ISSN: 0975-3583, 0976-2833 VOL 11, ISSUE 04, 2020

A SYSTEMATIC STUDY ON DDOS ATTACKS AND ITS DEFENSE MECHANISMS

Shaveta Gupta[1], Dinesh Grover[2]
[1]Research Scholar, IKG PTU Jalandhar, [2]Professor (Retd.), Dept. of EE & CSE, PAU Ludhiana
Corresponding Author: Shaveta Gupta. Email: shaveta@gc11.ac.in

Abstract: The Internet acts as a worldwide information source for all users. In this pendemic the whole world survive just because of the power of the internet. But the hackers used the openness and flexible features of the internet for cyber attacks. One of today's most prominent and significant cyber-attack is distributed denial-of-service attacks. This article focuses mostly on DDoS attacks, which block network availability by overloading the target with a significant number of illicit traffic usurping its bandwidth, overburdening it, and preventing legitimate traffic from passing through. In this research work, we are going to describe DDoS attacks, how they will be defended, and the goals of an ideal defense framework.

Keywords: DDoS, prevention, detection, internet

I. INTRODUCTION

The Internet is a public worldwide network. Organizations all across the world have changed their business models as a result of the internet's rise. Every day, an increasing number of people connect to the internet in order to take advantage of the new business model known as e-Business. Internetwork connectivity has therefore become a very critical aspect of today's business. Doing business on the internet there are two sides. On the one hand, the Internet offers businesses enormous possibilities in terms of reaching end customers. At the same time, it introduces numerous risks into the firm. On the internet, there are both benign and malicious people. While an organisation makes its information system accessible to innocent internet users, the information is also accessible to malicious users. For a variety of reasons, malicious people or hackers can get access to an organization's internal systems. These are weaknesses in software, failures in management, and systems that have been reset to their default settings. In all areas of business and industry, including bank transactions, social media, e-mail, and university e-services, network security has become critical. Recently, web and network services have experienced intruder attacks. Hackers are constantly developing new Distributed Denial of Service (DDoS) attacks that target both the application and network layers. [3]. DDoS is a cyber-attack in which the attacker attempts to disable a system or network resource by flooding the target. Researchers offered several ways of dealing with them. Attackers are sophisticated and intelligent enough to circumvent security systems, while researchers are always developing new tactics and countermeasures. Our contribution in this paper is as follows:

- Description of DDoS attack with latest DDoS attacks happened in the history along with its impact on the business.
- Various Defense Mechanisms used against DDoS Attacks.
- The goals of the Ideal Defense Framework have been described.
- Various Validation techniques used for DDoS research have been described.

II. DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDoS)

A DDOS attack is an attempt by a hacker to flood the victim server with vast packets or traffic that the server is inoperable to handle the further request as a result denial of service attack happens as shown in Fig. 1. These networks are made up of malware-infected computers and other devices allowing an attacker to control them remotely. Individual devices are known as bots (or zombies), while a botnet is a collection of bots. The attacker can lead an attack after building a botnet by providing remote commands to each bot.

ISSN: 0975-3583, 0976-2833 VOL 11, ISSUE 04, 2020

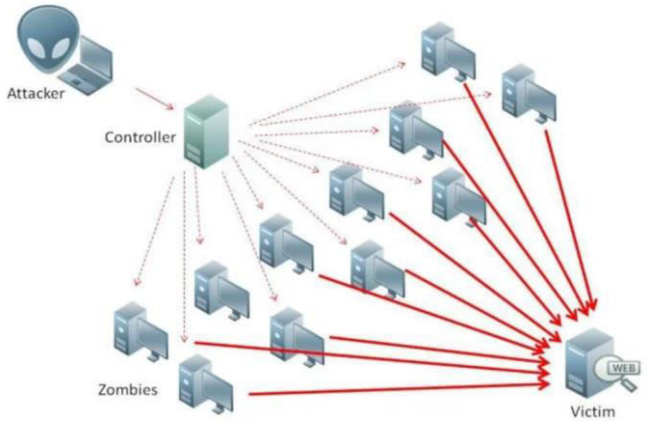

Figure 1: Distributed Denial of Service Attack

DDoS attacks are rising at an alarming rate in both frequency and severity in recent years [5]. Tab. 1. shows some recent DDoS attacks [1]. Fig. 2. shows how deeply it affects our society.

Table 1: Recent DDoS attacks

S. No	Date	Event	Impact
1.	2017	Google Attack	It was 2.5 Tbsp.
2.	2020	Amazon Cloud	It was 2.3 Tbsp.
3.	2016	Mirai Krebs	It was 1.1Tbsp.
4	2018	GitHub	It was 1.35 Tbsp.

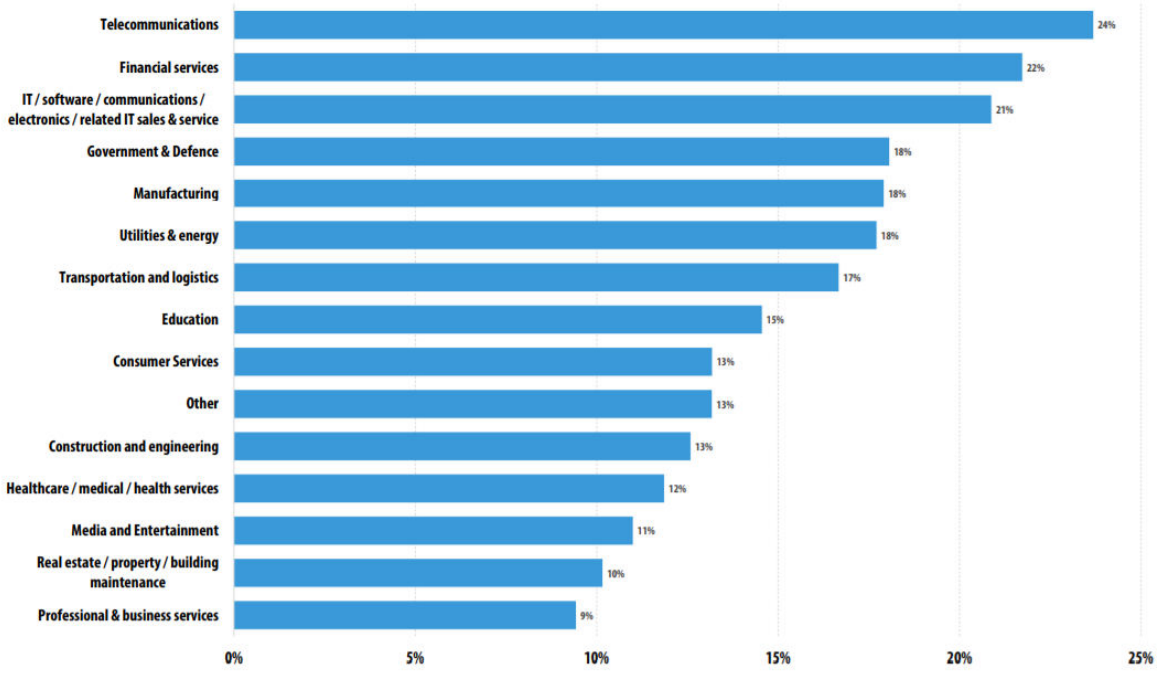

Figure 2. Companies affected by DDoS attack

III. DDOS DEFENSE MECHANISMS

DDoS is an abbreviation for Distributed Denial of Service. Attacks are on the rise, and they pose a serious concern in today's digital world; as a response, researchers have offered several solutions. Attackers are smart and intelligent enough to avoid security systems, and researchers are always

ISSN: 0975-3583, 0976-2833 VOL 11, ISSUE 04, 2020

creating new strategies and responses. There are four main approaches to dealing with attacks as shown in Fig. 3:

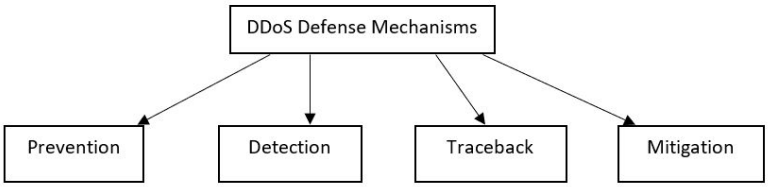

Figure 3: DDoS Defense Classification

Prevention: It is often preferable to cure. As previously said, attack prevention is a measure that is taken to deter an attack before it does harm to the network. Packet filtering is the most effective solution when implemented close to the attack source, intermediate infrastructure, or destination network [10]. Methods of prevention seek to address the vulnerability flaws that DDoS attackers use to initiate attacks. However, it is hard to specify the rules for filtering that can segregate legitimate and spoofed packets. Moreover, various filtering schemes require wide deployment to be more efficient. Due to the openness and decentralization of the internet, prevention is a tough task.

Detection: The seriousness of the DDoS crisis, as well as the increased frequency of DDoS attacks, has resulted in the development of various DDoS protection mechanisms. Detecting these in real-time is the first step in combating such types of attacks. A lot of research has been carried out to detect these attacks, but none of these schemes can satisfactorily detect these attacks [8-9]. Attacks can be detected during the attack or after the attack. For DDoS identification, there are mainly two approaches: signature-based and anomaly-based. Signature identification is based on a database of documented attack signatures. Both incoming packets are linked to this index, and those that fit are discarded. As a result, the signature must be specifically designed to explicitly define the attack to ensure that no valid traffic produces a match. The target is to obtain a false positive rate of zero. However, the utility of signature-based identification is limited to attacks involving easily matchable packet attributes and previously identified signatures. Furthermore, this method is incapable of detecting these new forms of attacks. As a result, false negatives are too common in novel assaults. Anomaly detection is the opposite of signature detection. It recognizes that malicious activities change and that no protection mechanism can anticipate or model them all. Anomaly detection, on the other hand, attempts to model legal traffic and raises an alarm if detected traffic deviates from the model. The clear advantage of this strategy is that previously unknown attacks can be identified if they differ enough from legitimate traffic. Anomaly identification, on the other hand, is a massive problem. Since new applications are being developed daily, legitimate traffic is becoming increasingly complex. Traffic dynamics vary depending on the type of application and how it is used. Because traffic fluctuates, a model that classifies real traffic too narrowly can result in a large number of false positives. A sloppy model, on the other hand, will allow several attacks to go unnoticed, resulting in a higher likelihood of false positives.

Traceback: If the attack has been found, the safest course of action is to stop the malicious traffic only at the originating end, until it has a chance to damage the network. So, traceback techniques help over here to find out the culprit and block it. There are different techniques used to trace back: Link testing, Messaging, Packet Marking, Hash-Based Scheme, etc. Cooperation among various ISPs is critical in the implementation of a traceback scheme. However, in the present situation, there is no such coordination, which is a significant source of concern. Many cutting-edge traceback mechanisms fail when an attacker is hidden under several layers of infected computers. Rather than exposing the name of the real perpetrator, traceback stops at steppingstones. Because of the lower storage and bandwidth requirements, marking methods have been commonly used in addition to other traceback techniques. A traceback scheme always necessitates changes to current protocols or router applications. Around the same time, there could be a need for extra support. As a result, ISPs are normally hesitant to implement any of these improvements without finding incentives.

Mitigation: DDoS attacks are growing by leaps and bounds and it creates a critical problem because of security breaches to the end-users a vast number of defense mechanisms have been implemented to resolve this issue. But a 100% bulletproof solution against attacks cannot be obtained, as hackers are intelligent enough to find the vulnerability in the existing defense mechanisms [4]. What people can do is to make a system through which attacks can be found quickly with less collateral damage. DDoS attack tolerance strategies focus on managing both intended and malicious traffic. Mitigation, on the other hand, is known as the method of reducing the effect of a DDoS attack. The mitigation mechanism

ISSN: 0975-3583, 0976-2833 VOL 11, ISSUE 04, 2020

involves coordination between the various modules of the overall protection process, such as identification, characterization, and traceback.

IV. VALIDATION TECHNIQUES USED FOR DDOS RESEARCH

When a academic suggests a new detection or protection approach in the field of network security, the suggested method must first be applied in the form of a network-based research for assessment and then verified using the available set of validation tools [16]. There are four ways to validate in network-based studies as described in Tab. 2.

Simulation: On a single computer system, simulation offers a repeatable and controlled framework for network-based research. It's easy to set up and manage a simulation-based experiment. It allows programmers to explore in a quick prototype and assessment environment, allowing many poor alternatives to be rejected before attempting a complete implementation.

Table 2: DDoS attacks validation techniques

Attributes	Extensibility	Repeatability	Fidelity	Programmability	Abstraction
Emulation	Moderate	Moderate	Moderate	Moderate	Moderate
Real dataset	Highest	Highest	Highest	Lowest	Lowest
Real system	Lowest	Lowest	Highest	Highest	Lowest
Simulation	Highest	Highest	Lowest	Highest	Highest

Emulation: It is the combination of simulation and real-world systems. Emulation combines genuine operating system and application parts with illusory and simulated aspects such as soft network connections, virtual intermediary nodes, and unrealistic background traffic. Emulation, on the other hand, uses soft routers to make connections.

Real Systems: Actual systems provide accurate network circumstances, applications, real operating systems, and platforms, and have been proved to be the best choice for network-based experiments.

Real Datasets: It provides the real data set to the researchers. Some attacks happened on the ecommerce websites; data set corresponding to that event is used to apply certain detection algorithms.

V. GOALS OF AN IDEAL DDOS DEFENSE FRAMEWORK

An effective DDoS defense solution is that which can effectively prevent the denial of the service of a victim to the legitimate users. According to the existing studies following are the goals for an ideal defense mechanism:

- **Effectiveness: -**A good DDoS detection and mitigation framework should effectively defend and provide either sufficient prevention that makes the system attack proof or an effective reaction so that the Dos effect is not observed at all. In the case of reactive techniques, the response should be quick and automated to guarantee that the victim is not seriously injured.
- **Completeness:** - A perfect DDoS protection should be all-encompassing. It must be able to deal with any type of attack. While completeness is a desirable aim, it is difficult to attain because attackers are likely to create new signatures for attack packets in order to get around existing defences.
- **Minimum Collateral damage:** - As previously stated, the goal of DDoS defence is to ensure that legitimate users may continue to use their services. DDoS defense solution is such that it can characterize the attack traffic from the normal traffic so that the defense framework can only drop DDoS attack traffic not the legitimate traffic to avoid collateral damage.
- **Low False Positive Rates: -**The DDoS defense should activate its reactive mechanism only when a DDoS attack is underway. A false positive occurs when a detective scheme detects an attack when no attack is taking place. These false positives lead to collateral damage, as they might trigger the filtering mechanism when there is no attack. It also results in extra computational overhead concerning CPU cycles, memory, and delay caused due to processing all the packets.
- **Low deployment and operational costs:** - A DDoS defense is meant to permit systems to resume operations during DDoS attacks. There is an apparent economic cost of installing any

ISSN: 0975-3583, 0976-2833 VOL 11, ISSUE 04, 2020

commercial solution, including the costs of purchasing the hardware and software used to operate it, as well as the administrative costs of setting up new security equipment or software.

VI. CONCLUSION

DDoS is becoming a significant component of a long-term threat strategy, and attack automation has increased. Several efforts are being made by researchers to battle it, but they are still unable to eliminate the problem; instead, they are likely to represent a greater risk in the future. Several flaws, such as the Internet infrastructure's dispersed and non-uniform architecture, corporate rules, privacy regulations, and return on investment attract the hacker to breach the security policies for unscrupulous reasons. But what we can do is to use effective and efficient defense approaches, so that false-positive rates and false-negative rates can be reduced.

Acknowledgment: The authors would like to express their gratitude to IKG PTU for providing all the resources needed to complete this study.

References

[1] https://www.a10networks.com/blog/5-most-famous-ddos-attacks/.

[2] J. Jinquan and M. A. Abdulhakim, A. Ali-Absi, H.J. Lee "Analysis and Protection of Computer Network Security Issues," in 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea, 2020.

[3] K.S. Vanitha, S.V. Uma, S. K. Mahidhar, "Distributed Denial of service: Attack techniques and mitigation," International Conference on Circuits, Controls, and Communications(CCUBE),2017.

[4] F.S. Silva, E. Silva, E. P. Neto, M. Lemos, A.J. Neto et al., "A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios," Sensors, Vol.20, Issue 11, 2020.

[5] S. Chakraborty, P. Kumar, B. Sinha, "A Study on DDoS Attacks, Danger and its Prevention," International Journal of Research and Analytical Reviews, Vol.6, Issue 2, 2019.

[6] T. Mahjabin, Y. Xiao, G. Sun, "A survey of a distributed denial-of-service attack, prevention, and mitigation techniques, SAGE, Vol.13, Issue 12,2017.

[7] A. Srivastava, B. B. Gupta, A. Tyagi, A. Sharma, A Mishra, "A recent survey on DDoS attacks and defense mechanisms, "Advances in parallel distributed computing, Springer, pp.570–580,2011.

[8] R. S. Chaudhari, G. R. Talemale, "A Review on Detection Approaches for Distributed Denial of Service Attacks", International Conference on Intelligent Sustainable Systems (ICISS), 2019.

[9] P. Kaur, M. Kumar, A. Bhandari, "A review of detection approaches for distributed denial of service attacks", System Science and Control Engineering, Vol.5, Issue 1, 2017.

[10] M.A. Saleh, A.A Manaf, "A Novel Protective Framework for Defeating HTTP-Based Denial of Service and Distributed Denial of Service Attacks, Hindawi Publishing Corporation, 2015.

[11] X. Liu., X. Yang, and Y. Lu, "To filter or to authorize: Network- layer DoS defense against multimillion- node botnets," In ACM SIGCOMM Computer Communications Review, pp. 195-206, 2008.

[12] J. Markovic, P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communications Review, Vol. 34, No. 2, 2004.

[13] A. S. Jose, L. R. Nair, "Mitigation of Distributed Denial of Service (DDoS) Attacks over Software Defined Networks (SDN) using Machine Learning and Deep Learning Techniques," International Journal of Innovative Technology and Exploring Engineering (IJITEE), pp. 563–568, 2019.

[14] Johari, Rahul, and Pankaj Sharma, "A survey on web application vulnerabilities exploitation and security engine for SQL injection",2012 International Conference on Communication Systems and Network Technologies.

[15] Sarasan, Sandra., "Detection and Prevention of Web Application Security Attacks", International Journal of Advanced Electrical and Electronics Engineering, (IJAEEE),2013.

[16] S. Behal, K. Kumar, "Trends in Validation of DDoS Research," International Conference on Computational Modeling and Security. pp. 7-15,2016.

[17] C. Iwendi, M. Uddin, J. Ansere, P. Nkurunziza, J H Anajemba et. al, "On Detection of Sybil Attack in Large-Scale VANETs using Spider-Monkey Technique," IEEE Access, 2018.