DDoS Attack (Distributed Denial-of-service)

S.Mohan
Assistant Professor of Computer Science V.S.B. College of Engineering Technical Campus. Coimbatore-Kinadukadavu-Tamil Nadu –India-642 109.

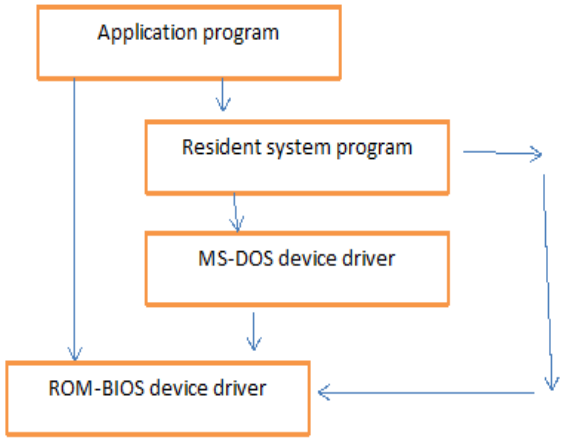
***Abstract*—A denial-of-service (DoS) attack is a malicious attempt to affect the availability of a targeted system such as a website or application to legitimate end user system. Typically, attacker generate large volume of packet or request ultimately over whelming the targeted system. in case of a Distributed denial-of-service (DDoS)attack and the attacker uses multiple compromised or control sources to generate the attack. the DDoS attack and it is crime in which the attack floods a secure with internet traffic to prevent uses from accessing connected online services and sites similar to other cybercrime like Sur vatting DDoS attack disrupt normal operation and less causes significant harm to individual and organization motivation for carrying out a DDoS vary wide as do the type of industrial and organization. Motivation for the carrying out a DDoS vary wide as to the type of individual and organization ague to preparate this form of cyber-attack some attack are carried out by disgruntled individual and hectivities wanting to take down a company's services simply make a statement have from by exploiting ague weakness or express disapproval this shutting down another business online operation to steel business away in the meantime , while preparators attack a company and install hostage ware or ransomware on their server DDoS attack are and rise and even some of largest global campaign or not immune to being (DDoS) attack can also be used by nation state to disrupt critical infrastructure and weakened public trust**

***Index Terms*—API, UDP, HTTP.**

I. INTRODUCTION

A DDoS (Distributed Denial-of-service)attack is a cyber-attack that over whelming a target server , service or network with massive traffic from multiple compromised devices making it unavailable to legitimate users the DDoS is malicious attempt to disrupt the normal function of the server , website or network by flooding it with exercise interact traffic from multi source unlike a standard DoS (Denial-of-Server) attack which originate from a single device a DDoS attack users multiple compromised device often forming a network called BOTNET. To originate over whelming traffic these device can include computer , server and IoT device infected with malware allowing attack to control these remotely a Distribute Denial-Of-Service (DDoS) attack is malicious attempt to crash or slow down targeted website , server or online service by flooding it with an over whelming rare of traffic unlike a standard and Denial-Of-Services(DoS) attack which typically come from single computer or IP address a DDoS attack uses multiple distributed system simultaneously the hacker infect thousand (million) of every day computers serve and IoT (Internet Of Thigs) devices which malware this network of infected remote controlled devices is called BOTNET . the attacker sends a remote command to every device in the BOTNET to direct massive amount of traffic of data requested towards single traffic IP address the targeted server or network run out of bandwidth, memory, or processing power making it slow unstable or completely offline for legitimate users.

DoS (Denial-of-service) Attack MEANS:

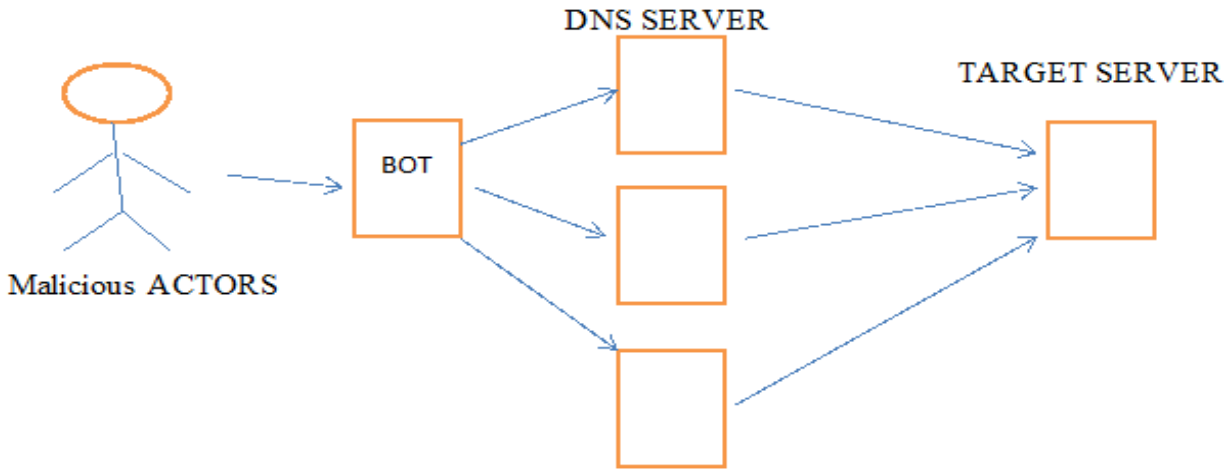


A Denial-of-service (DoS) attack is a cyber-attack that make a computer, website or network source unavailable to its legitimate users. the attacker typically floods the targeted system with excessive traffics, fake service request or malformed data packets to exhaust its hardware's and networks capacity. the server uses all its CPU, MEMORY or DISK space processing fake request learning from no room for real users. the incoming data volume exceeds the network maximum capacity causing server slow down or a computer crash. the single-originate source unlike a DDoS) Distributed Denial-Of-Service) attack which uses thousands of compromised devise or BOTNET. A standard DoS attack originates from a single system or connectors. \

II. TYPES OF DOS ATTACK

-Flood Attack: overwhelming a serve with massive volume of TCP,UDP,or ICMP packets such as sys Floods or ping of data.
-Buffer Overflow Attack; sending more data to a memory buffer then it can be handled to crash the system or execute the obituary code.
-Application LAYER attack: targeting the traffic web application (layer - 7) with partial are heavy request like slow to tie up server threats. the attacker send request that act as normal user to the target system application layers such as HTTP, DNS or SMTP exhausting its processing power and logics.
- Protocol Arrack; the attack exploits the weakness or flaws in the network protocol that the targeted system uses such as TCP, UDP, or ICMP coming it to malfunction or consumer resources unnecessarily

DDoS (Distributed Denial-of-service) Attack means :

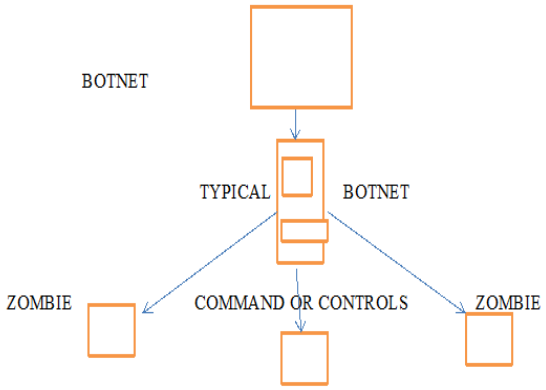


That is DDoS (Distributed Denial-Of-Service) attack is a cyber-attack when multiple compromised devices flood a largest system with traffic, making its unavailable to legislate users. A DDoS attack is a malicious attempt to disrupt the normal operation of the server , website , network or online service by over whelming it with traffic from multiple sources simultaneously unlike a standard denial – of -service (DoS) attack which originate from single device , DDoS attack uses thousand (million) of compromised device often forming a network called BOTNET to generate massive traffic this floods of request can exhaust bandwidth , CPU, memory or application resources carrying slow down , outage or complete server failure .

TYPES of DDoS Attacks:

- Volumetric attack: overwhelming network bandwidth using massive data traffic example UDP floods or DNS amplification.
- Protocol Attack: exploit weakness in network protocol to exhaust server or firewall resources Example SYS Floods.
- Application-Layer Attack: target specific application or service sending seemingly legitimate request to exhaust server resources example HTTP Floods.

ZOMBIE system



In this context of DDoS and DoS attack are zombie system refer to a compromised device that is part of BOTNET which is a network of multiple compromised devices controlled by a hacker. these devices are used to launch attack by flooding a targeted with traffic which can overwhelming the target sources and random it unavailable. the term - ZOMBIE -is used to describe the state of device that has been encrypted int o a BOTNET allowing it to be used for malicious activate without owners' knowledge.

III. BOTNET MEANS

A botnet is a network of computer infected with malwares and controlled by a malicious actor often referred to as a "BOT-HERDER "these infected devices known as BOT can be used various malicious activities, including – distributed Denial-of-Service attack.

BOTNET works:
BOTNET are created by infected devices through various method such as exploiting website volumetric, using Trojan horse malware or cracking weak authentication once device infected, it can be remotely controlled by the BOT-HERDER the infected devices may also attempt to propagate the malware to other devices in the network.

TYPES of BOTNET controller:
-client- server model: this model each bot connected to centralized server to receive the instruction. this model is easier to manage but has a single point of failure if the centralized server is disrupting the entire botnet can be taken down.

Peer-to-Peer (P2P) model:
This model eliminates a single point of failure by allowing each bot to act as both a client and a connected center this makes it harder to disrupt the BOTNET but also more complex to manage.
BOTNET driver (DDoS)attack can significance damage by overwhelming a target network or server with the flood traffic rendering it inaccessible to legitimate uses this attack can be monitored by various reason including activism, state – sponsored disruption or financial gain.

IV. DIFFERENCE: DDOS AND DOS ATTACK:

A DoS attack comes from a single source which a DDoS attack uses multiple distributed system (BOTNET) making DDoS attack faster herder to block and far more distributive. because both has (DoS & DDoS) attacker aim to over whelming a target with excessive traffic can service distributed they key difference lies in the number of sources used to generate the attack traffic

V. SOURCE ATTACK

DoS Attack: single system generates all malicious traffic
DDoS attack: multiple compromised system (BOTNET) co- ordinates the attack
TRAFFIC volume & impact;
DoS: lower traffic volume, moderate input
DDoS: massive traffic volume source and distribution and faster over load.
DIFFICULT of protect & BLOCKY:
DoS: easier to detect and block since traffic against from one location
DDoS: herder to detect and mitigate due to distributed sources that appear legitimate

TRACABLITY:
DoS: easier to trace the attack
DDoS: very difficult to trace between traffic comes from many organized devices
EXACT methods:
DoS: often uses simple swift or tools from one machine

DDoS; uses BOTNET controlled by a commands and controlled server. DoS attack is simple and easier to mitigate while DDoS attack is distributed more powerful and significantly harder to defend against due and their such a complexity.

VI. CLOUD AND IOT ATTACKED BY DDOS

Both cloud and IoT device are frequent target and primary pacificator in distributed denial-of-service.
-IoT attack TOOLS:
BOTNET in service to IoT device (such as smart camera router, and appliances) with default personal or weak severity are frequently hijacked by malwares to from massive BORNET. these botnets generate flood of traffic to crash extended target.
IoT as targets': IoT network and their management server are vulnerable to direct DDoS flood that are whelming the limited bandwidth and lower processing powers.

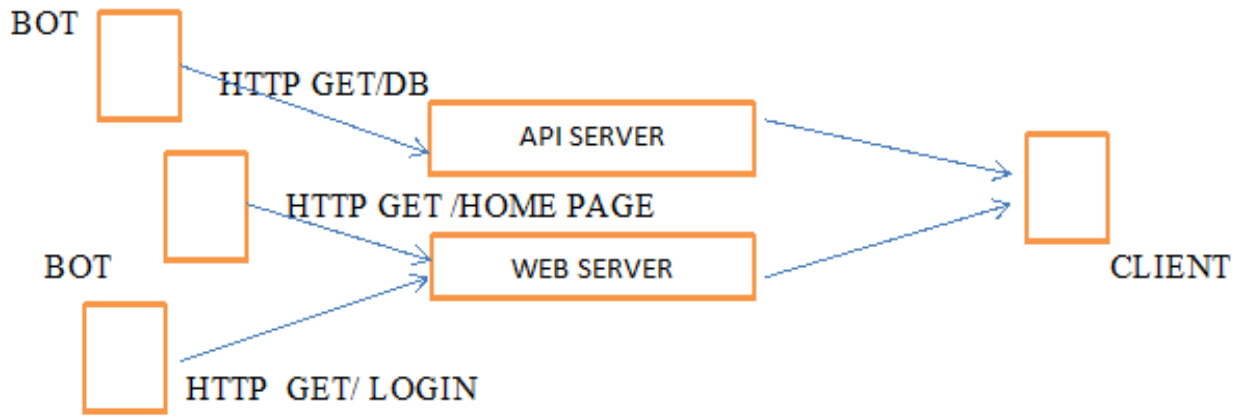
VII. CLOUD AS A TARGETS

Public tracing cloud service API data sum and web portal are heavily targeted by volumetric, protocol and application layer (layer 7) DDoS attack mend to distributed enterprises service.
CLOUD as a DEFENCE: cloud platforms (such as AWS, AZURE <and Google cloud) and edge provider (such as a wildly used to absorb and mitigated massive DDoS traffic through are searching and any cast and routing.

FIREWALL is DDoS:
A standard firewall block minor protocol floods and certain limits but it cannot stop large scale or volumetric distributing Denial-of-service (DDoS) attack state-based firewall easily run out of memory or session table capacity during massive BOTNET assaults requiring cloud scrubbing (DoS dedicated DDoS appliances).

FIREWALL instructions:
Firewall take active connection massive SYN or UDP floods fill up these connection table looking out legitimate users the traditional the traditional fire wall operates at network and transfer layer whereas operated web application fire wall (WAF) handle layer 7 HTTP /HTTPS flood the performance proving of malicious packet streams a fire wall CPU before it can drop them. in mitigates cap in coming request per source IP address to slow down automate BOT attempts the route traffic through like cloud flare Akamai or Fortinet DDoS protect to filler bad packet up stream user any cast routing to spread traffic or drop malicious traffic computing via black hole routing when under server attack the hybrid replacement place state less hardware (such as Arbor edge defense) in front of state full fire wall to absorb traffic spikes.

VIII. HTTP IN DDOS



An http floods in an application layer 7 distributed denial-of -service (DDoS) attack it our whelming less a web server or application with massive volume of standard HTTR GET or POST request, exhaust server CPU, memory and data base connection rather than network band width.

Looking traffic;
Unlike volumetric or protocol level attack (like SYN floods) that use malformed packets. HTTP floods use vapid well-formed request. this makes then hard to filter out without blocking real-user.

GET request:
Botnet repeatedly request static or dynamic resource (image, swift, web page) to free heavy rendering and database lookup.

POST request:
Attack such resources unlimited for submission or database heavily querying that demand high server - side processing.

HTTP rapid rest:
Advanced must like (CVE -202 – 44487) exploit stream multiplying by querying stream and immediately cancelling then with reset commands generally myths of request per seconds with minimal client efforts.

IX. CONCLUSION

A distributed denial-of-service (DDoS) is an assault a digital arbitrary by flooding server or network with traffic form multiple services financial losses broken certain trust and operation per analysis – proving that system availability is the core services method for modern business the DDoS attack core objective the goal is not necessarily to steel data directly, but to knock a service offline by exhausting down bandwidth, memory or CPU resources. the distributed sources unlike basic DoS attack use global BOTNET of compromised smart devices and server hard to block defending system struggle to tell the different between minimal use traffic and fake flood traffic. the basis's impact downtime trigger directly revenges loses high recovery cost and long-term brand damage. the main attack type volumetric attack and [protocol attack overwhelming network pipes and using share the data volumes (like UDP Floods) the exploit network layer weakness to freeze fire wall and route (like SYN protocol) It application layer Target web application with high frequency request that mimic real user (like HTTP FLOODS).

REFERENCES

[1]. S. Kumar, D. Singh, R. Singh, G. Gupta, and S. K. Singh, "An IoT-based secure transaction system using micro field communication," IOP Conference Series: Materials Science and Engineering, vol. 748, no. 1, Art. no. 012014, Feb. 2020.

[2]. S. Kumar, A. Negi, J. N. Singh, and A. Gaurav, "Brain tumor segmentation and classification using MRI images via fully convolutional neural networks," in Proceedings of the 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Oct. 2018, pp. 1178– [ending page missing].

[3]. S. A. Khanday, H. Fatima, and N. Rakesh, "Implementation of intrusion detection model for DDoS attacks in lightweight IoT networks," Expert Systems with Applications, vol. 215, Art. no. 119330, 2023.

[4]. K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges," Journal of Sensor and Actuator Networks, vol. 12, no. 4, Art. no. 51, 2023.

[5]. J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for DDoS attack detection in software-defined IoT (SD-IoT) networks," Engineering Applications of Artificial Intelligence, vol. 123, Art. no. 106432, 2023.

[6]. P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," Computers & Security, vol. 127, Art. no. 103096, 2023.

[7]. I. Priyadarshini, P. Mohanty, A. Alkhayyat, R. Sharma, and S. Kumar, "SDN and application layer DDoS attacks detection in IoT devices by attention-based Bi-LSTM-CNN," Transactions on Emerging Telecommunications Technologies, vol. 34, no. 11, Art. no. e4758, 2023.

[8]. F. M. Aswad, A. M. S. Ahmed, N. A. M. Alhammadi, B. A. Khalaf, and S. A. Mostafa, "Deep learning in distributed denial-of-service attacks detection method for Internet of Things

networks," Journal of Intelligent Systems, vol. 32, no. 1, Art. no. 20220155, 2023.

[9]. X. H. Nguyen and K. H. Le, "Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model," Internet of Things, vol. 23, Art. no. 100851, 2023.

[10]. W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks," IEEE Access, vol. 11, pp. 28934–28954, 2023.

[11]. "SDN-based detection and mitigation of DDoS attacks on smart homes," Computer Communications, vol. 221, pp. 29–41, 2024. [Author names missing].

[12]. P. Karthik, V. Vaddadi, L. P. Vakkapatla, L. Sridharala, S. Bulla, and S. Kavitha, "Comparative study of IDS against DDoS attack using machine learning algorithms," in Proceedings of the 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Feb. 2023, pp. 1568–1573.