CLASSIFICATION OF DDOS ATTACKS

Dilmurod Tuhtanazarov*

*Senior Teacher,
“ Department Of Modern Ict”,
International Islamic Academy Of Uzbekistan,
Tashkent, UZBEKISTAN
Email id: Dtuxtanazarov@Gmail.Com

DOI: 10.5958/2249-7137.2022.00848.5

ABSTRACT

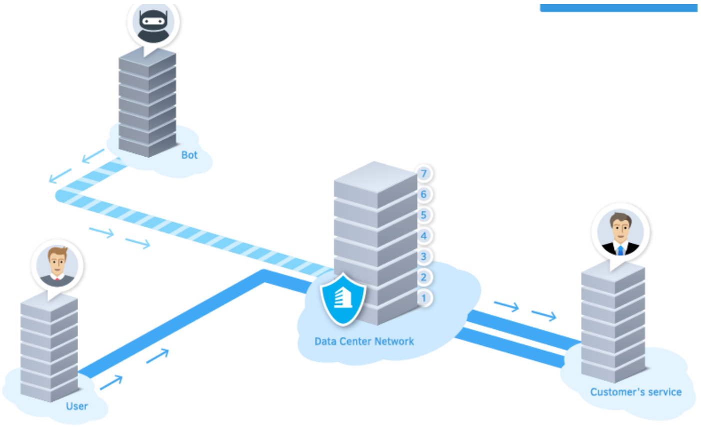
This article provides information about DDos attack and its types. Today's popular methods and types of DDos attack are described. There are no universal measures to protect against DDoS attacks, and a complex approach including hardware, software and organizational measures is required to solve such a problem.

KEYWORDS: *Ddos, Attack, Software, OSI Model, Request, Information, Confidentiality, Server, Network, Ethernet, Internet, Web Resource.*

INTRODUCTION

Cyber security concepts are based on availability, integrity and confidentiality. DOS attacks or denial of service attacks impose restrictions on access to information resources. An attack is successful if it has made the information resource unavailable. Large DDoS attacks or distributed denial of service attacks occur through a large number of malicious requests coming to the victim's equipment from different places on the planet. As a rule, such attacks are organized with the help of bots.

DDoS attacks can be divided into layers of the OSI model.



Pic. OSI model.

DDoS attacks occur on:

- 2nd level - channel;

- 3rd - network;

- 4th - transport;

- 7th - applied (application level).

The Main Part: At the moment, the world knows about the following attack methods:

- HTTP GET;

- HTTP POST;

- SYN-flood;

- UDP- flood;

- ICMP- flood;

- MAC- flood.

The most common type of traffic is HTTP requests. With the help of such requests, data is exchanged between the server and the user.

An HTTP GET request is a method that requests information from a server. With this request, the server can send some file, image, page or script.

HTTP GET flood is a DDoS attack method in which the attacker sends a powerful stream of requests to the server, which overflows its resource part. As a result, the server stops responding to any requests.

An HTTP POST request is a method based on placing data in the request body for further processing. The POST request encodes the information, puts it in the form, then sends the content to the server. This method allows you to transfer large amounts of information.

An HTTP POST flood is almost the same as a GET request. The bottom line is a high load on system resources, which can lead to a server shutdown.

SYN flood (TCP/SYN) establishes half-open connections to a host. When the victim receives a SYN packet on an open port, it must send back a SYN-ACK packet and establish a connection. After that, the initiator sends a response to the recipient with an ACK packet. Such connections remain half-open until the timeout expires, the connection queue overflows and new clients cannot connect to the server

UDP floods are most commonly used for broadband DDoS attacks. The advantage of this method is the ease of creating protocol 17 messages in different programming languages.

ICMP flood. The Internet Control Message Protocol (ICMP) is used primarily for error messages and is not used for data transmission. ICMP packets can accompany TCP packets when connecting to a server. ICMP flood is a DDoS attack method at the 3rd layer of the OSI model that uses ICMP messages to overload the attacked network channel.

MAC flood is a rare type of attack in which the attacker sends multiple empty Ethernet frames with different MAC addresses. Network switches consider each MAC address separately and, as a result, reserve resources for each of them. When all the memory on the switch is used up, it either stops responding or shuts down. On some types of routers, a MAC flood attack can cause entire routing tables to be deleted, thus disrupting the entire network.

There are currently no universal measures to protect against DDoS attacks. When solving such a problem, an integrated approach is required, which includes measures of a hardware, software and organizational nature.

CONCLUSION

If a web resource is attacked, the web server hardware resources must have some performance reserve, and distributed and redundant systems must be built as efficiently as possible. It is simply impossible to build effective protection without understanding the principles of DDoS operation. A large number of computers infected with malicious code are used to carry out DDoS attacks. These computers are united in botnets, which carry out DDoS attacks on the order of the attacker, and computer owners often do not even know about it.

BIBLIOGRAPHY:

1. DDoS attacks: types of attacks and levels of the OSI model. URL: https://firstvds.ru/technology/types-of ddos (Accessed 08/18/2020)

2. DDoS attack - what is it? URL: https://ddos-guard.net/ru/terminology/attacks/ddos-ataka (Accessed 08/18/2020)