EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
UIF = 8.1 | SJIF = 5.685
www.in-academy.uz

DDOS ATTACKS AND PROTECTION AGAINST THEM

[1]Yalg‘ashov Anvar Ikrom o‘g‘li
yalgashovanvar@gmail.com
Termiz State University
Teacher of the Department of Information Technologies

[2]Fayzullayev Ikrom Yusub o'g'li
fayzullayevikrom01@gmail.com
Termiz State University
Teacher of the Department of Information Technologies

[3]Norqobilov Sobir Hamza o'g'li
sobirnorqobilov6@gmail.com
Termiz State University
Teacher of the Department of Information Technologies

https://doi.org/10.5281/zenodo.7476343

ARTICLE INFO

Received: 13th December 2022
Accepted: 21th December 2022
Online: 23th December 2022

KEY WORDS

DDoS attack- Distributed denial of service, network, website, server, CDN port protocol.

ABSTRACT

A Denial of Service (DoS) attack is an attempt to harm a targeted system, such as a website or application, by making it unavailable to normal end users. Typically, attackers create a large number of packets or requests that overload the target system. An attacker uses many compromised or controlled resources to carry out a distributed denial of service (DDoS) attack. In general, DDoS attacks can be divided into types based on the level at which the attack occurs in the Open Systems Interconnection (OSI) model. Attacks on the network layer (layer 3), transport layer (layer 4), presentation layer (layer 6), and application layer (layer 7) are the most common.

Enter

According to experts, the total number of DDoS attacks will increase from 7.9 million in 2018 to more than 15 million by 2023. One of the reasons for this significant increase is that DDoS attacks are very easy to defeat, which makes them very attractive to cyberattackers. criminals around the world.

Research shows that small businesses can lose up to $120,000 per DDoS attack, while enterprise-level attacks can cost $2 million.

So it doesn't matter if you're a small business or a large multinational conglomerate, your online services, including email, websites, and everything else that faces the internet can be slowed down or completely blocked by a DDoS attack.

In this article, we list the most common types and offer resources to protect against DDoS attacks. DDoS Attacks in Brief Distributed Denial of Service or DDoS attacks are malicious attempts to block a business from its traffic. During a DDoS attack, the target server is flooded with malicious traffic generated by exploited systems on the Internet.

One of the first ways to neutralize DDoS attacks is to minimize the size of the attack zone. This technique limits the ability of attackers to attack and allows for the creation of a centralized defense. You must ensure that the application or resources do not affect ports, protocols, or applications that you do not intend to interact with. Thus, minimizing the number of possible attack points allows you to focus on neutralizing them. In some cases, this can be achieved by placing your computing resources behind content delivery networks (CDNs) or load balancers, and by restricting direct Internet traffic to certain parts of your infrastructure, such as database servers. You can also use firewalls or access control lists (ACLs) to control what traffic your applications receive. Two key elements in mitigating large-scale DDoS attacks are bandwidth (or transit capacity) and sufficient server performance to receive and mitigate the attacks.

transit capacity. When designing applications, you need to make sure that your hosting provider provides excess Internet bandwidth that can handle large amounts of traffic. Since the ultimate goal of DDoS attacks is to affect the availability of resources or applications, they should be located near large Internet processing nodes that provide easy access not only to end users, but also to users of even large-scale applications. traffic jam. Working with Internet applications gives even more opportunities. In this case, you can use content delivery networks (CDNs) and DNS Intelligent Address Translation services, which provide an additional layer of network infrastructure to serve content and resolve DNS queries from locations that are often closer to end users. provides

Server performance. Most DDoS attacks are large and resource intensive, so it's important to be able to scale up or down your computing resources quickly. This can be achieved by using redundant computing resources or resources with special capabilities such as faster network interfaces or improved network configuration to support the processing of large volumes of traffic. In addition, appropriate load balancers are often used to continuously monitor and distribute loads among resources and prevent any resource from becoming overloaded.

When your site is the victim of a DDoS attack, your website will be down for a while or a very long time depending on the intensity of the attack. Protecting your website from DDoS attacks by hackers to take over your server resources means to implement a number of solutions to deal with fake traffic sent by

Website owners don't have to wait until their sites are attacked before taking action. It is recommended to take a proactive approach against DDoS attacks, and here are some non-technical, effective solutions to protect your website from this malicious traffic.

Here are some things you can do to protect your site or web applications from various types of DDoS attacks and help keep your website always online.

One of the most basic steps you can take to protect against DDoS attacks is to "DDoS-proof" your hosting infrastructure. Essentially, this means that you have prepared enough bandwidth to handle possible congestion caused by cyber attacks.

Note that buying more bandwidth alone is not a complete solution to DDoS mitigation. When you increase bandwidth, it raises the bar that attackers must overcome before launching a successful DDoS attack, but you should always combine this with other mitigation tactics to fully protect your website.

CDN providers offer many cyber security features and tools to protect your website from hackers. They also offer free SSL certificates. Also, when you add your website to these service providers, it provides DDoS protection by default to mitigate attacks on your server network and application.

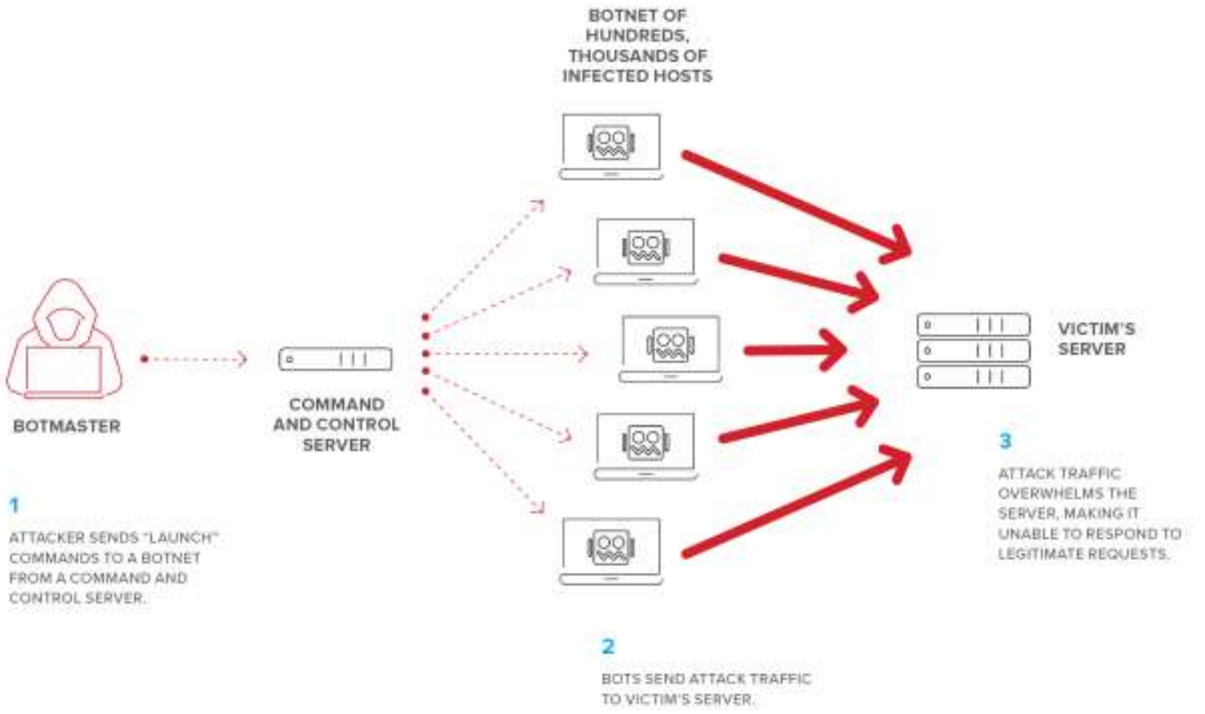
The rationale for this is that when you use a CDN, all malicious requests directed at L3/L4 that do not come through ports 80 and 443 are automatically filtered due to the CDN port protocol.

Using a CDN can balance website traffic so that your limited server is not overwhelmed. In addition, CDNs distribute your traffic across servers in different locations, making it difficult for hackers to identify your original server to launch an attack.

In addition, with a Multi CDN solution, you will be able to use a large PoP network of not just one, but several CDN providers, allowing your website to withstand multi-terabit per second DDoS attacks. global distributed network.

Some web hosts include server-level DDoS mitigation tools in their offerings. As this feature is not always offered by web hosting companies, you should check with your web host. Some companies include it as a free service, while others offer it as a paid add-on. It all depends on the provider and hosting plan.

Planning ahead for a cyber attack allows you to respond quickly before they do damage to your website.


BOTNET OF HUNDREDS, THOUSANDS OF INFECTED HOSTS
BOTMASTER
COMMAND AND CONTROL SERVER
VICTIM'S SERVER
1
ATTACKER SENDS "LAUNCH" COMMANDS TO A BOTNET FROM A COMMAND AND CONTROL SERVER.
2
BOTS SEND ATTACK TRAFFIC TO VICTIM'S SERVER.
3
ATTACK TRAFFIC OVERWHELMS THE SERVER, MAKING IT UNABLE TO RESPOND TO LEGITIMATE REQUESTS.

A proper cyber security plan includes a list of potential attackers. It also determines that the system prioritizes resources to keep many applications and services online, which can cause your business to crash. Finally, you can plan how to contact the ISP supporting the attack, as they may be able to help stop it altogether.

Many small business owners feel that their scale is not large enough to be a victim of cyber attacks. However, the reality is that cybercriminals target small businesses and startups more than large enterprises. This is because large companies are usually more inclined to implement security solutions to combat the attempts of hackers.

As mentioned above, small businesses can lose up to $120,000 per DDoS attack, so your website may be a victim of hackers and you should work on improving your website security.

When you switch to hybrid or cloud-based services, you get access to unlimited bandwidth. Many websites affected by DDoS are resource-constrained sites. Moving to a cloud-based solution will help you stay on the safe side.

You can prevent a DDoS attack by making a few simple hardware configuration changes.

For example, you can configure your firewall or router to drop incoming ICMP packets or block DNS responses from outside your network (by blocking UDP port 53). This helps protect against certain DNS and ping-based volume attacks.

Summary

Given that the number of DDoS attacks is increasing significantly, and that each attack can have devastating consequences for every business, regardless of its size and scale, it is necessary to think about DDoS attack mitigation tactics sooner.

The above tips and tactics will help you increase your website security and protect against cyber attacks.

References:

1. Social Engineering: The Science of Human Hacking 2nd Edition
by Christopher Hadnagy
2. Cyber Threat Hunting: Nadhem AlFardan
3. Enterprise Cybersecurity in Digital Business: Ariel Evans
4. Making Sense of Cybersecurity: Thomas Kranz