Botnets

A botnet is a network of devices that have been compromised and can be controlled remotely by a single entity, known as the botmaster. These devices, which may include computers, smartphones, and Internet of Things (IoT) devices, have malware installed on them that allows them to be controlled remotely. Once a device is infected and becomes a part of a botnet, it can be used for various nefarious purposes. One way that botnets are often used is for distributed denial of service (DDoS) attacks, in which the botnet is used to overwhelm a website or server with traffic, rendering it inaccessible to legitimate users. This can disrupt the operations of businesses, organizations, or even entire countries. Botnets are also commonly used for spamming and phishing campaigns, sending large volumes of spam emails or phishing messages with the aim of tricking people into divulging sensitive information or installing malware on their devices. Another use for botnets is cryptocurrency mining, in which the botmaster uses the compromised devices in the botnet to complete complex mathematical calculations to mine for cryptocurrency. This can be done without the knowledge or consent of the device owners, potentially causing slowed performance or damage to the device.