Botnet

Botnets are networks of hacked computer devices that are used to carry out various scams and cyberattacks. Botnet building is usually the infiltration stage of a multi-layered plan, bots serve as a tool to automate massive attacks, such as data theft, server blockade, and malware distribution.

How does it work?

They are developed to increase, automate, and accelerate a hacker's ability to carry out larger attacks. Bot controllers control a set of hacked devices with remote commands. Once a botnet is built, they use command programs to perform the next actions. A botnet can control all types of devices, such as traditional computers and mobile devices.

What are they used for?

- Financial theft.
- Information theft.
- Service sabotage.
- Cryptocurrency scams.
- Selling access to other criminals.

How are they controlled?

- Centralized: They have a direct connection that goes from the cybercriminal to the zombie computers. It is based on the client-server system and has a weak point since the C2 servers are easy to find and deactivate.
- Decentralized: There are several links between all the infected devices. They relegate the client-server model in favor of the peer-to-peer structure, which is known as P2P.

Examples

Cutwail

In 2007, a malware that targeted Windows systems via malicious emails was distributed via the PUSHDO Trojan to turn the infected system into a SPAMBOT. It is believed that it compromised between 1.5 and 2 million infected systems and had the capacity to send 74 billion spam emails per day.