Distributed Denial-of-Service (DDoS)

Return to Glossary

A **Distributed Denial-of-Service (DDoS)** is malicious attack attempting to disrupt normal traffic of a targeted Server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as Internet of Things (IOT) devices.

Source: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

In a distributed Denial-of-Service (DoS) attack, multiple compromised computer systems attack a target and cause a denial of service for users of the targeted resource. The target can be a server, website, or another network resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

Many types of threat actors, ranging from individual criminal hackers to organized crime rings and government agencies, carry out DDoS attacks. In certain situations – often ones related to poor coding, missing patches, or unstable systems – even legitimate, uncoordinated requests to target systems can look like a DDoS attack when they are just coincidental lapses in system performance.

Source: https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack