DDoS Attack

A Distributed Denial of Service (DDoS) attack seeks to overwhelm the capacity of a network resource such as a website or server by sending a massive volume of malicious requests. The main goal is to disrupt the service and make it inaccessible to legitimate users. In some cases, attackers may demand a ransom to stop the attack. Typically, these types of attacks are used to discredit or damage a competitor's business. To send an extremely large number of requests to the victim resource, the hacker uses a "zombie network" of affected computers.

How does it work?

All network resources have a finite limit of requests they can serve at the same time. In addition to the server's capacity limit, the channel that connects the server to the Internet has a limited bandwidth capacity. When there is a number of requests that exceeds the capacity limits, the services are affected, as follows:

- The attack consumes all available bandwidth.
- The server is overwhelmed by the number of requests and cannot process them all

How to detect a DDoS attack?

There is no way to detect a DDoS attack, but there are signs that can help identify it.

- Unusual and sudden increase in web traffic.
- Irregular performance or slow network
- The website goes offline completely

How to avoid it?

- Develop a defense strategy.
- Identify security gaps and assess potential threats in the configuration.

How to protect against a DDoS attack?

- Conduct a risk analysis on a regular basis.
- Organize a DDoS response team.
- Incorporate intrusion detection and prevention tools.
- Evaluate the effectiveness of the defense strategy.