

A COMPARATIVE STUDY ON DoS AND DDoS ATTACK

BY

Mst. Genius Yesmin Laboni

ID: 181-15-10657

Humayia Haque Himu

ID: 181-15-11101

Aklima Akter

ID: 181-15-10811

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Md. Abbas Ali Khan

Sr. Lecturer

Department of CSE

Daffodil International University

Co-Supervised By

Mr. Gazi Zahirul Islam

Lecturer

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

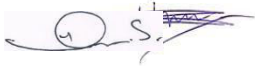
DHAKA, BANGLADESH

JANUARY, 2022

APPROVAL

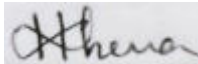
This project is titled “A COMPARATIVE STUDY ON DoS AND DDoS ATTACK”, submitted by Name: **Mst. Genius Yesmin Laboni (181-15-10657), Humayia Haque Himu (181-15-11101), Aklima Akter (181-15-10811)** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfilment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held in JANUARY, 2022.

BOARD OF EXAMINERS



Chairman

Dr. S.M Aminul Haque
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Internal Examiner

Most. Hasna Hena (HH)
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Internal Examiner

Md. Jueal Mia (MJM)
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



External Examiner

Dr. Md Arshad Ali

Associate Professor

Department of Computer Science and Engineering

Hajee Mohammad Danesh Science and Technology University

DECLARATION

I hereby declare that this project has been done by us under the supervision of **Md. Abbas Ali Khan, Department of CSE** Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for the award of any degree or diploma.

Supervised by:



Md. Abbas Ali Khan

Sr. Lecturer

Department of CSE

Daffodil International University

Co-Supervised By:


Md. Tarek. Habib

Lecturer

Department of CSE

Daffodil International University

Submitted by:



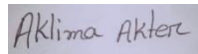
Mst. Genius Yesmin Laboni

ID: 181-15-10657

Humayia Haque

Humayia Haque Himu

ID: 181-15-11101



Aklima Akter

ID: 181-15-10811

Department of CSE

Daffodil International University

ACKNOWLEDGEMENT

At first, we would like to thank all people who have helped and inspired us during our thesis study. We are heartily thankful to our supervisor, Md. Abbas Ali Khan, Department of CSE, Daffodil International University, Dhaka, whose encouragement, guidance, and support from the initial to the final level enabled us to develop an understanding of the subject.

Besides our supervisor, we are grateful to Professor Dr. Touhid Bhuiyan and Head, Department of CSE, for his kind help to finish my project and also to other faculty members and the staff of the CSE department of Daffodil International University, for their kind co-operation and guidance during our thesis.

I would like to thank our entire coursemate in Daffodil International University, who took part in this discussion while completing the course work.

Lastly and most importantly we would like to thank our family: our parents for their unflagging love and support throughout our life; this thesis is simply impossible without them. We would like to dedicate this thesis to them.

ABSTRACT

A DoS attack is a denial of service attack, in this attack, a computer sends a massive amount of traffic to a victim's computer and shuts it down. A Dos attack is an online attack that is used to make the website unavailable for its users when done on a website. This attack makes the server of a website down, which is connected to the internet by sending a large number of traffic to it. In DDoS attack means distributed denial of service in this attack dos attacks are done from many different locations using many systems. During a DDoS attack, multiple systems target a single system with malicious traffic. By using multiple locations to attack the system the attacker can put the system offline more easily. We also prevent by using Know network's traffic, Organize a DDoS Attack Response Plan, Create a Denial of Service Response Plan, Make your network resilient, Practice good cyber hygiene, Scale-up your bandwidth, Take advantage of anti-DDoS hardware and software, Move to the cloud, Know the symptoms of an attack, Outsource your DDoS protection, Monitor for unusual activity, Perform a Network Vulnerability Assessment, etc.

TABLE OF CONTENTS

CONTENTS	PAGE
Board of Examiners	I
Declaration	II
Acknowledgements	III
Abstract	IV
CHAPTER 1: INTRODUCTION	5-6
1.1 Introduction	5
1.2 Objective	6
1.3 Motivation	6
1.4 Expected Outcome	6
CHAPTER 2: DDoS ATTACK CLASSIFICATION	7-16
2.1 Infrastructure Layer Attacks	7
2.2 Application Layer Attacks	7
2.3 DoS AND DDoS ATTACKS OCCUR	8
2.4 BROAD TYPES OF DoS AND DDoS ATTACKS	9
2.5 MOST COMMON FORMS OF DDoS ATTACKS	10,11
2.6 WHAT HAPPENS DURING A DDoS ATTACKS	12
2.7 WHY HAVE DDoS ATTACKS INCREASED	12,13
2.8 DIFFERENCE BETWEEN DoS AND DDoS ATTACKS	14
2.9 A BRIEF HISTORY OF DDoS ATTACKS	15
2.10 TOPMOST FAMOUS DDoS ATTACKS	16
CHAPTER 3: BEING TARGETED WITH DDoS	17

CHAPTER 4: PREVENT DoS AND DDoS ATTACKS **18-23**

4.1	Organize a DDoS Attack Response Plan	18
4.2	Secure your Infrastructure with DDoS Attack Prevention Solutions	18
4.3	Perform a Network Vulnerability Assessment	19
4.4	Identify Warning Signs of a DDoS Attack	19
4.5	Adopt Cloud-Based Service Providers	20
4.6	Know your network's traffic	20
4.7	Create a Denial of Service Response Plan	20
4.8	Make your network resilient	21
4.9	Practice good cyber hygiene	21
4.10	Scale up your bandwidth	22
4.11	Take advantage of anti-DDoS hardware and software	22
4.12	Move to the cloud	22
4.13	Know the symptoms of an attack	22
4.14	Outsource your DDoS protection	23
4.15	Monitor for unusual activity	23

CHAPTER 5: DDoS MITIGATION TECHNIQUES **24-30**

5.1	Classify legitimate traffic vs. DDoS attacks	24
5.2	Avoid becoming a bot	25
5.3	Reducing Attack Surface	25
5.4	CDNs	26
5.5	Black Hole Routing	26
5.6	Rate Limiting	27
5.7	WAF	27
5.8	Scale	27
5.9	Stages Of DDoS Mitigation	28
5.10	DDoS mitigation service	29,30

CHAPTER 6: SOME DoS vs. DDoS ATTACKS FAQs **31**

- 6.1 How to improve security using a Content Delivery Network (CDN)? 31
- 6.2 What is the detection process for a DDoS attack? 31
- 6.3 Can you trace a DDoS attack? 31
- 6.4 Does a DDoS attack damage hardware? 31

CHAPTER 7: CONCLUSION **32**

REFERENCES **33**

CHAPTER 1

INTRODUCTION

1.1 Introduction

In today's scenario, everyone is using the Internet to communicate with each other. Internet is not limited only to webmail and chat but also extended to the field of education, business, media, and many more. Day by day, we are becoming more and more dependent on the Internet, which makes our life easier. It is changing our way of communication, business model, and even everyday life.

Now question is, whether it is safe to deal with each and everything using the Internet, whether it is secure enough. The answer is 'no' as we are not fully safe using the Internet. This is because, as the Internet grows, the number of attacks also increases. If we analyze all the records, we will find that a DDoS attack is one of the most common and major threats to the Internet.

This attack becomes more dangerous when it uses many computers to launch a coordinated DoS attack against one or more targets. It uses client-server technology and is called DDoS. This attack is launched in a very coordinated manner in which it uses many compromised computer machines, also known as zombies, to send a useless traffic flow to overload the victim's resources. The goal of the DDoS attack is personal, popularity, and material gain. Most of the DDoS attacks are performed by organized criminals targeting financial institutions, e-commerce, gambling sites, etc.

Now, we can be told "All DDoS = DoS, but not all DoS = DDoS."

A DoS attack is a denial of service attack where a computer is used to flood a server with TCP and UDP Packets.

A DDoS attack is one of the most common types of DoS attacks in use today. During a DDoS attack, multiple systems target a single system with malicious traffic. By using multiple locations to attack the system the attacker can put the system offline more easily. Such as a website or application, to legitimate end-users.

1.2 Objective

The objective of a DDoS attack is to prevent legal users from accessing your website. For a DDoS attack to be successful, the attacker needs to send more requests than the victim server can handle. Another way successful attacks occur is when the attacker sends faked/false requests.

1.3 Motivation

The main goal of an attacker that is leveraging a denial of service (dos) attack method is to disrupt website availability. The website can become slow to respond to legal requests. The website can be disabled fully, making it impossible for legal users to access it.

1.4 Expected Outcome

During a DDoS attack, multiple systems target a single system with malicious traffic. By using multiple locations to attack the system the attacker can put the system offline more easily.

CHAPTER 2

DDoS ATTACK CLASSIFICATION

While thinking about mitigation techniques against these attacks, it is useful to group them as Infrastructure layer (Layers 3 and 4) and Application Layer (Layer 6 and 7) attacks [1].

2.1 Infrastructure Layer Attacks

Attacks at Layer 3 and 4, are typically categorized as Infrastructure layer attacks. These are also the most common type of DDoS attack and include vectors like synchronized (SYN) floods and other reflection attacks like User Datagram Packet (UDP) floods. These attacks are usually large in volume and aim to overload the capacity of the network or the application servers. But fortunately, these are also the type of attacks that have clear signatures and are easier to detect.

2.2 Application Layer Attacks

Attacks at Layer 6 and 7, are often categorized as Application layer attacks. While these attacks are less common, they also tend to be more sophisticated. These attacks are typically small in volume compared to the Infrastructure layer attacks but tend to focus on particular expensive parts of the application thereby making it unavailable for real users. For instance, a flood of HTTP requests to a login page, or an expensive search API, or even Word press XML-RPC floods also known as Word press pingback attacks.

2.3 DoS AND DDoS ATTACKS OCCUR

Whether it is a DoS or DDoS attack, there are many nefarious reasons why an attacker would want to put a business offline. In this section, we'll look at some of the most common reasons why DDoS attacks are used to attack enterprises [2]. Common reasons include:

2.3.1 Ransom – Perhaps the most common reason for DDoS attacks is to extort a ransom. Once an attack has been completed successfully the attackers will then demand a ransom to halt the attack and get the network back online. It isn't advised to pay these ransoms because there is no guarantee that the business will be restored to full operation.

2.3.2 Malicious Competitors – Malicious competitors looking to make a business out of operation are another possible reason for DDoS attacks to take place. By taking an enterprise's network down a competitor can attempt to steal your customers away from you. This is thought to be particularly common within the online gambling community where competitors will try to put each other offline to gain a competitive advantage.

2.3.3 Hacktivism – In many cases, the motivation for an attack won't be financial but personal and political. It is not uncommon for Hacktivism groups to put government and enterprise sites offline to mark their opposition. This can be for any reason that the attacker deems to be important but often occurs due to political motivations.

2.3.4 Causing Trouble – Many attackers simply like causing trouble for personal users and networks. It is no secret that cyber attackers find it amusing to put organizations offline. For many attackers, DDoS attacks offer a way to prank people. Many see these attacks as 'victimless' which is unfortunate given the amount of money that a successful attack can cost an organization.

2.3.5 Disgruntled Employees – Another common reason for cyber-attacks is disgruntled employees or ex-employees. If the person has a grievance against your organization then a DDoS attack can be an effective way to get back at you. While the majority of employees handle grievances maturely there is still a minority who use these attacks to damage an organization they have personal issues with.

2.4 BROAD TYPES OF DoS AND DDoS ATTACKS

There are several broad categories that DoS attacks fall into for taking networks offline [2]. These come in the form of:

2.4.1 Volumetric Attacks – Volumetric attacks are classified as any form of attack where a target network's bandwidth resources are deliberately consumed by an attacker. Once network bandwidth has been consumed it is unavailable to legitimate devices and users within the network. Volumetric attacks occur when the attacker floods network devices with ICMP echo requests until there is no more bandwidth available.

2.4.2 Fragmentation Attacks – Fragmentation attacks are any kind of attack that forces a network to reassemble manipulated network packets. During a fragmentation attack the attacker sends manipulated packets to a network so that once the network tries to reassemble them, they can't be reassembled. This is because the packets have more packet header information than is permitted. The result is packet headers that are too large to reassemble in bulk.

2.4.3 TCP-State Exhaustion Attacks – In a TCP-State Exhaustion attack, the attacker targets a web server or firewall in an attempt to limit the number of connections that they can make. The idea behind this style of attack is to push the device to the limit of the number of concurrent connections.

2.4.4 Application Layer Attacks – Application layer or Layer 7 attacks are attacks that target applications or servers in an attempt to use up resources by creating as many processes and transactions as possible. Application layer attacks are particularly difficult to detect and address because they don't need many machines to launch an attack.

2.5 MOST COMMON FORMS OF DDoS ATTACKS

As you can see, DDoS attacks are the more complex of the two threats because they use a range of devices that increase the severity of attacks. Being attacked by one computer is not the same as being attacked by a botnet of one hundred devices!

Part of being prepared for DDoS attacks is being familiar with as many different attack forms as you can. In this section, we're going to look at these in further detail so you can see how these attacks are used to damage enterprise networks [2].

DDoS attacks can come in various forms including:

2.5.1 Ping of Death – During a Ping of Death (POD) attack the attacker sends multiple pings to one computer. POD attacks use manipulated packets to send packets to the network which have IP packets that are larger than the maximum packet length. These illegitimate packets are sent as fragments. Once the victim's network attempts to reassemble these packets network resources are used up, they are unavailable to legitimate packets. This grinds the target network to a halt and takes it out of action completely.

2.5.2 UDP Floods – A UDP flood is a DDoS attack that floods the victim network with User Datagram Protocol (UDP) packets. The attack works by flooding ports on a remote host so that the host keeps looking for an application listening at the port. When the host discovers that there is no application it replies with a packet that says the destination wasn't reachable. This consumes network resources and means that other devices can't connect properly.

2.5.3 Ping Flood – Much like a UDP flood attack, a ping flood attack uses ICMP Echo Request or ping packets to derail a network's service. The attacker sends these packets rapidly without waiting for a reply in an attempt to make the target network unreachable through brute force. These attacks are particularly concerning because bandwidth is consumed both ways with attacked servers trying to reply with their ICMP Echo Reply packets. The result is a decline in speed across the entire network.

2.5.4 SYN Flood – SYN Flood attacks are another type of DoS attack where the attacker uses the TCP connection sequence to make the victim's network unavailable. The attacker sends SYN requests to the victim's network which then responds with a SYN-ACK response. The sender is then supposed to respond with an ACK response but instead, the attacker doesn't respond (or uses a spoofed source IP address to send SYN requests instead). Every request that goes unanswered takes up network resources until no devices can make a connection.

2.5.5 Slow Loris – Slow Loris is a type of DDoS attack software that was originally developed by Robert Hansen to take down web servers. A Slow Loris attack occurs when the attacker sends partial HTTP requests with no intention of completing them. To keep the attack going, Slow Loris periodically sends HTTP headers for each request to keep the computer networks is used by attackers because it doesn't require any bandwidth.

2.5.6 HTTP Flood – In an HTTP Flood attack, the attacker uses HTTP GET or POST requests to launch an assault on an individual web server or application. HTTP floods are a Layer 7 attack and don't use resources tied up. This continues until the server can't make any more connections. This form of attack malformed or spoofed packets. Attackers use this type of attack because they require less bandwidth than other attacks to take the victim's network out of operation.

2.5.7 Zero-Day Attacks – Zero-Day attacks are attacks that exploit vulnerabilities that have yet to be discovered. This is a blanket term for attacks that could be faced in the future. These types of attacks can be particularly devastating because the victim has no specific way to prepare for them before experiencing a live attack.

2.6 WHAT HAPPENS DURING A DDoS ATTACKS

Cybercriminals perform their DDoS attacks by sending out malicious code to hundreds or even thousands of computers, instructing each one to send requests to a single organization. This is usually accomplished through tools, such as a botnet. The botnet can be a network of private computers infected with malicious software that is controlled as a group, without the knowledge of each owner [3].

2.7 WHY HAVE DDoS ATTACKS INCREASED

Hackers frequently target critical services such as web services and platforms that are often used by large businesses, banks, governments, and educational institutions. There are multiple forms of DDoS attacks, including volumetric attacks, amplification-layer attacks, and protocol attacks. While they differ in how they inflict damage, all three approaches can attack a victim on multiple fronts to completely overwhelm their infrastructure and applications [3].

If you are not concerned about DDoS attacks yet, you should be. The last year has seen a significant rise in the amount of DDoS attacks, and there is no evidence that they'll decrease anytime soon.

Global information and technology provider Neustar reported that it found a 168% increase in DDoS attacks in Q4 2019 from Q4 2018. Overall, there was a 180% increase in DDoS attacks in 2019 compared with 2018. The report also found alarming statistics that attack intensity has increased overall as well. In 2019, the largest threat was 31% larger than the largest DDoS attack in 2018, at 587 gigabits per second while the most attack intensity of 2019 at 343 million packets per second was 252% higher than the most intense attack of the previous year. Neustar predicts that the sudden shift to teleworking due to COVID-19 will only increase DDoS attacks, especially against VPD infrastructure.

As more organizations adopt internet-connected devices, cybercriminals see the opportunities for DDoS attacks, which may explain the rise. The more companies integrate unsecured Internet of Things devices without the right cyber security precautions, the more they place themselves at risk and contribute to the rise in DDoS attacks.

TABLE: 2.8 DIFFERENCE BETWEEN DoS AND DDoS ATTACKS [8]

DoS	DDoS
I. DoS Stands for Denial of service attack.	DDoS Stands for Distributed Denial of service attack.
II. In a DoS attack single system targets the Victim's system.	In DDoS multiple systems attacks the Victim's system.
III. Victim PC is loaded from the packet of Data sent from a single location.	Victim PC is loaded from the packet of Data sent from multiple locations.
IV. DoS attack is slower as compared to DDoS.	The DDoS attack is faster than DoS Attack.
V. In DoS Attack only a single device is used with DoS Attack tools.	It is difficult to block this attack as multiple devices are sending packets and attacking from Multiple locations.
VI. DoS Attacks are Easy to trace.	In DDoS attacks, Bots are used to attack at At the same time.
VII. The volume of traffic in DoS attacks is Less as compared to DDoS.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim Network.
VIII. Types of DoS Attacks are:	Types of DDoS Attacks are:
<ul style="list-style-type: none"> • Buffer overflow attacks 	<ul style="list-style-type: none"> • Volumetric Attacks
<ul style="list-style-type: none"> • Ping of Death or ICMP flood 	<ul style="list-style-type: none"> • Fragmentation Attacks
<ul style="list-style-type: none"> • Teardrop Attack 	<ul style="list-style-type: none"> • Application Layer Attacks

2.9 A BRIEF HISTORY OF DDoS ATTACKS

The first known distributed denial of service attack occurred in 1996 when PA nix, now one of the oldest internet service providers, was knocked offline for several days by a SYN flood, a technique that has become a classic DDoS attack. Over the next few years, DDoS attacks became common and Cisco predicts that the total number of DDoS attacks will double from the 7.9 million seen in 2018 to something over 15 million by 2023 [5].

However, it's not just the number of DDoS attacks that are increasing. Threat actors are creating ever bigger botnets – the armies of hacked devices that are used to generate DDoS traffic. As the botnets get bigger, the scale of DDoS attacks is also increasing. A distributed denial of service attack of one gigabit per second is enough to knock most organizations off the internet but we're now seeing peak attack sizes above one terabit per second generated by hundreds of thousands or even millions of suborned devices. For more background about what's technically involved in a distributed denial of service.

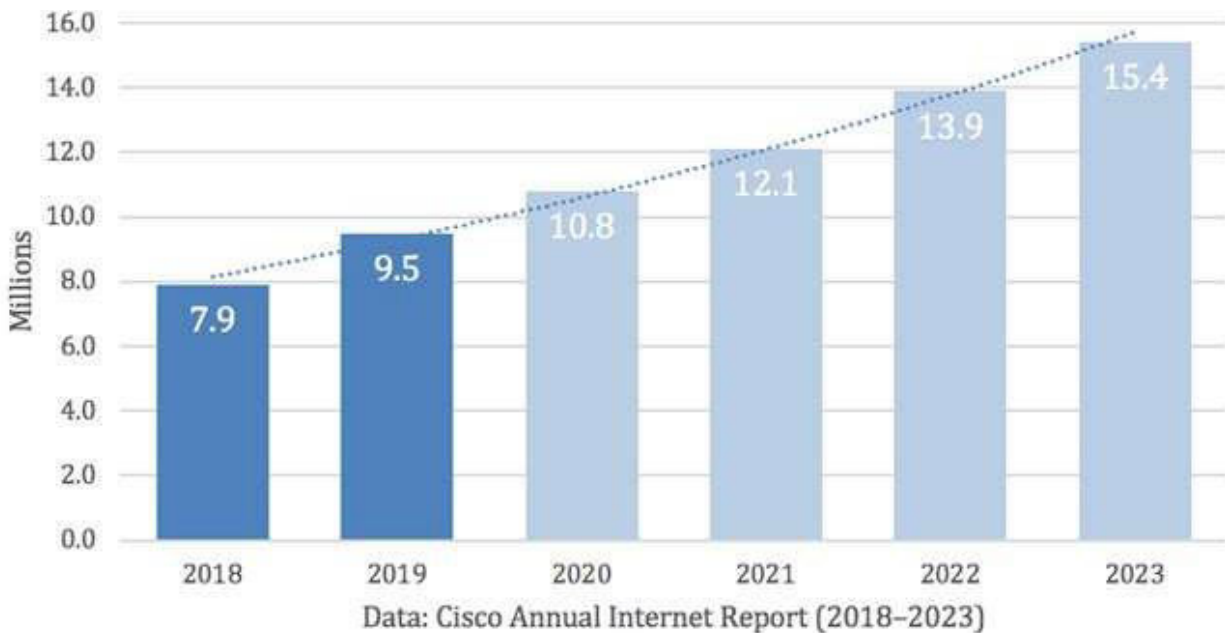


Figure2.7.1: Cisco's analysis of DDoS total attack history and predictions

2.10 TOPMOST FAMOUS DDoS ATTACKS [5]

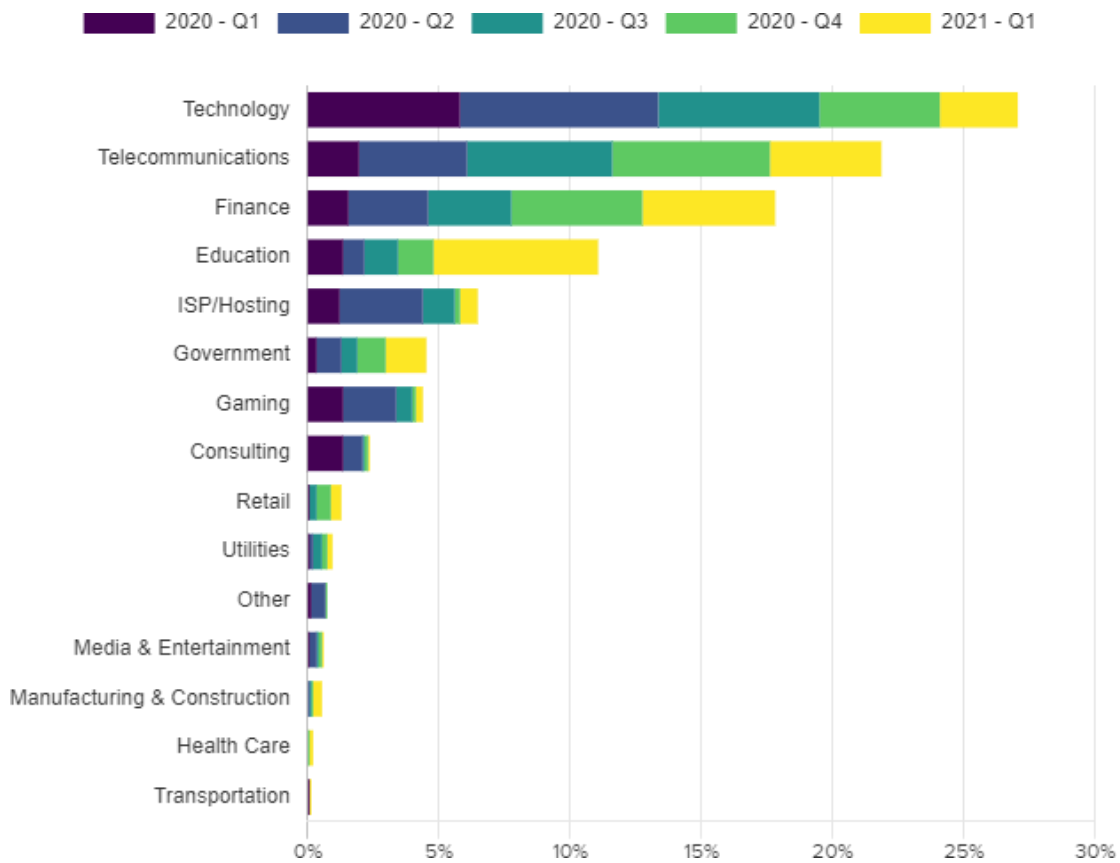
- The Six Banks DDoS Attack in 2012
- The Spamhaus DDoS Attack in 2013
- The Cloud Flare DDoS Attack in 2014
- Occupy Central, Hong Kong DDoS Attack in 2014
- The Mirai Dyn DDoS Attack in 2016
- The Mirai Krebs and OVH DDoS Attacks in 2016
- The GitHub Attack in 2018
- The Google Attack, 2020
- The AWS DDoS Attack in 2020
- A European Gambling Company, 2021 [5]

CHAPTER 3

BEING TARGETED WITH DDoS

Launching DDoS attacks has a very low barrier to entry for the would-be hacker. YouTube contains tutorials for creating new botnets, and DDoS-for-hire services offer cheap rates for those looking to launch an immediate attack with zero effort. Because of this, no industry is safe. Whether it be a determined attack from an organized crime group or a politically motivated form of protest, DDoS attacks are cheap and easy to launch [4].

Over the past few years, we have observed that the most attacked industries are education, finance, gaming, technology, and telecommunications, with the top spot changing in any given month. This time around, technology, which took 27% of all attacks, was the most targeted sector in the past 15 months, as shown in Figure



CHAPTER 4

PREVENTION DoS AND DDoS ATTACKS

4.1 Organize a DDoS Attack Response Plan

Don't be caught blindsided by DDoS attacks; have a response plan ready in case of a security breach so your organization can respond as promptly as possible. Your plan should document how to maintain business operations if a DDoS attack is successful, any technical competencies and expertise that will be necessary, and a systems checklist to ensure that your assets have advanced threat detection [3].

Additionally, establish an incident response team in case the DDoS is successful and define responsibilities, such as notifying key stakeholders and ensuring communication throughout the organization.

4.2 Secure your Infrastructure with DDoS Attack Prevention Solutions

Equip your network, applications, and infrastructure with multi-level protection strategies. This may include prevention management systems that combine firewalls, VPN, anti-spam, content filtering, and other security layers to monitor activities and identify traffic inconsistencies that may be symptoms of DDoS attacks.

If you're looking for protection by leveraging cloud-based solutions, many providers allow for advanced protection resources for additional charges. Other options allow for businesses to go "full cloud," entrusting sensitive data with a reputable cloud provider that offers heightened security protocols, both virtual and physical.

4.3 Perform a Network Vulnerability Assessment

Identify weaknesses in your networks before a malicious user does. A vulnerability assessment involves identifying security exposures so you can patch up your infrastructure to be better prepared for a DDoS attack, or any cyber security risks in general. Assessments will secure your network by trying to find security vulnerabilities. This is done by taking inventory of all devices on the network, as well as their purpose, system information, and any vulnerabilities associated with them, and including what devices need to be prepared for upgrades or future assessments. Doing so will help define your organization's level of risk so you can optimize any security investments.

4.4 Identify Warning Signs of a DDoS Attack

If you can identify the symptoms of a DDoS attack as early as possible, you can take action and hopefully mitigate damage. Spotty connectivity, slow performance, and intermittent web crashes are all signs that your business may be coming under attack from a DDoS criminal. Educate your team on signs of DDoS attacks so everyone can be alert for warning signs.

Not all DDoS attacks are extensive and high volume; low-volume attacks that launch for short durations are just as common. These attacks can be particularly nefarious because they are more likely to go under the radar as just a random incident rather than a potential security breach.

Low-volume DDoS attacks are likely distractions for damaging malware; while your IT security staff is distracted by a low-volume attack, malicious software like ransomware can infiltrate your network.

4.5 Adopt Cloud-Based Service Providers

There are several benefits to outsourcing DDoS attack prevention to the cloud.

Cloud providers who offer high levels of cyber security, including firewalls and threat monitoring software, can help protect your assets and network from DDoS criminals. The cloud also has greater bandwidth than most private networks, so it is likely to fail if under the pressure of increased DDoS attacks.

Additionally, reputable cloud providers offer network redundancy, duplicating copies of your data, systems, and equipment so that if your service becomes corrupted or unavailable due to a DDoS attack, you can switch to secure access on a backed-up version without missing a beat.

4.6 Know your network's traffic

Every organization's infrastructure has typical Internet traffic patterns — know yours. When you understand your organization's normal traffic pattern, you'll have a baseline. That way, when unusual activity occurs, you can identify the symptoms of a DDoS attack.

4.7 Create a Denial of Service Response Plan

Do you know what will happen when and if a DDoS attack happens? How will your organization respond? By defining a plan in advance, you'll be able to respond quickly and efficiently when your network is targeted.

This can take some planning; the more complex your infrastructure, the more detailed your DDoS response plan will be. Regardless of your company's size, however, your plan should include the following:

- A systems checklist.
- A trained response team.
- Well-defined notification and escalation procedures.
- A list of internal and external contacts should be informed about the attack.
- A communication plan for all other stakeholders, like customers, or vendors.

4.8 Make your network resilient

Your infrastructure should be as resilient as possible against DDoS attacks. That means more than firewalls because some DDoS attacks target firewalls. Instead consider making sure you're not keeping all your eggs in the same basket put data centres on different networks, make sure that not all your data centres are in the same physical location, put servers in different data centres, and be sure that there aren't places where traffic bottlenecks in your network.

4.9 Practice good cyber hygiene

Your users should be engaging in best security practices, including changing passwords, secure authentication practices, knowing to avoid phishing attacks, and so on. The less user error your organization demonstrates, the safer you'll be, even if there's an attack.

4.10 Scale up your bandwidth

If DDoS is creating a traffic jam in your network, one way to make that traffic jam less severe is to widen the highway. By adding more bandwidth, your organization will be able to absorb more to absorb a larger volume of traffic. This solution won't stop all DDoS attacks, however. The size of volumetric DDoS attacks is increasing; in 2018, for example, a DDoS attack topped 1 Tbps. in size for the first time. That was a record until a few days later when a 1.7 Tbps attack occurred

4.11 Take advantage of anti-DDoS hardware and software

DDoS attacks have been around for a while and some kinds of attacks are very common. There are plenty of products that are prepared to repel or mitigate certain protocol and application attacks, for example. Take advantage of those tools.

4.12 Move to the cloud

While this won't eliminate DDoS attacks, moving to the cloud can mitigate attacks. The cloud has more bandwidth than on-premise Resources, for example, and the nature of the cloud means many servers are not located in the same place.

4.13 Know the symptoms of an attack

Your network slows down inexplicably. The website shuts down. All of a sudden, you're getting a lot of spam. These can all be signs of a DDoS attack. If so, the organization should investigate.

4.14 Outsource your DDoS protection

Some companies offer DDoS-as-a-Service. Some of these companies specialize in scaling resources to respond to an attack, others bolster defence, and still, others mitigate the damage of an ongoing attack.

4.15 Monitor for unusual activity

Once you know your typical activity and the signs of an attack, monitor your network for odd traffic. By monitoring traffic in real-time, your organization will be able to spot a DDoS attack when it starts and mitigate it.

CHAPTER 5

DDoS MITIGATION TECHNIQUES

DDoS mitigation refers to the process of successfully protecting a targeted server or network from a DDoS. By utilizing specially designed network equipment or cloud-based protection service, a targeted victim can mitigate the incoming threat.

Before we discuss the DDoS mitigation techniques, you need to understand the identification of web attacks [7].

5.1 Classify legitimate traffic vs. DDoS attacks

Identification of attacks is very essential and the first step of DDoS mitigation. After all, you can't afford to block legitimate traffic to your website.

You probably would have thought of IP tables or similar methods to handle the attacks. All these come with certain drawbacks and are not complete solutions. Also, even if you're going to use something as simple as that, you will have to identify the legitimate traffic. In this case, you could do so by navigating through your website from a specific IP and then watching the HTTP access log to see how many connections are made from your IP to the webserver. This might give you a rough estimate of how many connections in a given timeframe can be considered legitimate or so. Now, let's discuss some DDoS mitigation techniques out there that can be used to mitigate such attacks.

5.2 Avoid becoming a bot

Let's say your internal website which is not open to the public is down due to a DDoS attack. What's the catch? No employee would possibly attack their company asset. Hence, the possible chances are that few of the employees' systems are compromised and are being used as bots. So, the employees must be educated on how not to be exploited.

They should be aware of basic security measures such as

- Using a strong password.
- Configuring local firewall and managing the same.
- Not open random attachments.
- Always use antivirus to scan anything before opening.
- Apply timely security patches and keep the machine up to date
- If they doubt that they could be compromised, then install some network monitor like glassware to monitor the traffic
- But what if they've become a bot? Then the machine needs to be isolated, detached from the network, and cleaned up before it is reconnected to the network

5.3 Reducing Attack Surface

Reducing the surface that can be attacked limits the options for attackers. This is one of the methods.

- You will have to separate and distribute assets in a network so that it's harder to be targeted. For example, you can have your web servers in the public subnet, but the underlying database servers should be in a private subnet. Also, you can restrict access to database servers from your web servers and not from other hosts.

- You will have to separate and distribute assets in a network so that it's harder to be targeted. For example, you can have your web servers in the public subnet, but the underlying database servers should be in a private subnet. Also, you can restrict access to database servers from your web servers and not from other hosts.
- Using Firewalls and Network Access Control Lists to allow only necessary traffic, to necessary ports from necessary hosts. In the case of web servers, you allow traffic from anywhere to port 80 of your web server. And in such cases, you further take other protective measures like the ones we've listed here.
- Even for sites that are accessible over the internet, you can reduce the surface area by restricting traffic to countries where your users are located.

5.4 CDNs

A Content Delivery Network (CDN) distributes your content and boosts performance by minimizing the distance between your resources and end-users. It stores the cached version of your content in multiple locations and this eventually mitigates DDoS attacks by avoiding a single point of failure, when the attacker is trying to focus on a single target. Popular CDNs include Akamai CDN, Cloud flare, AWS Cloud Front, etc.

5.5 Black Hole Routing

As the name suggests, black hole routing without any filtering routes both legitimate and malicious traffic to a null route or black hole where it's going to be dropped from the network. Based on the pattern, if you could identify the attacker, then you could filter those packets and route them to the black hole.

5.6 Rate Limiting

Limiting the number of requests a server will accept over a certain time window from an IP is a way of mitigating denial of service attacks, similar to that of IPtables. However, in the case of DDoS, rate-limiting alone wouldn't be sufficient. Nevertheless, it's useful for DDoS protection.

5.7 WAF

A Web Application Firewall (WAF) is a tool that can assist in mitigating the Layer 7 DDoS attack. You can place a WAF in between the internet and origin server and WAF can act as a reverse proxy protecting the server from exposure by making the clients pass through them before reaching the server. Using WAF, you can quickly implement custom rules in response to an attack and turn, mitigate them, so that the traffic is dropped before even reaching your server, thus taking an offload from the server. Depending upon where you implement WAF, it can be implemented in one of the three ways

- Network-based WAF
- Host-based WAF
- Cloud-based WAF

5.8 Scale

In this method, you scatter the DDoS traffic across a cluster of nodes so that it's handled like any other legitimate traffic. For example, consider you have implemented auto-scaling of your web resources when the incoming connection requests are beyond a certain number.

Now, this auto-scaling will ensure new web servers are being spawned to handle the connection requests. You can set up alerts so that you're notified when more than a certain number of instances are spawned. By doing so, you will know that there's some issue with it and you can further implement the mitigation techniques to block those traffic and bring the server back to its normal functioning. This depends on

- The size of the attack
- The efficiency of the network (Transit capacity)
- Compute resources (Server capacity)

Now that you're aware of some of the techniques to mitigate DDoS, let's look at the stages of DDoS mitigation that help in the implementation of the techniques.

5.9 Stages of DDoS Mitigation

- I. **Detection:** The first step to mitigating the attack is to detect if there's an attack. Here's where you will have to identify the legitimate traffic and malicious traffic. In the event of mitigating DDoS, you shouldn't accidentally drop potential customer traffic which would be disastrous.
- II. **Response:** Once you've detected the attack, you will have to find a way to respond to those attacks. For example, you will have to work on dropping that malicious DDoS traffic before it reaches your server so that it doesn't throttle and exhaust your server. Here's where you will filter the traffic so that only legitimate traffic reaches the server.

- III. **Routing:** By intelligent routing, you can break the remaining traffic into manageable chunks that can be handled by your cluster resources to which it's being routed.

- IV. **Adaption:** The most important stage in DDoS mitigation is where you will look for patterns of DDoS attacks and use those analyses to further strengthen your mitigation techniques. For example, blocking an IP that's repeatedly found to be offending.

5.10 DDoS mitigation service

Traditional DDoS mitigation solutions involved purchasing equipment that would live on-site and filter incoming traffic. This approach involves purchasing and maintaining expensive equipment and also relied on having a network capable of absorbing an attack. If a DDoS attack is large enough, it can take out the network infrastructure upstream preventing any on-site

The solution from being effective. When purchasing a cloud-based DDoS mitigation service, certain characteristics should be evaluated.

- I. **Scalability** - an effective solution needs to be able to adapt to the needs of a growing business as well as respond to the growing size of DDoS attacks. Attacks larger than 2 terabits per second have occurred, and there's no indication that the trend in attack traffic size is downward. Cloud flare's network is capable of handling DDoS attacks considerably larger than have ever occurred.

- II. **Flexibility** - being able to create ad hoc policies and patterns allows a web property to adapt to incoming threats in real-time. The ability to implement page rules and populate those changes across the entire network is a critical feature in keeping a site online during an attack.

- III. **Reliability** - much like a seatbelt, DDoS protection is something you only need when you need it, but when that time comes it better be functional.

The reliability of a DDoS solution is essential to the success of any protection strategy.

Make sure that the service has high uptime rates and site reliability engineers work 24 hours a day to keep the network online and identify new threats. Redundancy, failover, and an expansive network of data centres should be central to the strategy of the platform.

- IV. **Scalability** - an effective solution needs to be able to adapt to the needs of a growing business as well as respond to the growing size of DDoS attacks. Attacks larger than 2 terabits per second have occurred, and there's no indication that the trend in attack traffic size is downward. Cloud flare's network is capable of handling DDoS attacks considerably larger than have ever occurred.
- V. **Flexibility** - being able to create ad hoc policies and patterns allows a web property to adapt to incoming threats in real-time. The ability to implement page rules and populate those changes across the entire network is a critical feature in keeping a site online during an attack.
- VI. **Reliability** - much like a seatbelt, DDoS protection is something you only need when you need it, but when that time comes it better be functional. The reliability of a DDoS solution is essential to the success of any protection strategy. Make sure that the service has high uptime rates and site reliability engineers work 24 hours a day to keep the network online and identify new threats. Redundancy, failover, and an expansive network of data centres should be central to the strategy of the platform.
- VII. **Network size** - DDoS attacks have patterns that occur across the Internet as particular protocols and attack vectors change over time. Having a large network with extensive data transfer allows a DDoS mitigation provider to analyze and respond to attacks quickly and efficiently, often stopping them before they ever occur. Cloud flare's network runs Internet requests for ~10% of the Fortune 1,000, creating an advantage in analyzing data from attack traffic around the globe.

CHAPTER 6

SOME DoS vs. DDoS ATTACKS FAQs

6.1 How to improve security using a Content Delivery Network (CDN)?

A content delivery network (CDN) stores copies of the website content, including entire web pages on servers around the world. Visitors to the site get those web pages from a CDN server and not your infrastructure. So, Denial of Service attacks gets directed at the CDN server. These servers have a great deal of capacity and can absorb large volumes of bogus connection requests.

6.2 What is the detection process for a DDoS attack?

A DDoS attack involves high volumes of traffic from a large number of sources. DDoS detection software will notice a surge in connection requests. DDoS defence system samples connection requests randomly rather than inspecting each one. When typical DDoS strategies are detected, mitigation processes will be triggered [2].

6.3 Can you trace a DDoS attack?

The devastating tactics of a DDoS attack lie in its ability to overwhelm a web server with more connection requests than it can handle. Thus, there is little time during an attack to trace the source of attacks. Also, there is little point in doing that as each zombie computer usually only sends one request. Thus, if you got to the source of a malformed connection message, you wouldn't prevent thousands of other computers from sending requests at that moment. Most of the source IP addresses on DDoS connection requests are genuine, but they do not belong to the computer of the real attacker.

6.4 Does a DDoS attack damage hardware?

No. DDoS attacks are designed to push routers, load balancers, and servers to their performance limits. Those limits mean that a device can never be forced into a physical failure through factors such as overheating.

CHAPTER 7

CONCLUSION

A DDoS attack uses network vulnerability, which makes a loss of network connection persistently, slows down the system performances, and creates more traffic on the internet, resulting in the inability to use internet service for a long period of time. This practice is favourable for the trespasser who wishes for the valid user to cooperate with the safety measures of his essential and sensitive information. Once the system gets attacked by DDoS, it might not be found easily, and its prevention is also not the easiest one. The only way to get relieved from this is to determine whether any injuries were caused by it and to take action to recover them. In this survey, we have presented a comprehensive and systematic analysis of DDoS attacks. In our work, we have analyzed well-known prevention.

In this survey, we have presented a comprehensive and systematic analysis of DDoS attacks. We have enlisted different attack types seen so far. In our work, we have analyzed well-known prevention and mitigation techniques based on their success and failures. We have summarized different types of attacks, filtering techniques, and attack detection methods. We have identified the key features of the attacks as well as the different deface mechanisms. However, still there exists the chance to see new unseen attacks with new signatures and features. However, this survey will work as an easy-to-understand foundation of the DDoS attacks for its systematic explanation and analysis. As this survey has also included recent attacks and recent research against DDoS attacks, it also presents the current state of the art of DDoS attacks. We also provided some discussions about DDoS attacks on non-traditional systems such as clouds, smart grids, smart homes, CPSs, and IoT systems. Finally, we have also enlisted the challenges involved in the research of DDoS attacks. Thus, it outlines some extremely important future research directions deserving attention.

REFERENCES

- [1] DDoS Attack Classification, Available at: <https://aws.amazon.com/shield/ddos-attack-protection/>, Last access 6-8-21 / 9.10 pm
- [2] DoS and DDoS Attacks Occur, Broad Types of DoS and DDoS Attacks, Most Common Forms of DDoS Attacks, Some DoS Vs. DDoS Attacks Faqs, Available at: https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/#What_is_the_detection_process_for_a_DDoS_attack, Last access 26-9-21 / 11.10 am
- [3] What Happens during a DDoS Attacks, Why Have DDoS Attacks Increased, Prevention DoS and DDoS Attacks, Available at: <https://www.dsm.net/it-solutions-blog/prevent-ddos-attacks>, Last access 15-10-21 / 9.00 pm
- [4] Being Targeted with DDoS, Available at: <https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020>, Last access 2-11-21 / 2.40 pm
- [5] A Brief History of DDoS Attacks, Topmost Famous DDoS Attacks, Available at: <https://www.a10networks.com/blog/5-most-famous-ddos-attacks/>, Last access 9-12-21 / 7.15 pm
- [6] Online, Available at: <https://journals.sagepub.com/doi/full/10.1177/1550147717741463>, Last access 23-11-21 / 8.10 pm
- [7] DDoS Mitigation Techniques, Available at: <https://www.indusface.com/blog/ddos-mitigation-techniques/>, Last access 5-8-21 / 11.25 am
- [8] Difference between Dos and DDoS Attacks, Available at: <https://www.geeksforgeeks.org/difference-between-dos-and-ddos-attack/>, Last access 13-12-21 / 12.00 am

DoS and DDoS

ORIGINALITY REPORT

20%

SIMILARITY INDEX

%

INTERNET
SOURCES

%

PUBLICATIO
NS

20%

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to DeVry, Inc. Student Paper	1%
2	Submitted to Leicester College Student Paper	1%
3	Submitted to Istanbul Aydin University Student Paper	2%
4	Submitted to UNITEC Institute of Technology Student Paper	1%
5	Submitted to Hellenic American University Student Paper	4%
6	Submitted to Fulton schools Student Paper	1%
7	Submitted to Kaplan University Student Paper	1%
8	Submitted to Canberra Institute of Technology Student Paper	1%
9	Submitted to Swinburne University of Technology	2%