

EVERYTHING YOU NEED TO KNOW ABOUT DDOS ATTACKS





DDoS attacks are on the rise, and they can be devastating to anyone who experiences them.

That's why it is so important to understand what a DDoS attack is and know how to identify it and protect your business from one.

What is a DDoS Attack?

A DDoS (Distributed Denial of Service) attack happens when an attacker uses multiple devices to flood their targets' server networks with so much traffic that their bandwidth or resources get overwhelmed.

Basically, instead of using one computer to send requests for information at once, they use hundreds or thousands of compromised computers all at once! This overloads servers until they become unavailable and causes a denial-of-service condition that keeps legitimate users out.

DDoS attacks are a type of cyber-attack that can happen to anyone. They are also one of the most challenging types of attacks to defend against because it's not just a matter of blocking an IP address or two - you must identify which devices were compromised to take them out and keep your network secure!

How Do You Know If You Are Under a DDoS Attack?

Generally, the first sign of a DDoS attack is an increase in traffic. You might notice that your site's statistics have spiked, or you may find it difficult to load pages or send emails.

While other reasons may have caused a spike in your traffic, the following signs may indicate that a business is suffering from a Denial-of-Service (DDoS) assault:

1. Website error messages
2. Slow-loading web pages/timeouts when loading web pages
3. Email service is unavailable or too slow to be of use
4. General slowness and sluggishness with everything you do online
5. Loss of connection, when you can't connect to the internet or other network resources

Types of DDoS Attacks

Every DDoS attack begins when a hacker overwhelms a target system. The process of overwhelming a target system can be done in three ways, and the type of attack will depend on which method is used.

Application Layer Attacks

These are the most common type of DDoS attacks. They overwhelm the target's system by sending a high volume of requests to access the site or service. For these attack types, attackers focus on the server that the site or service is running on.

Volumetric Attacks

These attacks use large volumes of data to flood your website's bandwidth and ground the server due to a lack of available space.

Volumetric attacks manifest commonly as DNS amplification, where hackers use bots to request information, thus taking up large data amounts. The bots then redirect the data to the origin server.

Read more about the different types of DDoS attacks that you should know about.

Protocol Attacks

Protocol attacks occur when attackers target parts of your system and send tons of requests from all directions.

What Can You Do If You're Under A DDoS Attack?

If you suspect that your business is suffering from a DDoS attack, take the first step is to create a timeline and know when the attack started and how long it's been active.



Next, identify applications, services, and servers that have been impacted by the attack and how they are affecting your website visitors and your business as a whole.

Notify your web hosting company of the DDoS attack and manage the attack by performing an IP switch.

Involve a web security service that offers DDoS mitigation services to reduce the extent of the attack.

Alert your website visitors and customers about the attack to avoid frustrations or confusion due to lack of information.

How to Prevent DDoS Attacks

The most effective way of preventing DDoS attacks from bringing your business down is by distributing your resources to multiple locations. That way, it will be difficult for attackers to target your whole business.

It's also important that you monitor your website traffic and have an accurate idea of how your website traffic looks like on a typical day. This will help you spot DDoS attacks early enough and mitigate the problem before it cripples your services.



Configure firewalls and routers in the right way to help in deflecting potentially dangerous traffic. Firewalls and routers then analyze, identify, and block the traffic before it hits your resources. For this to work, your firewalls and routes should remain patched with the latest updates.

You can also use DDoS mitigation services to protect your network from DDoS attacks. Radware, Akamai, and Cloudflare are some of the service providers that help in preventing DDoS attacks.

When choosing a DDoS mitigation service to work with, ensure that you understand your circumstances and needs as an organization. That way, you will be better placed deciding on the type of service you choose for your website.

In conclusion, understanding DDoS attacks and knowing how to mitigate their effects can mean the difference for your business. Knowing the different types of DDoS attacks and how to identify them can help you take preventive action. Having the best mitigation service is important as it can help you quickly recover from a DDoS attack.

References

<https://www.zdnet.com/article/what-is-a-ddos-attack-everything-you-need-to-know-about-ddos-attacks-and-how-to-protect-against-them/>



<https://www.loggly.com/blog/ddos-monitoring-how-to-know-youre-under-attack/>

<https://www.okta.com/identity-101/ddos-attack/>