Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 9, Issue 3, pp: (29-32), Month: September - December 2022, Available at: www.noveltyjournals.com

Countermeasures to DDOS attacks based on amplification

KABEYA TSHISEBA Cedric

Associate Professor at DRC Pedagogic National University
Faculty of Sciences
Department of Mathematics and Computing Science

DOI: https://doi.org/10.5281/zenodo.7491775

Published Date: 29-December-2022

Abstract: **A Distributed Denial of Service (DDoS) attack is a cybersecurity weapon aimed at disrupting the operation of services or extorting money from targeted organizations. These attacks can be motivated by politics, religion, competition or profit.**

Technically, a DDoS attack is a distributed version of a Denial of Service (DoS) attack whose goal is to disrupt the target's business operations. This type of attack sends a high volume of traffic to overload the normal operation of a service, server, or network interconnection, rendering them unavailable. DoS attacks disrupt service, while Distributed Attacks (DDoS) are carried out on a much larger scale, bringing down entire infrastructures and scalable (cloud) services.

In this work, we have addressed a rather particular DDoS, that relating to amplification. It was therefore a question here not only of talking about it, but also of presenting different forms of attacks, in addition to the related countermeasures for better security of our information systems.

Keywords: **Cryptosystem, DDOS, DDoS basé sur l'amplification, information system.**

1. INTRODUCTION

Denial of service attacks, this is a type of attack that is frequent today, in particular because of the relative simplicity of their implementation, and their effectiveness against an unprepared target. These attacks can cause significant financial losses through the interruption of service or even indirectly, through damage to the image of the target.

In this work we present the need for companies to anticipate this threat, and to take a number of technical and organizational measures to deal with it. This document presents denial of service attacks in general and attacks based on amplification in particular. In addition, the last point of this reflection recalls some good practices to implement in order not to involuntarily participate in a DDoS attack.

2. DDSO ATTACK

A denial of service attack is a computer attack aimed at making a service unavailable, preventing legitimate users of a service from using it. At present the vast majority of these attacks are made from several sources, we then speak of a distributed denial of service attack (abbr. DDoS attack for Distributed Denial of Service attack).

It can be:

- flooding of a network to prevent its operation;
- disruption of connections between two machines, preventing access to a particular service;
- obstruction of access to a service for a particular person;
- also the fact of sending billions of bytes to an internet box.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 9, Issue 3, pp: (29-32), Month: September - December 2022, Available at: www.noveltyjournals.com

The denial of service attack can thus block a file server, make it impossible to access a web server or prevent the distribution of e-mail in a company.

The attacker does not necessarily need sophisticated equipment. Thus, some DoS attacks can be executed with limited resources against a larger and more modern network. This type of attack is sometimes called an "asymmetric attack" because of the difference in resources between the protagonists.

The first attacks were perpetrated by a single “attacker”; quickly, more advanced attacks appeared, involving a multitude of attackers. This is called DDoS (distributed denial of service attack). Some hackers have specialized in "raising" armies of "zombies" which they can then hire out to other malicious people or groups to attack a particular target. With the sharp increase in the number of commercial exchanges on the Internet, the number of denial of service blackmails has risen sharply2.

3. AMPLIFICATION-BASED DDOS ATTACK

Also called a volumetric attack, an attack based on amplification aims to exhaust the available network bandwidth in order to make one or more services inaccessible. This type of attack is often carried out by exploiting the properties of certain protocols in order to maximize the volume of traffic generated. In addition, volumetric attacks aim to generate a very large number of packets per second in order to saturate the processing resources of a target.

Some protocols generate responses much larger than the request. The number of packets induced by the response can also be larger than the number of packets needed to send the request. The amplification generated by these protocols can be exploited to carry out volumetric attacks.

Most of the time, volumetric attacks take advantage of reflection and amplification. There are a number of protocols that can be leveraged to carry out these types of attacks. These include DNS (Domain Name System), NTP (Network Time Protocol), SNMP (Simple Network Management Protocol), SSDP (Simple Service Discovery Protocol), or CHARGEN (Character Generator protocol).

It is important to note that an entity can be the victim of a volumetric attack exploiting a protocol even though it does not have an active service exposed on the Internet based on this same protocol.

An entity can be the victim of a volumetric DDoS attack exploiting a protocol although it does not expose a service based on this same protocol.

4. SOME COUNTERMEASURES TO AMPLIFICATION-BASED DDOS ATTACKS

The objective of this point is to propose a certain number of countermeasures against DDOS attacks, particularly against those based on amplification.

It is important to note here that we have listed several countermeasures which we have tried to summarize in these few points below:

- Countermeasure 1: preparing a DDoS response plan

The first countermeasure against DDoS attacks is to prepare a plan focused on how the business will react in the event of a successful attack. It is a question here of setting up a detailed plan; the more complex the structure, the more important it will be to be clear when writing this plan. This response plan should include:

- A systems checklist
- A trained response team
- Notification and escalation protocols
- How to continue operations
- List of mission critical systems
- List of internal and external entities that must be notified of an attack

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 9, Issue 3, pp: (29-32), Month: September - December 2022, Available at: www.noveltyjournals.com

- Countermeasure 2: Decrease attack surface exposure

The approach here is to minimize the scope of the attack and the intensity of the damage by reducing the surface exposed to the threat actors. It is important here to protect documents, applications, ports, protocols, servers and other important entry points to avoid DDoS attacks.

Consideration should also be given to using load balancers to protect web servers and compute resources from exposure.

- Countermeasure 3: Keep an eye out for red flags

Take DDoS protection measures if you notice any of the following signs:

- Excessive traffic on a specific webpage or endpoint;
- Frequent crashes;
- Slow performance;
- Low connectivity;
- Unusual traffic from a single group or single IP address.

It is important to understand that not only is heavy traffic dangerous, but low traffic and short duration can also lead to breaches.

- Countermeasure 4: Provision of server redundancy

The use of multiple distributed servers makes it difficult for malicious actors to hit all servers simultaneously. The other servers will remain safe if they launch an attack on a single hosting device. They can also support the traffic load until the targeted system is back online.

To avoid network bottlenecks, you can host servers in data centers and colocation facilities located in different geographies. A CDN can also help you distribute the load.

- Countermeasure 5: Moving to the Cloud

Moving to the cloud does not eliminate the risk of DDoS attacks, but it does help mitigate their effects. The high bandwidth of the cloud distributes your data.

You can also read the top 5 email security tools of all time to stay ahead of threat actors.

- Countermeasure 6: Develop and practice good cyber hygiene habits

Your team should be trained to practice good cyber hygiene habits to prevent DDoS attacks. These habits include:

- Set strong passwords and change them regularly. A unique and complex password has at least 12 characters, including numbers, symbols, upper and lower case letters.
- Avoid sharing and reusing passwords.
- Use multi-factor authentication to add an extra layer of security to your accounts. Thus, hackers will not be able to access it despite stealing your passwords.
- Employ device encryption on laptops, tablets, smartphones, external drives, backup tapes and cloud storage for DDoS protection

- Countermeasure 5: early detection and continuous profiling of traffic and packets

Early detection is essential for DDoS protection. The most effective way is to regularly monitor website traffic, requests, and data packets to understand patterns and behaviors. This helps you block malicious traffic and requests, as well as payloads.

Ask your team to react according to the prepared response plan if they notice suspicious activity. This gives you enough time to prevent DDoS attacks.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 9, Issue 3, pp: (29-32), Month: September - December 2022, Available at: www.noveltyjournals.com

5. CONCLUSION

Businesses should take steps to prevent DDoS attacks because they can impact your finances, customer relationships, and brand equity. Start by creating a response plan, so your team knows what to do in the event of an attack. Educate people to notice the warning signs like unusual traffic from an IP address, poor connectivity, slow performance, frequent crashes, etc.

REFERENCES

[1] Arbor Networks Releases Fifth Annual Infrastructure Security Report [archive] - Arbor Networks, 2010 January 19

[2] Kaspersky Lab, « Denial Of Service: How Businesses Evaluate The Threat Of Ddos Attacks », It Security Risks Special Report Series, 2015, p. 2

[3] Anonymous activists target Tunisian government sites [archive] - BBC, 4 janvier 2011

[4] PlayStation Network hackers access data of 77 million users [archive] - Ben Quinn et Charles Arthur, The Guardian, 2011 April 26

[5] WikiLeaks: des millions de cyberattaques [archive] - Le Figaro/AFP, 2020 december 03

[6] Leading Tibetan news portal suffers from DDoS attacks [archive] - Lobsang Wangyal, Tibet Sun, 2010 november 10

[7] « Message Regarding the ProtonMail DDoS Attacks » [archive], ProtonMail, 2015 november 10