# Botnet

Son redes de dispositivos informáticos pirateados que se utilizan para llevar a cabo distintas estafas y ciberataques. El armado de un Botnet suele ser la etapa de infiltración de un plan de múltiples capas, los bots sirven como herramienta para automatizar ataques masivos, como el robo de datos, el bloqueo de servidores y la distribución de malware.

## ¿Cómo funciona?

Se desarrollan para aumentar, automatizar y acelerar la capacidad de un hacker para llevar a cabo ataques más grandes. Los controladores de bots controlan un conjunto de dispositivos pirateados con comandos remotos. Una vez que se arman una red de bots, utilizan programas de comandos para realizar las próximas acciones. Una Botnet puede controlar todo tipo de dispositivos, como las computadoras tradicionales y dispositivos móviles.

## ¿Para qué se usan?

- Robo financiero.
- Robo de información.
- Sabotaje de servicios.
- Estafas con criptomonedas.

## ¿Cómo se controlan?

- **Centralizado:** Poseen una conexión directa que va desde el ciberdelincuente a los equipos zombi. Se basa en el sistema cliente-servidor y poseen un punto débil ya que los servidores C2 son fáciles de encontrar y desactivar.
- **Descentralizado:** Existen varios nexos entre todos los dispositivos infectados. Relegan el modelo de cliente-servidor en favor de la estructura entre pares lo que se le conoce como P2P.

## Ejemplos

### Mirai

En 2016 surge la botnet Mirai, es una de las botnets más grandes y conocidas de internet, llego a ser descubierta por investigadores de seguridad y se propago rápidamente a través de dispositivos IoT infectados. Fue crea con el objetivo de lanzar ataques DDoS contra sitios web y servicios en línea en todo el mundo, llego a utilizar técnicas avanzadas de propagación como escanear automáticamente internet en busca de dispositivos vulnerables y utilizando una lista de contraseñas determinadas comunes para comprometer los dispositivos.