DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK

Distributed Denial of Service (DDoS) attacks are a subclass of denial of service (DoS) attacks. In general, a DoS attack refers to the deliberate attempt by an attacker to make your website or application unavailable to users through sending excessive illegitimate traffic to overload your system through a single source.

A DDoS attack on the other hand, involves the attacker utilising multiple sources such as connected online devices or botnet, with the same objective of flooding the system with huge bandwidths and denying access to the users.

Overview of DDoS Attack

In the year 1998, well-known hacker Khan C. Smith demonstrated to the world what a DoS (Denial of Service) Attack is, and the Internet since then, was never the same again.

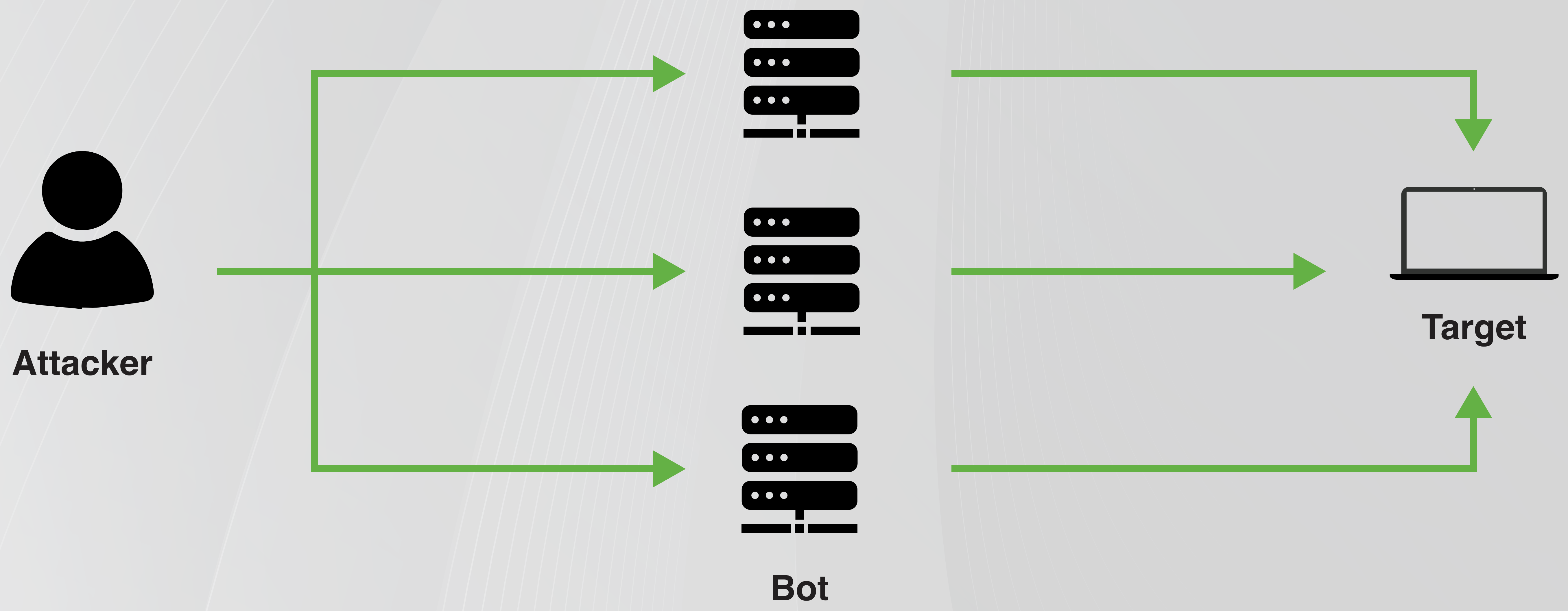
Whereas DoS (denial-of-service) attacks are sent by one person or system, a distributed denial-of-service (DDoS) attack usually involves two or more persons or bots to make a machine, computer or network resource unavailable to its intended users. These attacks may indefinitely interrupt or suspend services of a host on the Internet.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as the government, banks, credit card payment gateways, e-commerce portals and even name servers.

Whatever the motives may be, ultimately the attackers want your business operations disrupted. As a testament to its effectiveness, there has been no letup in DDoS attacks ever since it emerged two decades ago. In fact, the contrary is true. Today the frequency of DDoS attacks averages at 28 per hour. It is ever on the rise, and is a real problem.

How does it work?

The attacker uses multiple connected devices or bots to flood the system with crushing volumes of traffic with the aim to infect and bring down the target's application or website.



Examples of DDoS attacks

Network Volumetric DDoS Attack

Overwhelm the targeted network capacity and centralised DDoS mitigation scrubbing facilities with high amounts of traffic

Protocol Attack

Consume the processing capacity of an actual server/infrastructure resource with malicious connection requests

Web Application Attack

Target vulnerabilities within applications and bring them down by creating huge number of seemingly legitimate and innocent requests

Prevention Tips

Secure your network infrastructure
Implement an anti-DDoS solution that is able to effectively screen and scrub malicious traffic so that only legitimate traffic passes through your network.

Perform a Network Vulnerability Assessment
Identify possible security exposures and network vulnerabilities as to be prepared when an attack does occur.

LGA
BUSINESS
UN-INTERRUPTED™

In business for the last 25 years, LGA is one of the top B2B Services-Based Operators (SBO). LGA's Headquarters is in Singapore with a regional presence, as a System Integrator for Connectivity, CyberSecurity & Compute solutions, serving 2000 Enterprise, SME, regional and MNC customers. Our backbone is across multiple data centres, with our security and network operations team operating 24x7x365.

sales@lgatelecom.net ☎ +65 6892 2308 lgatelecom.net