scalability without much concern for security, malicious users can exploit the design weaknesses of the internet to wreak havoc in its operation. It is not hard to picture the potentially catastrophic damage to a company that earns its revenue by online advertising if it were knocked offline, or to an online retailer if an unscrupulous competitor hired a criminal to launch an attack on the former's website at the height of the holiday shopping season.

DDos has recently emerged as one of the major threats to network security as evident from a series of attacks that shut down some of the world's most high-profile websites, like GitHub, Amazon, Twitter and Yahoo on October 21 when a Mirai botnet launched an attack against Dyn, an internet performance management company. Not only these big corporations but several public web properties and organizations affiliated with the Rio Olympics suffered a sustained DDoS attack that lasted for several months. These attacks are becoming big business.



Attackers build networks of infected computers, known as 'botnets', by spreading malicious software through emails, websites and social media.

Botnets can generate huge floods of traffic to overwhelm a target.

Demand money from firms

There are many types of DDoS attacks which can be grouped into the following three classes:

- **Traffic attacks:** Traffic flooding attacks send a huge volume of TCP, UDP and ICPM packets to the target. Legitimate requests get lost and these attacks may be accompanied by malware exploitation. Eg: TCP SYN flooding, ICMP flooding

- **Bandwidth attacks:** This DDoS attack overloads the target with massive amounts of junk data. This results in a loss of network bandwidth and equipment resources and can lead to a complete denial of service.
- **Application attacks:** Application-layer data messages can deplete resources in the application layer, leaving the target's system services unavailable.

Two of the most common and dangerous attacks are :

1. **The TCP SYN flooding -** It exploits the TCP's three-way handshake mechanism and its limitation in maintaining half-open connections. The attacker compromises machines and ordering them to send, at the same time, a stream of flooding SYN packets with inaccessible IP addresses to the victim' server, making it unavailable to other users. Since it is difficult to distinguish between legitimate SYN packets and attack SYN packets, these attacks are very hard to detect.
2. **Internet Control Message Protocol (ICMP) attack**- In this, the attacker flood large amount of ICMP_ECHOREQUEST packets in the network using target host IP Address, if the attacker does not forge the IP address then he will be affected because he will receive all the reply for the request sent. Since the IP address was forged now the target host will be affected.

Some of the common ways to detect and prevent DDoS attacks used worldwide are:

1. **Application front end hardware -** An intelligent hardware placed on the network before traffic reaches the servers to analyzes data packets as they enter the system
2. **Blackholing and sinkholing -** All the traffic to the attacked DNS or IP address is sent to a "black hole" or to valid IP address which analyzes traffic and rejects bad packets.
3. **Intrusion prevention systems(IPS)** - Monitors a network or systems for malicious activity or policy violation.

There are many research studies going on to detect, prevent and fight DDoS attacks. Some of them use Encrypted Marking based Detection And Filtering(EMDAF) while others use feature extraction, firewalls and cracking algorithms. There are also talks about using blockchain technology ending the DDoS once and for all.

The most important yet weird thing to note about these attacks is that in the beginning they were being brushed aside as the domain of bored teenagers engaging in some wanton cybervandalism but now they are the favorite tool of career cybercriminals and hacktivists.

The objective of the paper is to explore various defence mechanism and novel schemes to detect any type of DDoS attacks including preventive, reactive and source-tracking mechanisms, how are they applied, what are their limitations and how encryption mechanism can enhance the speed of detection. Since this topic is very vast, the report will discuss all the mechanism in a concise yet clear way and group the similar ones for better classification.