What is a Botnet?

A botnet is a network of hijacked computer devices that are used to conduct various crimes and cyber attacks. Botnet assembly is often the infiltration step of a multi-layer strategy. Bots are used to automate large-scale attacks including data theft, server crashes, and virus spread. To delay their ability to take advantage of the botnet, hackers usually take every precaution to make sure the victims are unaware of the infection. To an organization's cyber security. Botnets create several threats. If an organization's systems are detected with malware, they can be recruited into a botnet and used to launch automated attacks on other systems.

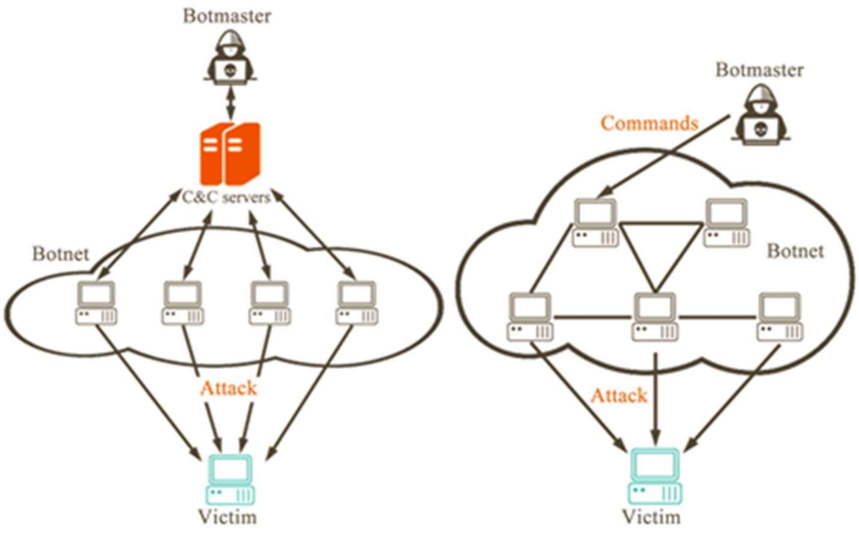
Several of the most common reasons botnets are created include:

- Cryptocurrency mining
- Theft of financial and sensitive information
- Sabotage (such as taking services or sites offline)
- Cyberattacks (such as phishing, ransomware, and distributed denial-of-service attacks)
- Selling access to other cybercriminals (i.e., botnet-as-a-service).

Types of Botnets

Botnets come in different forms based on their structure and control. Understanding these types helps you identify and mitigate threats more effectively.

- **Centralized Botnets**: These rely on a single command-and-control (C2) server. All infected devices (bots) connect to this central point for instructions.
  - Pros for attackers: Simple to manage and deploy.
  - Weakness: If the C2 server is taken down, the entire botnet can collapse.
- **Decentralized (Peer-to-Peer) Botnets**: Instead of a central server, bots communicate with each other in a peer-to-peer (P2P) fashion. Each bot can act as both a client and a server.
  - Pros: More resilient to takedown attempts.
  - Challenge for defenders: Harder to trace and shut down due to distributed control.
- **Hybrid Botnets**: Combining centralized and P2P structures. Attackers can push commands centrally, but they can also allow bots to share instructions across the network.
  - Best of both worlds: Flexible control with added resilience.



BOTNET ATTACK