



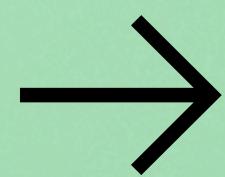
Ciberseguridad



BOTNET 101:

la red secreta detrás
de un solo atacante

Concientización





¿QUÉ ES UNA BOTNET?

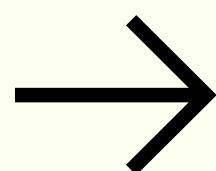
Una botnet (robot network) es una red de dispositivos infectados con malware que los convierte en bots, es decir, máquinas controladas remotamente por un atacante.

- Cada uno ejecuta órdenes sin que el usuario lo sepa.
- El atacante puede controlar cientos o miles de estos bots al mismo tiempo desde un único lugar.
- Se usan para DDos, spam, infectar con malware, y más.

DISPOSITIVOS VULNERABLES:

- PCs y notebooks sin parches
- Routers mal configurados
- Cámaras de seguridad
- IoT con contraseñas por defecto

Concientización





C2: EL CEREBRO DE LA BOTNET

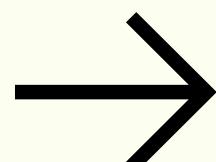
El servidor de C2 (Command and Control) es donde el atacante envía comandos y recibe información. Es la forma de *hablarle* al malware. Los bots se conectan periódicamente al C2 para:

- Pedir nuevas instrucciones
- Informar si cumplieron una orden
- Descargar nuevos payloads

TIPOS DE ARQUITECTURA C2:

- **Centralizada:** un único servidor coordina todo
- **Descentralizada (P2P):** los bots se conectan entre ellos
- **Encubierta:** usando redes sociales, foros o servicios legítimos

Concientización





¿CÓMO SE COMUNICAN? PROTOCOLOS Y CAMUFLAJE

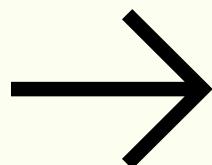
El malware intenta pasar desapercibido. Por eso usa protocolos comunes en la red.

PROTOCOLOS USADOS EN C2:

- **HTTP/HTTPS**: simulan tráfico web
- **DNS**: resuelven dominios especiales con comandos escondidos
- **IRC**: más antiguo, usado en las primeras botnets
- **Custom C2**: protocolos propios para evadir detección
- **TLS**: cifrado para que no se vea el contenido

💡 Muchos bots usan dominios generados automáticamente (DGA), cambiando todos los días para evitar ser bloqueados.

Concientización





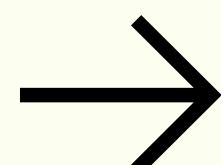
¿CÓMO DETECTARLAS?

Aunque se escondan bien, una botnet deja rastros.

TIPS PARA DETECTAR ACTIVIDAD C2:

- **Analizá tráfico** saliente que no es habitual (por destino, hora o volumen)
- Correlacioná logs de DNS y conexiones externas
- Usá **IDS/IPS** para identificar patrones comunes de botnets conocidas
- **Bloqueá conexiones** a dominios sospechosos o generados por DGA
- **Segmentá la red**: los dispositivos IoT no deberían hablar con todo
- Sumá un **EDR** o **NDR** para monitorear y alertar ante tráfico sospechoso

Concientización





Ciberseguridad

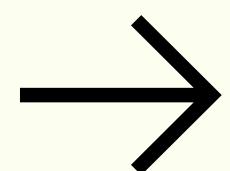
¿POR QUÉ ENTENDER ESTO ES CLAVE EN CIBERSEGURIDAD?

Porque muchos ataques masivos empiezan con una botnet silenciosa. Y esa red necesita comunicarse para funcionar.

🌐 Aprender cómo hablan los bots te ayuda a:

- ✓ Detectar infecciones tempranas
- ✓ Reconocer comportamientos maliciosos
- ✓ Monitorear tráfico que *parece* legítimo, sin serlo
- ✓ Te entrena para pensar como atacante.

Concientización





Ciberseguridad

**SEGUINOS Y
UNITE AL
DISCORD PARA
SEGUIR
APRENDIENDO**

Guardar

Compartir

Seguir

Concientización