ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 10, October 2022

Review on DDOS Attack and Its Global Effects and Prevention Measures

[1] Dharani Prasad S, [2] Brij Vishal Rajput, [3] Hasnain Shariff, [4] Chethan Shetty, [5] Agraz Agrawal, [6] Dr Pooja Nayak S

[1] [2] [3] [4] [5] Student, Department of Information Science and Engineering, DSATM, Bangalore, Karnataka, India.
[6] Faculty, Department of Information Science and Engineering, DSATM, Bangalore, Karnataka, India.
Corresponding Author Email: [1] prasadsdharani@gmail.com, [2] brijvishal.bv@gmail.com, [3] hasnainshariff7@gmail.com, [4] csshetty619@gmail.com, [5] agraz888agrawal@gmail.com, [6] pooja-ise@dsatm.edu.in

Abstract*— The present generation is wholly dependent on Data and Data services provided by the internet for global level information and for communication between different sources for all the system users. Hence the functioning of Internet is very important for all the users. One of the important strategies that Hackers employ to hinder the performance of the system is Distributed Denial-Of-Service attacks (DDOS). This paper solely focuses on the prevention measures taken to withstand DDOS attacks in which the hacker sends loads of traffic and obstructs the working of a system and burdens the system. The study of this research is to find various methods to avoids becoming a victim of DDOs attacks..

I. INTRODUCTION

In this kind of DDOs attacks (Denial of service), many individual computers with a single purpose of attacking an target with high level of abundant traffic to target a particular resource. The hosts that are targeted with this kind of threats are Websites, server or an individual system. The traffic maybe incoming messages, stream of requests or packets that slow down the targeting host.[1] These kinds of malicious acts are often carried out by individual hacker (Hacktivists) or an criminal organization rings and even government agencies. It is tough to identify DDOs attacks as even poor code, missing patches of code or unstable host systems, large number of legitimate requests to host seem like DDOs attacks or just an coincidental lapse or fall in systems performance.[4]

Working:

In most of the DDOS attacks typically the malicious attacker identifies and utilizes the critical vulnerability in the targeted system and marks it down as DDOS master system/Host. That system identifies other defenseless systems and achieves control over them and infects them with malware (virus) that affects the critical working of the whole network of systems. The master system can even bypass authentication security controls like identifying the default password on that system. [3] The network of computers or devices that are under the influence of hacker is referred to as zombie, or a bot. The malicious hacker creates a command-and control server to achieve control over all the host under the network that network is called as botnet or network of bots. The person in control of botnet is the bot master. The same term is used to represent the first computer in the bot-net.

Botnets can contain any number of bots/vulnerable systems; botnets can be of any number ranging from tens to hundreds or even thousands based on the extent of hacker's abilities have become common. There is no upper-bound limit to the number of bots in botnet. The target of these attacks are not always a sole host it may also result in harming the other devices in the network. The system used by the hacker also gets hindrance in resources because of generating and propagating heavy traffic.

Various Types of DDos attacks [2]:

There are classified mainly into 3 types of attacks:

1. Network-centric / volumetric attacks: These overload a targeted hosts resource by consuming available bandwidth with packet streams. An typical example of this kind of attack isa domain name system (DNS) amplification attack, which makes requests to a DNS server using the target's Internet Protocol (IP) address. The server then overwhelms the target with responses or replies to the requests.

2. Protocol attacks: These mainly target network layer or transport layer protocols using flaws in the protocols to overwhelm targeted resources. A SYN flood attack, for example, sends the target IP addresses a high stream of "initial connection request" packets using spoofed source IP addresses. This drags out the Transmission Control Protocol handshake, which is never able to finish because of the constant stream of requests.[2]

3. Application layer: In this method the operational database of the host gets overwhelmed with high volume of traffic/packets. This in turn results in denial of query requests from the host. one of the most widely used attack is HTTP flood attacks in which the server or the website of the host

ISSN (Online) 2394-2320

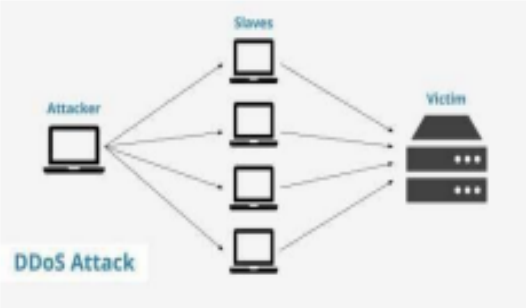
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 10, October 2022

gets jam-packed with request messages/packets.

Understanding The DDOS Attack

The communication between computers through interconnection on which the World Wide Web (WWW) relies, identifies itself as an easy victim for DDOS attacks In which the resources of that machine or network becomes unavailable for the users who are currently trying to access it, this attacks temporarily suspends or interrupts the services of the software. According to B. B. Gupta (2008) CERT defines the term "Denial of Service" as "Occupancy of limited resource or difficult to renew such as network bandwidth, data structure or memory of a system". An DDOS is an part of DOS attack in which the victim is flooded with abundant of attack packets and the attack takes place from multiple points simultaneously from various points. These attacks are also referred to as Distributed reflector DOS (DRDOS). These attacks are more dangerous than normal DOS attacks as identification becomes really tough and tricky. [3]



Popular DDoS Attack Trends on ISP Network:[3]

The significant number of attacks on ISP (Internet service provider) are based on network Infrastructure Attacks. These attacks do not only affect the system but effects all the system associated with the provider these attacks can create global or regional disturbances and harm cause harm at large impact. These includes:

• **Control Plane Attacks:** These are the attacks that usually occur against the routing protocols and affect the Lan system/devices, and can lead to service outage at small regions these attacks usually target protocols which are dynamic such as BGP (Border Gateway Protocol), EIGRP and OSPF and so on.

• **Management Plane Attacks:** In this trend hacker gains control over the configuration settings of the network and has the free will ability to alter any settings. This plane of attack includes many IPs like HTTP, SMTP, FTP, SSH, NTP etc.

• **Network Services Attacks:** The main objective of attacks like these are the basic services provided by the ISP. The domain name server (DNS) is a critical network service for ISP attacks. In this attack the hacker redirects the host to malicious websites and infects virus by interrupting the DNS server.

Defense Mechanisms:

The attacks are getting more and more Sophisticated over the years as Iot and Automation has increased. with increase in automation in institution and organization they are becoming more easy prey to hackers. Fully developed software is available for the Naïve user to make use of them to achieve easy interruption they can cause large scale damage with very little knowledge

• **Monitoring**: Cisco Monitoring team have developed an pattern detection tool which detects the pattern of the traffic sent by the DDOs attacker and ignores those malicious packets and discards them, this tool is very famous and used by many ISP's around the world to avoid DDOS. This tool uses system attributes like Source and Destination IP, Source and Destination port etc. To monitor and discard traffic in by-directionally all router interfaces must be monitored, along with the uplinks of the base routers.

• **Ingress/Egress Filtering:** It is a IP filtering method in which the ISP only allows the traffic to enter or leave the network only if the address of that traffic is in the expected IP address list. But the main drawback of this method is that Ingress-egress cannot be employed universally due to curse of dimensionality. The attacker can still sneak into the network by identifying the expected IP list and choosing an network without ingress-egress filters. hence these methods are not ideal for DDOS reduction or avoidance.

• **Black Holing:** Few ISP's employ remotely triggered blackholing also known as RTBH, by which they use the upslope systems to discard the redundant/malicious traffic, hence the traffic generated by the hacker won't even make it to the desired destination the disadvantage of this method is it becomes utterly useless if upstream system is offline.

• **Scrubbing:** Here the center of the scrubbing system has an inbuilt filter which automatically identifies and discards unwanted traffic, here only clean traffic makes the destination (ISP) the main drawback is that most of these centers are of high cost and maintenance is challenging..

• Proposed Methodology and solution:[3]

The best measures that have to be employed everywhere to avoid DDOS and to strengthen the security aspects to further level these steps have to be followed:

• Authentication of each and every user who access the computer should contain an unique username and password for verification.

• The host should employ some filtering interface to avoid traffic from each static connection possible.

• Host is recommended to allow access to only SSH connection-based users and avoid with Telnet on vtys.

• Employing vtys filters to prevent leakage of response information to public routers.

• Make use of TACACS (Terminal Access Controller Access Control System) for user authentication.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 10, October 2022

• Employing and using security labs or to set aside at least one extra router and server for individual services rather than implementing multiples services on the same servers. • Minimize the number of transits (ISP) ideally one.

• Grouping with other local ISPs to make use of their infrastructures like centers for scrubbing, band management and to set up better labs.

DDOS mitigation stages [5,4]:

1. Detection - The primary goal to identify the deviating pattern on traffic which might indicate the start of an DDOS attack. The most effective system will be that which identifies the DDOS assault as early as possible.

The main objective is to identify as early and not letting the system to become an DDOS assault victim.

2. Diversion- the goal of this to change path of the malicious traffic either by DNS or by BGP and a decision is made whether to filter or to discard the traffic. In this method DNS routing is always on to respond to these attacks quickly and it effectively avoids both application and network level attacks, whereas BGP routers are always-on or ondemand

3. Filtering- As soon as the pattern is identified which distinguishes it from legitimate traffic either by humans or API calls and response is employed. Responsiveness is a function of being able to avoid the attack without interfering with hosts experience. the main objective is to maintain transparency to website users.

4. Analysis- Here data analysts collect information about the attack, with an aim to identify the hacker and to increase resilience to those attacks. It makes use of system logs logging is legacy approach and does not have physical analysis. it provides complete visibility to attacks stream of traffic and avoids it completely.

II. CONCLUSION

DDoS Attacks are becoming a major component of a long term threat-costly campaign and the level of attack automation is increasing rapidly. Several effective measures are being taken by ISP's are fighting constantly against these attacks and still not been able to avoid these attacks completely they pose even higher order of risk and danger with increase in automation ISP's have to overcome their weaknesses like nonuniform architecture, poor and unstructured code, privacy policies and Roi to eradicate DDOs to some extent. With increase in AI-ML, IOT DOS protection is turning out to be a valuable market skill. Hence it seems completely impossible to eradicate DDOs from cyber security.

By following the methods and steps mentioned above organization might be able to fight DDOs much more effectively.

REFERENCES & WEBLINKS:

[1] https://journals.sagepub.com/doi/full/10.1177/1550147717741463
[2] International journal of Distributed Sensor Network
[3] https://blog.eccouncil.org/types-of-ddos-attacks-and-their-prevention-and-mitigation-strategy/
[4] http://users.eecs.northwestern.edu/~khh575/pub/pub/Report-DDoS-1.p
[5] International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013 https://www.researchgate.net/publication/258790077_DDoS_Attack_Prevention_and_Mitigation_Techniques_A_Review