Scientific Research Publishing

Journal of Information Security, 2023, 14, 464-471
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

The History, Trend, Types, and Mitigation of Distributed Denial of Service Attacks

Richard Kabanda, Bertrand Byera, Henrietta Emeka, Khaja Taiyab Mohiuddin

College of Engineering, University of New Haven, West Haven, USA
Email: rkabanda2015@gmail.com

How to cite this paper: Kabanda, R., Byera, B., Emeka, H. and Mohiuddin, K.T. (2023) The History, Trend, Types, and Mitigation of Distributed Denial of Service Attacks. *Journal of Information Security*, **14**, 464-471.
https://doi.org/10.4236/jis.2023.144026

Received: September 14, 2023
Accepted: October 24, 2023
Published: October 27, 2023

Abstract

Over time, the world has transformed digitally and there is total dependence on the internet. Many more gadgets are continuously interconnected in the internet ecosystem. This fact has made the Internet a global information source for every being. Despite all this, attacker knowledge by cybercriminals has advanced and resulted in different attack methodologies on the internet and its data stores. This paper will discuss the origin and significance of Denial of Service (DoS) and Distributed Denial of Service (DDoS). These kinds of attacks remain the most effective methods used by the bad guys to cause substantial damage in terms of operational, reputational, and financial damage to organizations globally. These kinds of attacks have hindered network performance and availability. The victim's network is flooded with massive illegal traffic hence, denying genuine traffic from passing through for authorized users. The paper will explore detection mechanisms, and mitigation techniques for this network threat.

Keywords

DDoS (Distributed Denial of Service Attacks) and DoS (Denial of Service Attacks), DAC (DDoS Attack Coefficient), Flood, SIEM (Security Information and Event Management), CISA (Cybersecurity and Infrastructure Security Agency), NIST (National Institute of Standards and Technology), XDR (Extended Detection and Response), ACK-SYN (Synchronize Acknowledge Packet), ICMP (Internet Control Message Protocol), Cyberwarfare

1. Introduction

Many businesses and companies have transformed digitally to gain a competitive advantage over others in the bid to discover new opportunities. Digital transformation has led to the explosion of internet-connected devices, ranging from IoT devices to smartphones, laptops, and servers. This has come along with several challenges which included the evolving cyber threat landscape.

Attacker knowledge has grown exponentially with attackers always ahead of the defenders. They have more options and time than ever before. Artificial intelligence and Machine learning tools have created an added advantage for hackers to launch very deadly attacks. Cybercriminals have access to advanced tools and techniques with many exploit kit options which have allowed them to identify and exploit vulnerabilities before even defenders discover them.

Attackers use their underground forums and dark web to share techniques and keep updated with the latest attack vectors. There is too much motivation whereby some hackers are being sponsored by the states hence changing and making the cybersecurity ecosystem trend sophisticated.

Amongst the deadly attacks launched is Denial of service attacks.

It should be noted that very large botnets which form the armies of hacked devices that are used to generate DDoS traffic have been created by Threat actors. As the botnets get bigger, the scale of DDoS attacks is also increasing making it expensive to mitigate them [1].

A denial of service (DoS) attack is a cyber-attack that intends to block legitimate or authorized users from accessing machines or network services by making the machine or network temporarily or indefinitely unavailable.

A DoS attack makes a machine or other devices unavailable to its legitimate users. The attack is executed by overwhelming the targeted machine with massive requests until the machine is flooded and cannot process normal traffic. In a DoS attack, a single computer launches the attack on a network or other client machines [2].

A DDoS attack is when the hacker sends multiple files that flood the traffic to a victim server. The server will be overwhelmed and hence stops functioning normally. With DDoS attacks, multiple systems distributed on the internet will simultaneously attack a single server [3].

2. The Origin and Trend for Distributed Denial of Service (DDoS) Attacks

The first-ever Denial of service (DoS) attack happened in 1974 and was executed by David Dennis who was 13 years old. He was a university student from the University of Illinois. Dennis effectively succeeded in bringing down 31 PLATO computer terminals. It was during an experiment where he wrote a program, however, as such there was no legal implication. The hackers around then adopted the principle and wrote more complex codes for cyber selfish reasons to come up with DDoS attacks [4].

These attacks continue to evolve. For example, in 1996, Panix company, the third oldest Internet service provider in the world based in New York USA, was affected by an SYN flood DDoS attack. Using these fake SYN packages, the hacker interrupted service delivery and network performance by using a spoofed IP address to overwhelm the company's servers. It was reported that the server stopped processing actual requests. Panix company took a full 36 hours to recover from this attack which was regarded to be the major DDoS attack at that time [5].

In 1999, a cybercriminal managed to overwhelm the network of the University of Minnesota with a massive UDP flood attack for more than 48 hours. This attack sent a signal to the public that DDoS attacks were for real, and companies had to take note of them with proper mitigation actions [5].

Reuters which is a leading news agency reported that a giant tech company's server in Russia called Yandex was attacked by a major distributed denial-of-service (DDoS) attack known to be one of the largest in internet history with a devastating 22 million requests per second which were all repelled by Russia's Yandex [6].

Constantin. (2016, June 28) PC World reported that "25,000 CCTV cameras and digital video recorders were compromised and used to execute DDoS attacks." It is said that attackers sent 50,000 HTTP requests per second to flood and overwhelm the target [5].

Wikipedia, Google revealed one of the largest DDoS attacks where they experienced an attack with a volumetric peak of 2.54 Tb/s on September 17, 2020. [7].

However, in 2022, Microsoft mitigated the largest DDOS attack ever in the History of the internet with a peak of 3.47Tbps DDoS Attack [8].

U.S. Cybersecurity and Infrastructure Security Agency in June 2023, a warning was issued to the public about the massive and continuing distributed denial-of-service (DDoS) attacks towards USA organizations across multiple industries. If the trend continues like this, then the public should be reminded that DDoS attacks are continuing to get stronger and more advanced hence, organizations should develop standard operating procedures to stop cybercriminals from DDoS attacks [9].

A 7th Layer DDoS attack was launched against Microsoft services of Azure, one Drive, and Outlook by a threat actor called Storm-1359 commonly known as Anonymous [10].

DDoS attacks have further evolved and are used as weapons in cyber warfare. For example, Aaron *et al.* 2009, May 2007, there was a misunderstanding that arose between Estonia and Russia. This was because Estonia disallowed the construction of an oil pipeline to Germany through its land. This issue annoyed the Russian government for which they took efforts to disrupt the economy of Estonia. Russia used all the known traditional weapons and methods such as transportation and cut-off supply lines. It was in this conflict that Russia introduced a new tactic that was referred to as cyber warfare where DDoS attacks were launched against the Estonian government. This incapacitated the Estonian government from running normal functions.

The innovation of Internet of Things (IoT) and their vast connectivity around the universe has improved efficiency and productivity. However, it has also harmed the digital infrastructure whereby it is a known enabler for the increased DDoS attacks. The security of IoT devices has proved to be weak. This has made them vulnerable to such attacks whereby cyber criminals have utilized them to send out heavy unauthorized traffic. This is because cyber criminals hijack IoT devices in very large numbers to create vast botnets hence significantly increasing the amount of data from gigabytes to terabytes that a cybercriminal could send.

3. Importance of DDoS Attacks to Cyber Criminals

The goal of DDoS to cyber criminals is to overload the system resources and hence bring it down, crash or become vulnerable due to massive requests. The design of the internet largely contributes to the success of DDoS attacks with several devices interconnected.

Cyber criminals use DDoS attacks for blackmail, for example, they may request system owners or website owners to pay a ransom fee for them to stop any DDoS attack.

Cyber criminals use DDoS attacks for competitive advantage, for example, some companies may use them against rival businesses.

Cyber criminals have used DDoS attacks for activist behavior for protests and upstaging.

4. Indicators for DDoS Attacks

Below are some of the indicators of a DDoS incident.

a) One sign of a DDoS attack is usually slow network performance. For example, the user will experience slowness in accessing a website or opening files.

b) Monitoring may show high processor and memory utilization.

c) Applications may perform unusually slowly.

d) DDoS attacks may be characterized by abnormally high network traffic.

e) Websites and applications become unavailable and inaccessible.

5. Examples of DDoS

5.1. SYN-Flood

SYN-flood, the attacker will bombard massive traffic with TCP SYN packets from spoofed source IP addresses toward a victimized target. The spoofed IPs may be one or many. The victimized source will then set up communication back to the attacker with SYN packets by sending ACK-SYN packets to the spoofed IP addresses. A spoofed IP address will not respond as it should have been with normal ACK. The result will be the creation of a half-open connection which will be queued subsequently for a given period that will in turn exceed the threshold of the awaiting connections to drop all subsequent requests hence, leading to the DDoS to the authorized users. The cybercriminals will intend to overutilize all the resources of the victim to make it unresponsive to requests from authorized users [11].

5.2. Ping of Death

"The Ping of Death sends fragmented ICMP Echo Requests that, once reassembled, are larger than the maximum size of an IP packet more than the specified IP limit (65536 bytes) are sent to the victim machine hence making it to hang, reboot or crash" [12].

5.3. DNS Flood

This is an example of a DDoS attack where the cybercriminal floods Domain Name System (DNS) servers to antagonize the resolution of the resource records of a zone and its sub-zones. This kind of attack is one of the toughest DDoS attacks because its detection and prevention are very difficult. During DNS flooding, a spoofed IP address will send a large number of DNS requests to the victim server machine. The request packets mimic a real DNS request and are very hard to distinguish from legitimate ones. The fact that the server must serve all the incoming DNS requests, it will run out of resources. All the server's existing I/O bandwidth will be consumed until it is completely exhausted [12].

5.4. Smurf Attack

During the "smurf" DDoS attack, the cybercriminal attacker sends a spoofed IP address to the broadcast address of the network. The packet will be distributed to all hosts on the network in that subnet. A packet that the attacker sends out is an ICMP echo request and the victimized hosts will respond with an ICMP echo reply to the target system. The attacker sends out one packet and generates 254 responses. If the attacker sends out the spoofed packets to many hosts or networks of computers, the targeted host will become overwhelmed and hence crash, shut down, or reboot to deny service to the authorized users [11].

5.5. Land Attack

It is another denial-of-service attack where the cybercriminal attacker will manipulate and spoof the source and destination IP addresses to look the same. When a vulnerable machine receives the message from the attacker, it will reply to the destination address in effect sending the packet for reprocessing in an infinite loop. The vulnerable machine will freeze because of the indefinite consumption of the CPU [12].

5.6. Mail Bomb Attack

In a Mail bomb attack, the cybercriminal attacker floods emails to the victim server causing the mail servers queue to get overloaded which makes the server fail in return. To detect a mail bomb attack, the intrusion detection system may look for many email messages all coming from or sent to a particular user within a given threshold of time. For example, the firewall rule may be configured to fire if mail messages destined to the SMTP port 25 for an established TCP session exceed 850 emails/second.

5.7. HTTP Flooding

In HTTP flooding, a three-way handshake is established by a connection from the cybercriminal attacker. This is followed by high-volume HTTP requests destined for the server to overwhelm its resources in terms of CPU, Memory, and bandwidth. Too much saturation of HTTP GET or POST requests will make the target unable to respond to the normal traffic hence causing a denial of service to any additional requests from legitimate users.

6. Mitigation for DDoS

To mitigate and encounter the challenges that come along with DDoS attacks, Security professionals will require a comprehensive approach that addresses cyber threats at all layers. It is devastating that as much as the organizations have hardened their defense mechanisms, cybercriminals have proved to be in front of the defenders whereby they have in turn responded with newer attack types targeting multiple applications and services.

Mitigation of DDoS attacks should include human firewalling with effective collaborative efforts within the cybersecurity ecosystem. This should include sharing threat intelligence information about attack vectors and learning from each other's experiences to stay up to date with the latest attack vectors. Develop strategies to counter DDoS attacks effectively as a team. This may include cooperation between organizations, internet service providers (ISPs), and law enforcement agencies.

CISA advised companies to contact their ISP to determine if their network was under a direct attack or there was an outage on their side and indirectly you are a victim. Communication with your ISP about the findings is very crucial to stop DDoS attacks. The ISP may then advise on the proper action to take. y may be able to advise you on an appropriate course of action [13].

Companies should employ load balancers and firewalls to help protect data from such attacks. These will reroute traffic to other servers and reduce single points of failure and add resiliency to the server data. The firewall blocks unwanted traffic and manages requests made at a definite rate. It checks for multiple attacks from an IP.

Infinity capacity allocates more bandwidth and resources to prevent clogging of data, although this is very expensive and not recommended.

Companies may deploy redundancy technologies. With redundancy, a device or data will be duplicated or mirrored to prevent it from becoming lost or unavailable. In this case, if the primary infrastructure is bombarded with DDoS attacks, then the secondary infrastructure will provide a fail-safe the organization can shift to as the team works out the possibility to stop DDoS.

Monitoring is one way to mitigate DDoS. Organizations should deploy SIEM and XDR to combat Security information and event management. According to Microsoft, SIEM will help companies to detect, analyze, and respond to security threats before they destabilize business operations. It provides real-time threat identification and response [10].

Making use of intrusion detection prevention systems (IDPS) like SNORT can mitigate almost all types of DDoS. Once SNORT rules are configured appropriately, content matching and protocol analysis will detect attacks. For example, a snort rule may be designed to identify the ping of death packets whereby the size of the ICMP packet is measured and if it is found to be larger than a certain threshold of bytes, the rule executes [12].

For DNS flooding, the Snort rule may be designed to fire when the number of DNS requests to the DNS server exceeds a chosen threshold for example if it exceeds 1000 requests per second.

Furthermore, a rule may be configured to detect land attacks, for example, a Snort rule with the keyword "sameip" is used in the rule which checks and compares the source and destination values of IP address to see if they are the same. The rule will be fired if the condition is true.

To detect HTTP flooding, a Snort rule checks for every established TCP session, the number of GET requests received by the server. The snort rule will be fired if the number of UDP packets per second is more than 1500 [12].

To mitigate Layer 7-based DDoS attacks, it is recommended to use protection services such as a Web application firewall (WAF) [10].

Other measures to mitigate DDoS include patching, and hardening systems, for instance, disabling and uninstalling any applications and services that are not needed on a server to reduce the chances of the criminal exploiting or launching DDoS. Use strong passwords. Companies may migrate to cloud service providers with advanced security features to detect and stop DDoS attacks.

7. Conclusions

What the future holds for DDoS attacks is in a bad state. The current trend shows that DDoS attacks will only become more massive, with frequency. The creation of Internet of Things (IoT) devices with the deployment of faster internet technologies like 5G across the world has turned out to be deadly. During the recent pandemic of COVID-19, many companies underwent digital transformation which made them potential targets for DDoS hence registering an exponential increase in these attacks.

Current research shows that DDoS criminal attacks are on the rise with the most organizations trying to protect their data and information from intruders and hacking criminals. The attacker's knowledge has increased. It should be noted that cybercriminals are now using cloud technologies to effectively execute DDoS. However, organizations must consider embracing new technologies, tactics, and methods used by hackers, to safeguard their information and data.

A DDoS Attack Coefficient (DAC) was developed by NetScout Systems, Inc., which is one of the providers for application performance and management products. The DAC showed that in the middle of 2020, there were over 4 million DDoS attacks registered which translated into a 15% increase in comparison with the previous year. DAC is defined as the amount of DDoS traffic that crosses the internet in each country or region at any one minute [5].

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Cisco Annual Internet Report (2018-2023) White Paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[2] Neil, I. (2018) CompTIA Security + SYO-501 Certification Guide. 2nd Edition, Packt Publishing, Mumbai.

[3] Wang, J. and Kissel, Z. (2015) Introduction to Network Security: Theory and Practice. 2nd Edition, Wiley, Singapore.

[4] Rafter, D. (2022) Emerging Threats: What Are Denial of Service (DoS) Attacks? DoS Attacks Explained. https://us.norton.com/blog/emerging-threats/dos-attacks-explained#

[5] Davis, R. (2021) The History and Future of DDoS Attacks. Cybersecurity Magazine. https://cybersecurity-magazine.com/the-history-and-future-of-ddos-attacks/

[6] Reuters (2018) Russia's Yandex Says It Repelled Biggest Ddos Attack in History. https://www.reuters.com/technology/russias-yandex-says-it-repelled-biggest-ddos-attack-history-2021-09-09/

[7] Denial-of-Service Attack. In Wikipedia. https://en.wikipedia.org/wiki/Denial-of-service_attack

[8] Klotz, A. (2022) Microsoft Fends off 3.47 Tbps DDOS Attack on Azure Servers. https://www.tomshardware.com/news/microsoft-mitigates-record-ddos-azure-attack

[9] Cybersecurity and Infrastructure Security Agency (2023) DoS and DDoS Attacks against Multiple Sectors. https://www.cisa.gov/news-events/alerts/2023/06/30/dos-and-ddos-attacks-against-multiple-sectors

[10] Microsoft Corporation (2023) Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks. https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks/

[11] Conklin, A.W., White, G., Cothren, C. and Davis, R.L. (2021) Principles of Computer Security: Comptia Security + and beyond. 6th Edition, McGraw Hill, New York, 587-588, 589.

[12] Gupta, A. and Sharma, L.S. (2019) Mitigation of DoS and Port Scan Attacks Using Snort. *International Journal of Computer Sciences and Engineering*, **7**, 248-258. https://doi.org/10.26438/ijcse/v7i4.248258

[13] Cybersecurity and Infrastructure Security Agency (2022) Understanding and responding to Distributed Denial-of-Service Attacks. https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf