DDOS ATTACK

What is a DDoS Attack and What Should I do About It?

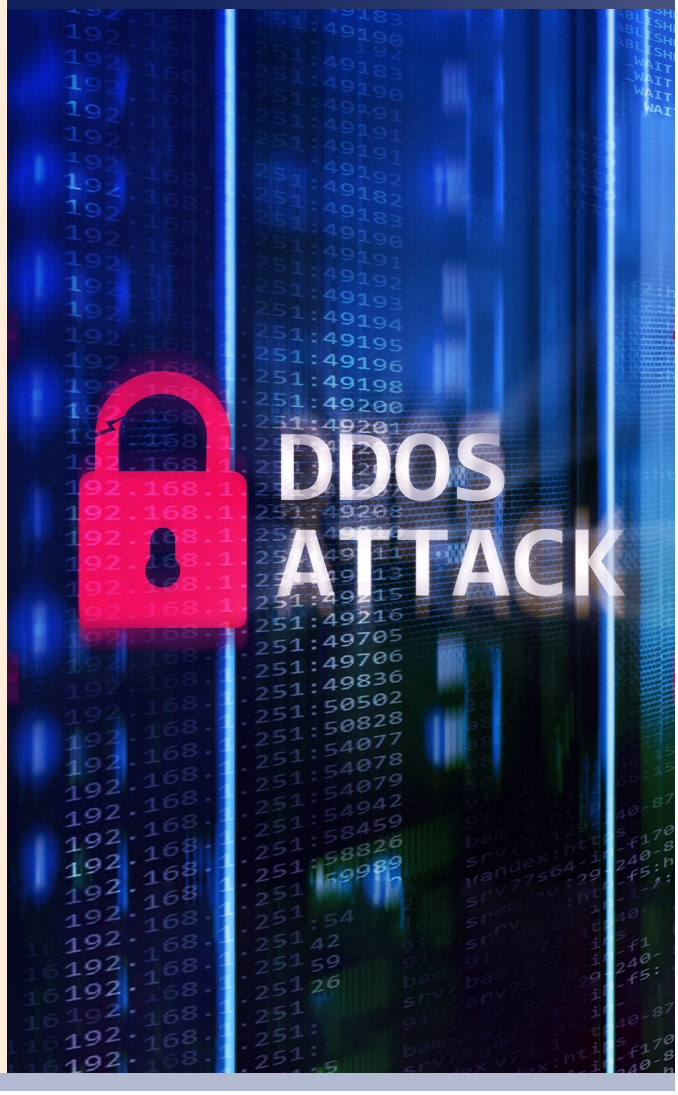
The term **"DDoS attack"** has become increasingly common in today's connected world, so ubiquitous that household name companies and even nations have been the targets of enormous DDoS attacks. Distributed Denial of Service (DDoS) attacks are a form of cyber threat that can cripple online services, disrupt businesses (and nations) and undermine cybersecurity efforts. This article will explore what a DDoS attack is, how it works, and why it poses risks to both organizations and individuals.

What is a DDoS Attack?

A DDoS attack is a malicious attempt to disrupt the functioning of a computer network, service, or website by overwhelming it with a flood of internet traffic. Such an attack can vary in size and complexity, but its primary goal is to render the targeted system unavailable to users.

Key Characteristics:

1. **Distribution:** Unlike traditional cyber-attacks, which are carried out from a single source, DDoS attacks involve multiple compromised devices distributed across varying geographic locations. The distributed nature of the attack makes it highly challenging to trace the source of the original attack and to mitigate its impacts.
2. **Volume:** DDoS attacks are characterized by a massive volume of traffic sent to the target. This can overwhelm the target's servers, leading to service degradation or complete unavailability.
3. **Variety:** Attackers use a variety of techniques to launch DDoS attacks. They may use UDP (user data protocol) floods, SYN (half open connection) floods, HTTP (hypertext transfer protocol) floods, and DNS (domain name server) amplification attacks. Others have been dubbed with names such as "Ping of Death, "Smurf Attack," or "My Doom." Don't let the cute names fool you, though, as each of these techniques exploit specific vulnerabilities in the target's infrastructure.
4. **Botnets:** Most DDoS attacks are orchestrated using botnets, which are networks of compromised devices under the control of a malicious actor. These devices can be computers, servers, IoT (internet of things) devices, and even smartphones.



DDOS ATTACK

How does a DDoS Attack Work?

DDoS attacks generally follow this basic pattern:

1. **Recruitment of Botnets:** An attacker is a composition of a multitude of devices, either through malware, phishing and other means, assembling a botnet.
2. **Command and Control:** The attacker gains control over the botnet and commands it to send a flood of traffic to a specific target. By controlling the botnet, the attacker can tap into vast amounts of aggregate computing power to launch the automated DDoS.
3. **Traffic Flood:** The compromised devices in the botnet simultaneously send requests or data to the target, overwhelming its resources.
4. **Service Disruption:** The targeted system becomes incapable of handling the excessive traffic, causing service degradation or complete unavailability for legitimate users.

How to Indentify a DDoS attack:

The hallmark of a DDoS attack is when a site or service suddenly becomes slow or unavailable. However, as a legitimate spike in traffic can also create similar signs, further investigation is usually needed. Analytic tools can help spot some other signs, including:

- Suspicious amounts of traffic coming from a single IP location;
- An unexplained surge in requests to a single page or endpoint;
- A flood of traffic from users with a shared characteristic such as a single device type, geolocation, or web browser version;
- Unusual traffic patterns such as traffic spikes at unusual times of day or odd spike patterns, such as every 15 minutes.

How to Prevent a DDos Attack?

Protection against DDoS attacks is crucial for organizations. The key to mitigation is differentiating between attack traffic and legitimate traffic. Some best practices include:

1. **Traffic Filtering:** Employing traffic filtering mechanisms to distinguish legitimate traffic from malicious traffic.
2. Organize a **DDoS Attack Response Plan in advance.**
3. **Activate a Web Application Firewall (WAF):** A WAF is a set of rules and policies that help protect web applications and application programming interfaces (API) against attacks.