(Distributed) Denial of Service

A denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

A distributed denial-of-service (DDoS) attack occurs when multiple machines are operating together to attack one target. DDoS allows for exponentially more requests to be sent to the target, therefore increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

DDoS attackers often leverage the use of a botnet—a group of hijacked internet-connected devices to carry out large scale attacks. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack.

Once established, the botnet—made up of compromised devices—may also be rented out to other potential attackers. Often the botnet is made available to “attack-for-hire” services which allow even the most unskilled user to launch DDoS attacks.

DDoS attacks have increased in magnitude as more and more devices come online through the Internet of Things (IoT) IoT devices often utilize default passwords and do not have sound security postures, making them vulnerable to compromise and exploitation. Infection of IoT devices often goes unnoticed by users, and an attacker could easily compromise hundreds of thousands of these devices to conduct a high-scale attack without the device owners’ knowledge.