

Botnets SWARM, la nueva amenaza

David Castillo System Engineer

Diciembre 2018

Swarm – Supervivencia individual usando el grupo

Comportamiento
colectivo

Los estorninos se agrupan hacia el atardecer para evitar a los depredadores ... crean un "murmullo"



Moviéndose juntos
en alguna dirección con
un objetivo común

Las hormigas construyen estructuras cooperativas y
estrategias de defensa / ataque masivo

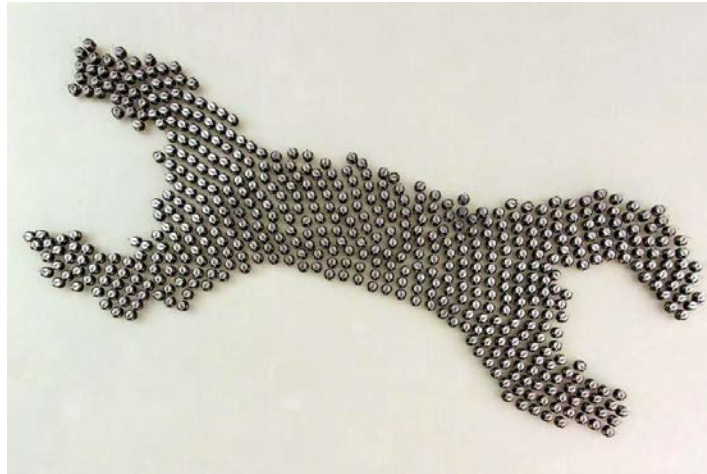


Ejemplos : Swarm Robotics

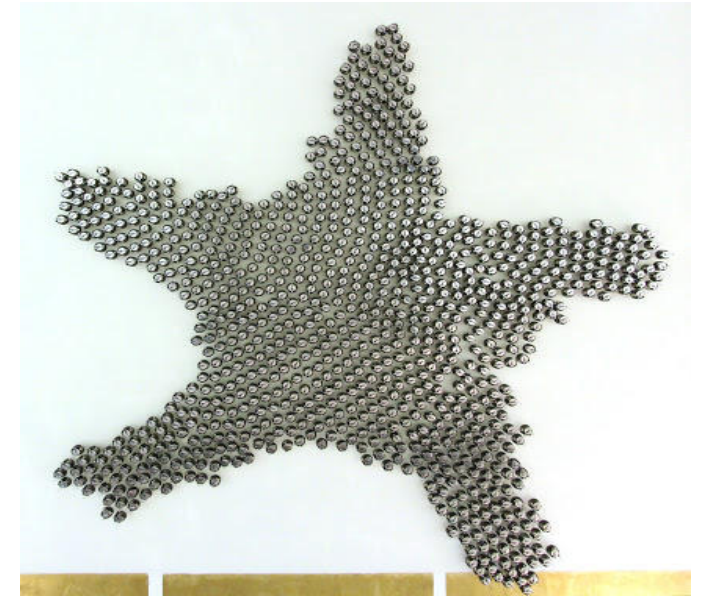
Kilobots: Enjambre sin líderes



Enfoque basado en soluciones



Comunicación entre nodos vecinos

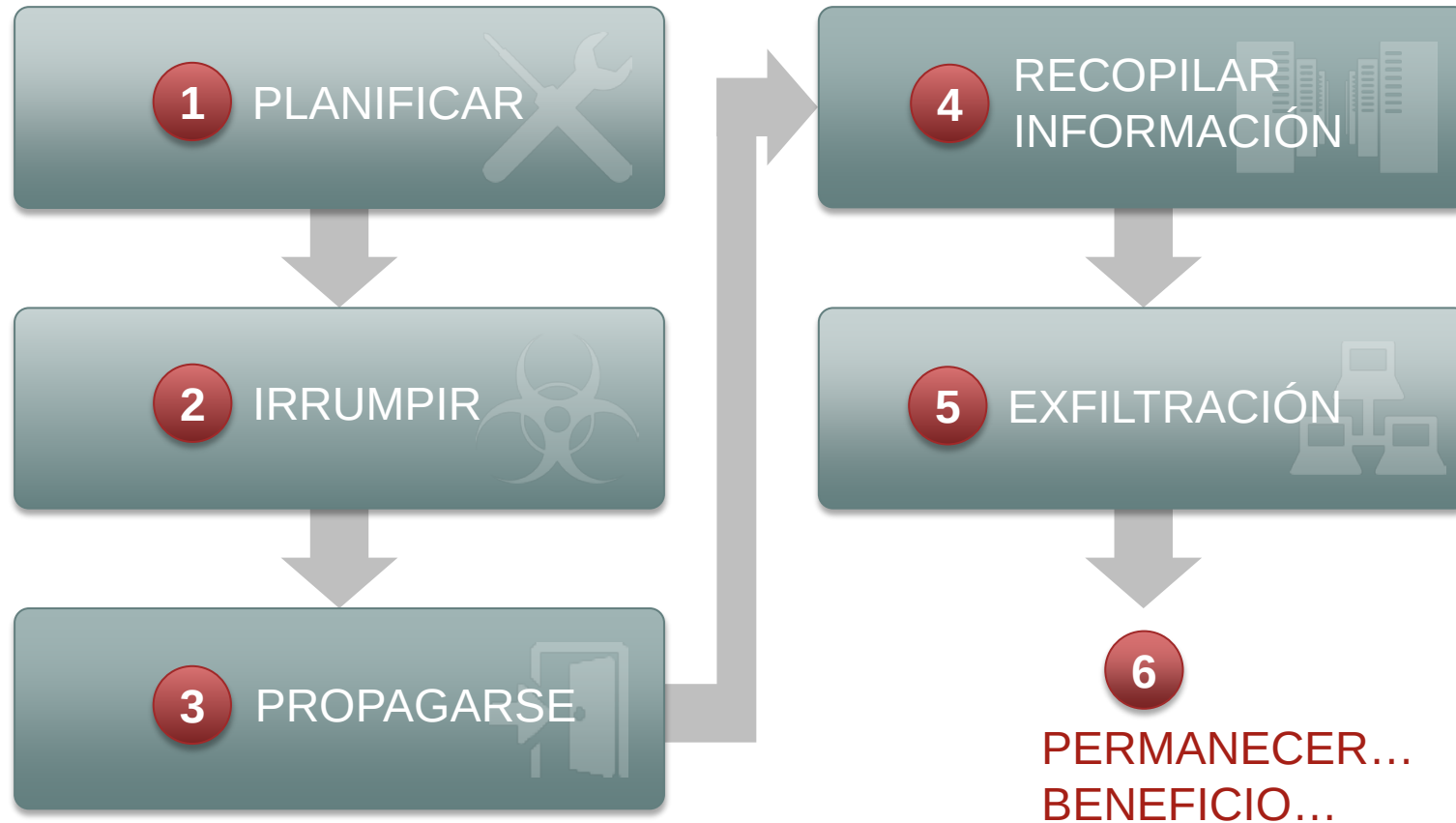




Acelerando la cadena de ataque

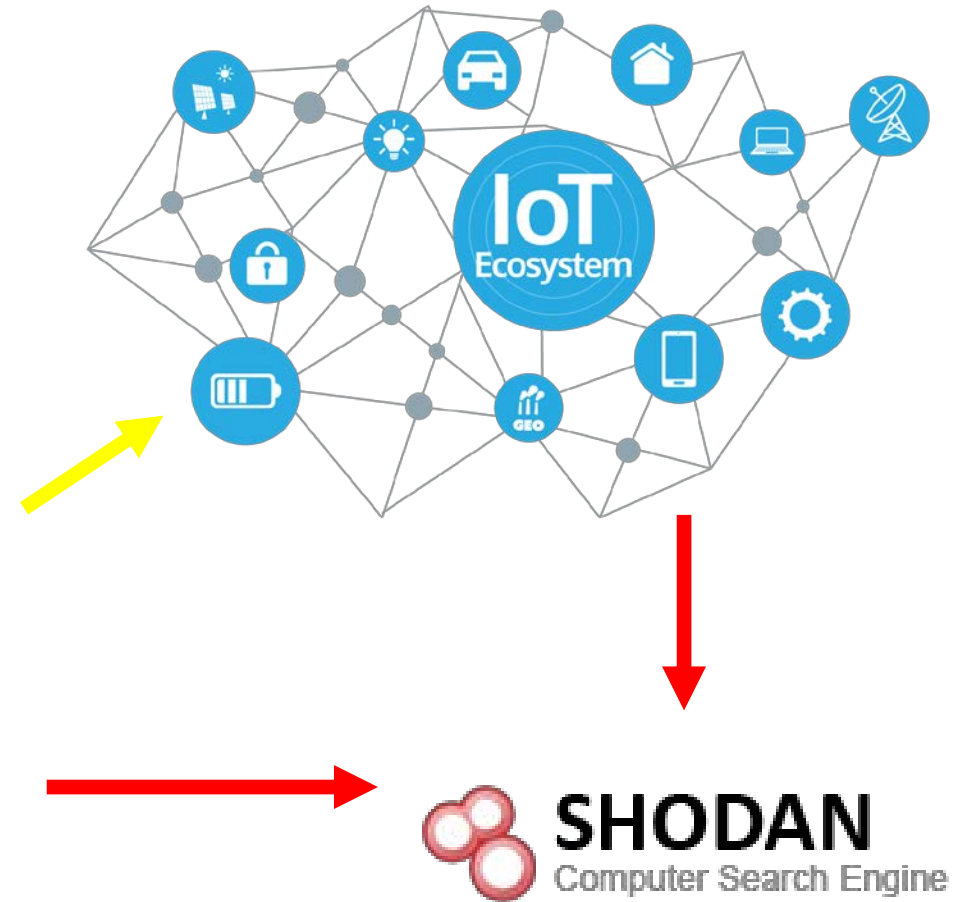
Automatización

Los swarm reducen muchísimo el tiempo de brecha



Autosploit – Construyendo Swarms

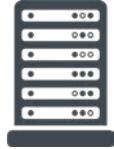
- Shodan es un engine de búsqueda que indexa puertos y servicios
- El atacante realiza consultas a Shodan
- El atacante usa exploits para atacar a sistemas IoT u otros sistemas basándose en información de Shodan.
- El atacante consigue acceso a los sistemas vulnerables.



Componentes típicos de la red de botnet



Atacante



Servidor C&C



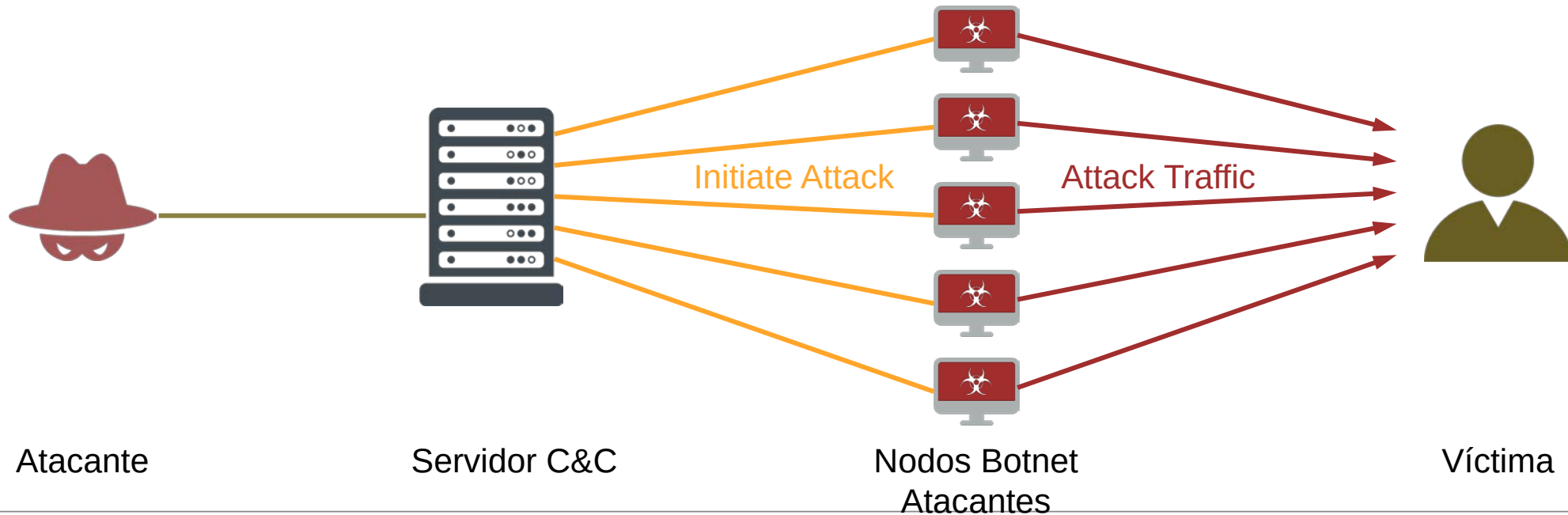
Zombis



Víctima / objetivo



Communications
channels



Blackhat Swarms – Eliminando el C&C

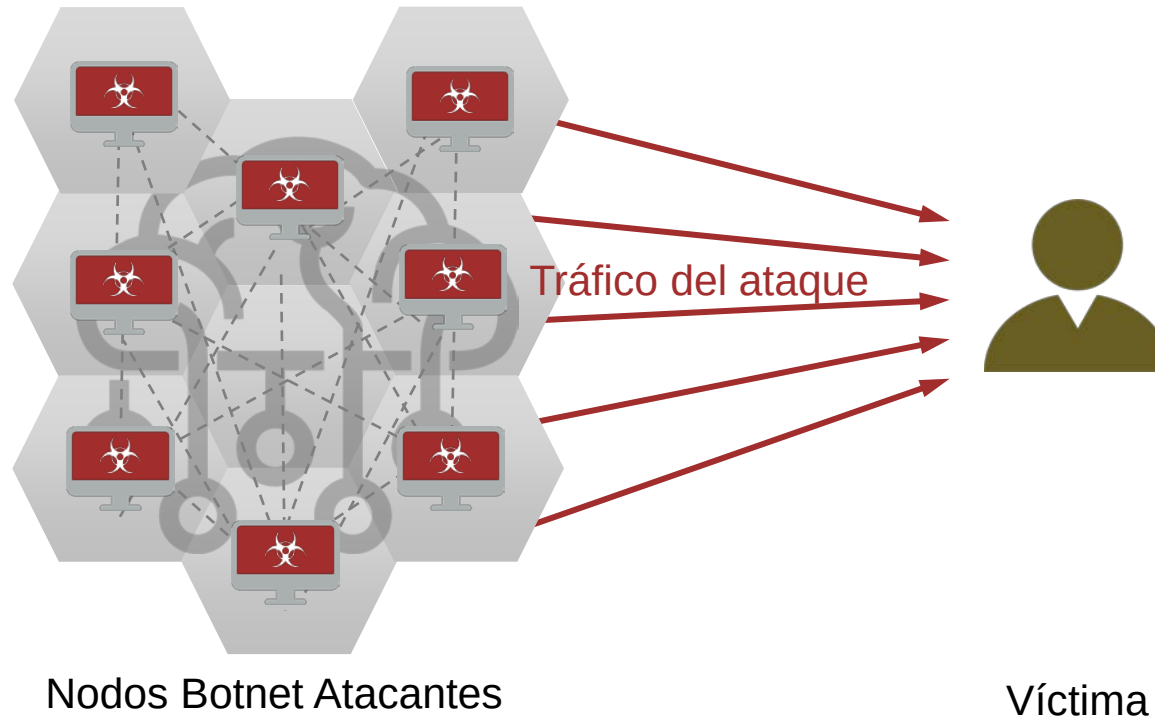
Next Generation Botnet 3.0: Swarm

Qué pasaría si las botnets pudieran utilizar la inteligencia de los enjambres?

- Aceleraría muchísimo la cadena de ataque
 - **Eliminar el componente humano**

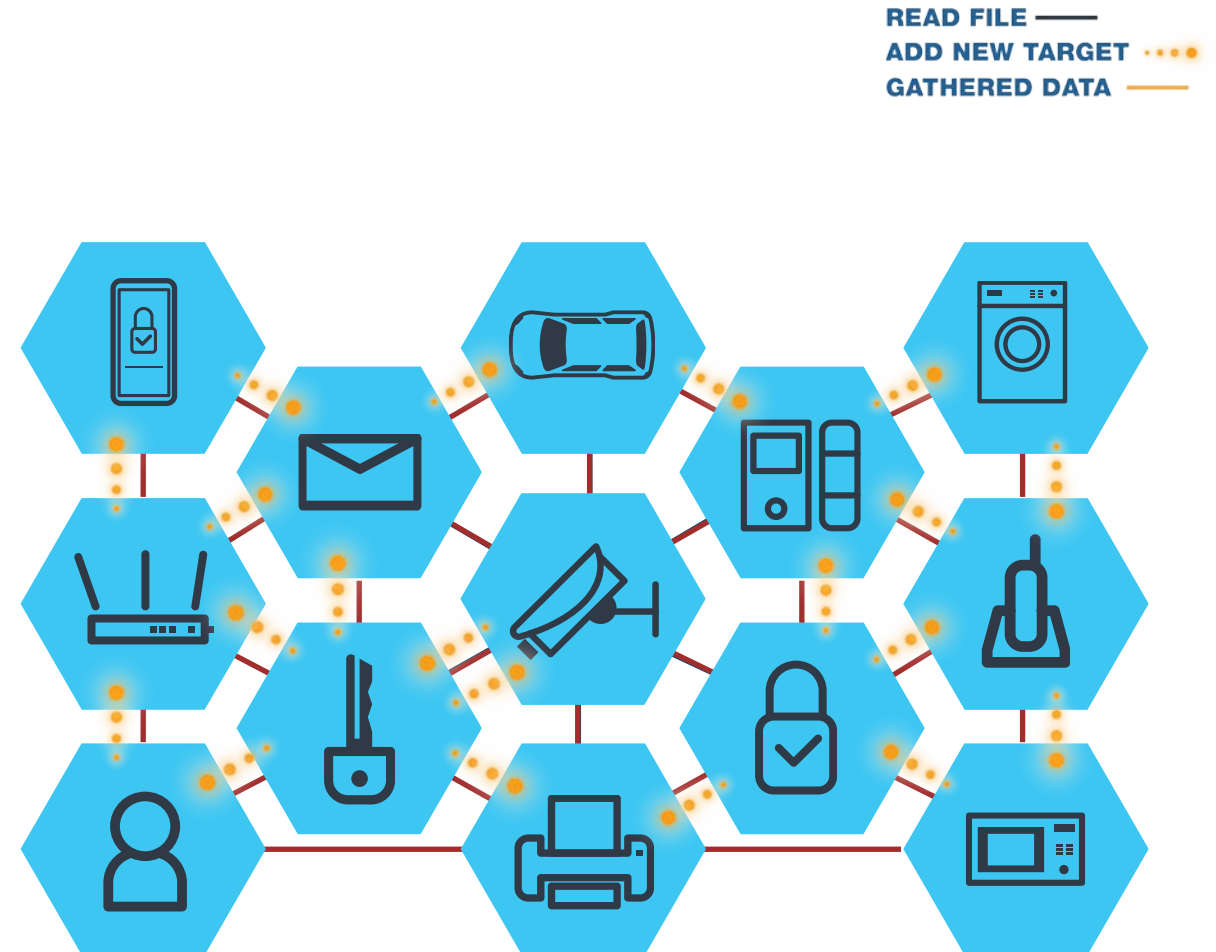
Ejemplo Satori Botnet

- Si la cámara es hackeada o con la carga muy alta, salta dicho objetivo si se encuentran mejores víctimas.



Botnet Hide and Seek

- Segunda red descentralizada P2P IOT botnet
- *Con características de swarm*
- Usa un exploit conocido para propagarse por routers TP Link
- Capacidades Confirmadas
 - AMD x64, ARM
 - Ataques Brute force
 - Lista de objetivos dinámica
 - Comandos de recuperación de archivos a través de nodos P2P
- **Modelo Peer request-response**
 - 'i' petición → 'I' respuesta
 - 'h' petición → 'H' respuesta
 - 'z' petición → 'O' respuesta
 - '~' petición → '^' respuesta



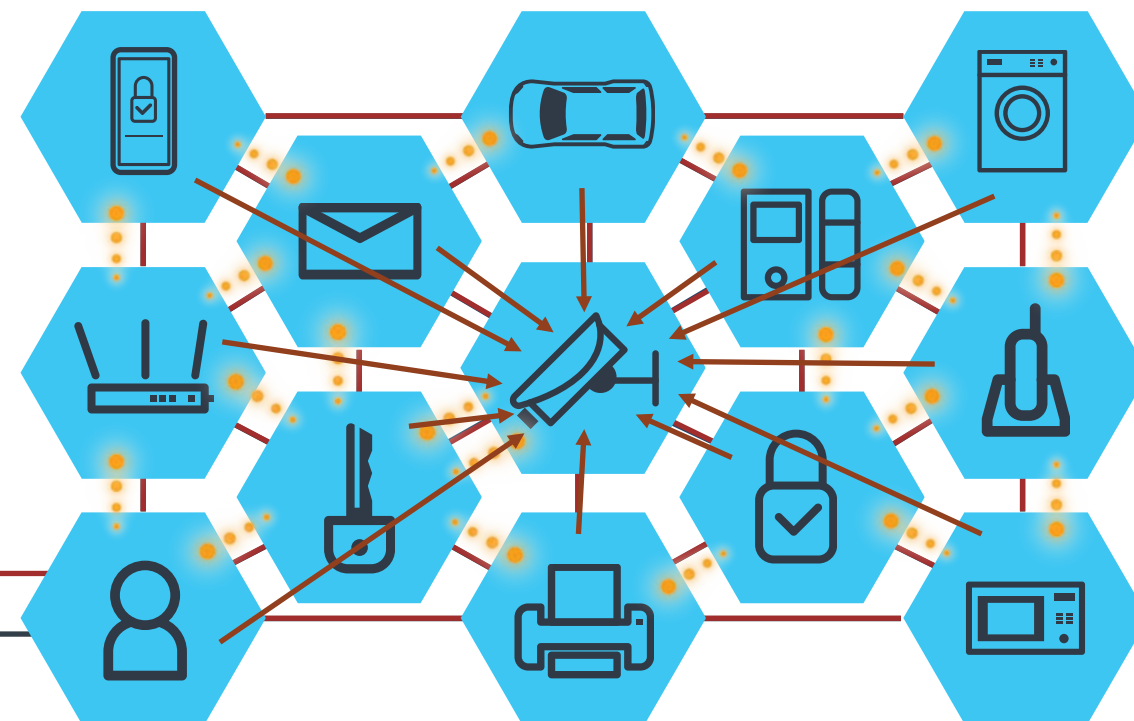
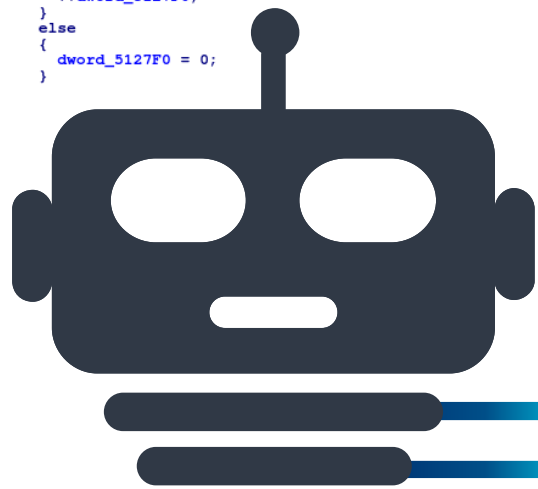
Botnet Hide and Seek

```
arg = (char *)v4[1];
_arg = *arg;
if ( *arg == 'k' )
{
    port = strtol(arg + 1);
}
else if ( *arg > 'k' )
{
    if ( _arg == 'l' )
    {
        sp_port = strtol(arg + 1);
    }
    else if ( _arg == 's' )
    {
        v2 = 0;
        loadfpath(arg + 1);
    }
}
else if ( _arg == 'a' )
{
    sub_40B9B1((__int64)(arg + 1), 0);
}
else if ( _arg == 'e' )
{
    v7 = sub_40E480((unsigned __int64 *)qword_5127E8, 16LL * (unsigned int)(dword_5127F0 + 1));
    qword_5127E8 = v7;
    if ( v7 )
    {
        sub_401346(arg + 1, v7 + 16LL * (unsigned int)dword_5127F0);
        ++dword_5127F0;
    }
    else
    {
        dword_5127F0 = 0;
    }
}
```

- 2) El Objetivo es identificado por el swarm
- 3) El objetivo ahora forma parte del swarm
- 4) La información es filtrada a través del swarm IP, etc)

READ FILE —
ADD NEW TARGET
GATHERED DATA —

's' le path
'm<data>PORT<data>'

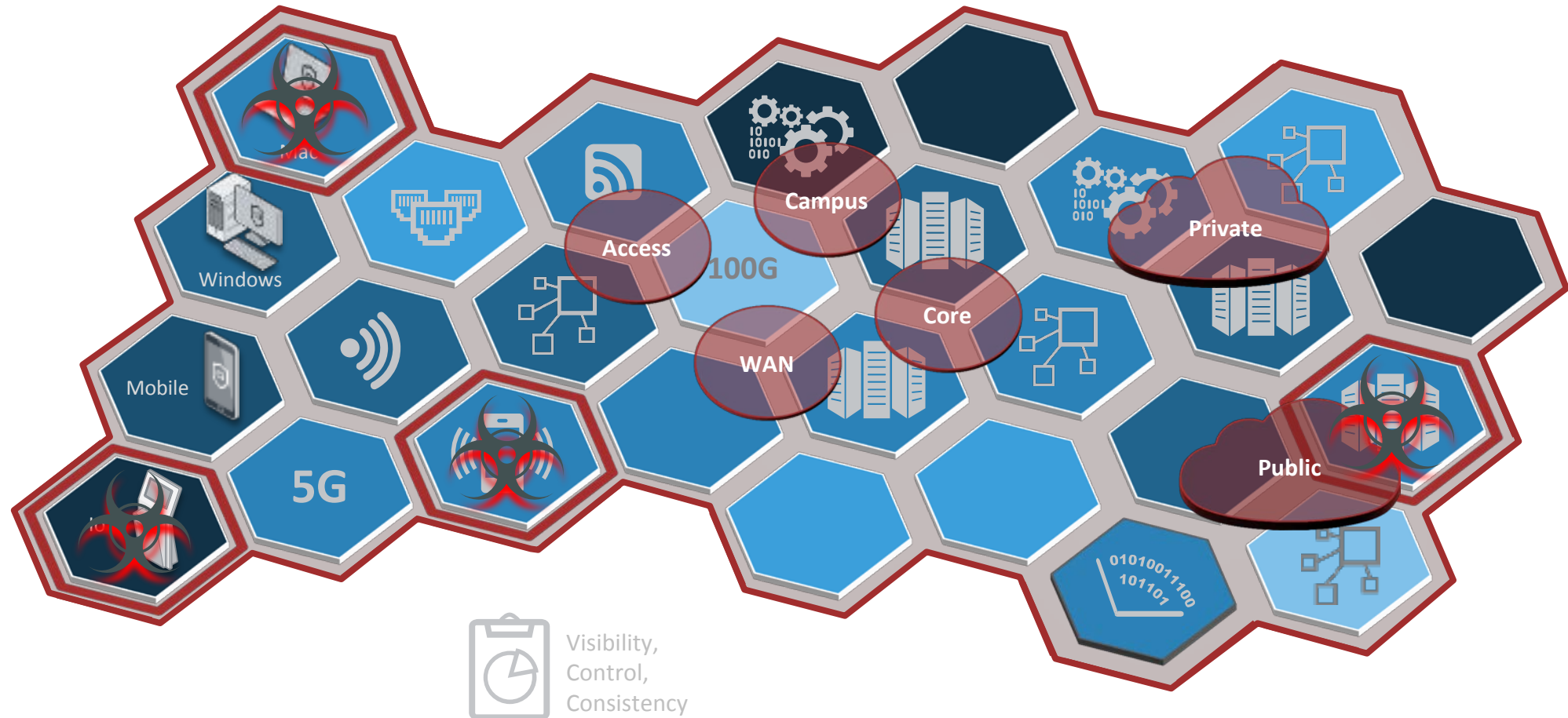


1) Se genera el Swarm (Autosploit) →

Recomendaciones

- Sistemas de sandboxing para proteger todos los vectores de ataque.
- Herramientas capaces de detectar anomalías en la red. (IA)
- Integración de todos los dispositivos de seguridad.
- Automatización
 - » En base a una amenaza detectada.
 - » Remediación automática instantánea.

Automatización



The image features a solid red background with a complex pattern of white hexagons and lines. Some hexagons are solid, while others are outlines. Lines connect some of the hexagons, creating a network-like structure. The pattern is denser in the corners and fades towards the center where the text is located.

FERTINET®