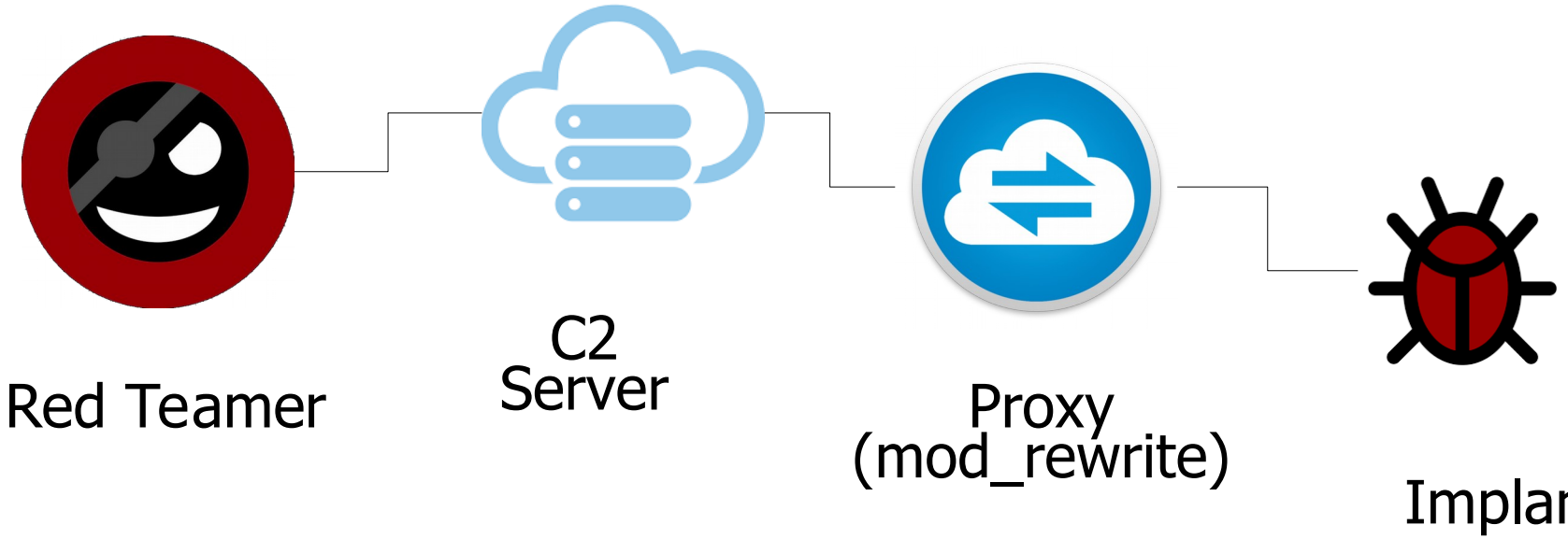
Estableciendo un C2

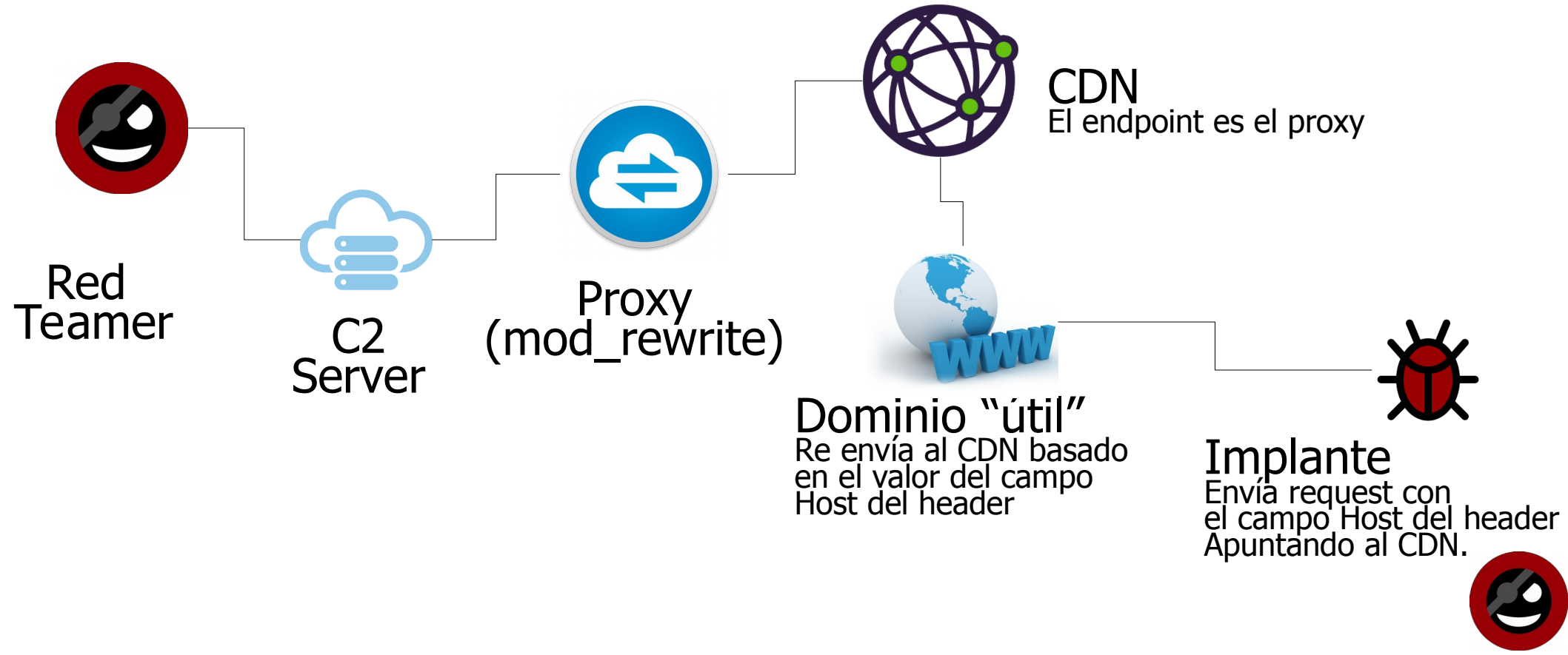
Desplazamiento Lateral ...solamente el inicio

- El desplazamiento lateral implica realizar labores sobre diferentes targets que pueden presentar condiciones diferentes
  - Diferentes targets = Diferentes Implantes
- Red **TEAM**
  - Se requiere mantener la persistencia del ataque y no morir en la gestión del mismo > Se necesita una forma controlada y uniforme de mantener la persistencia
- Los frameworks como MetaSploit y el venerable Empire tienen funcionalidades de centros de Comando y Control (C2)
  - Sin embargo, carecen de ciertas características mantener a los blue teamers confundidos, ser persistente y mantener una infraestructura "oculta"

Arquitectura de un C2

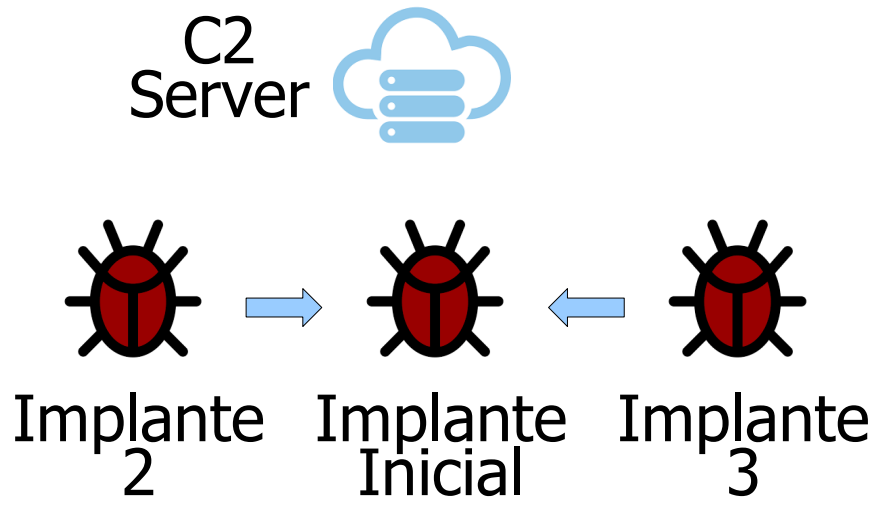


Arquitectura de un C2 : Sumando Domain Fronting



Persistencia

- Al nivel más elemental
  - Para perdurar al reinicio del computador
    - Entradas en registry
    - Tareas programadas
    - Directorio Startup
    - Cualquier forma o ubicación donde se tomen programas que se ejecutan cada que se inicia el sistema operativo
- Más especializado > Daisy Chain



Fundamentales

- Beaconing
  - E.T phone home
  - Pregunta al server por tareas, las descarga, duerme
  - Cada cierto tiempo o interactivo
- Jitter
  - Para prevenir enviar el beacon exactamente cada X minutos
  - Por ejemplo, una variación de 40% permite que el tráfico no sea tan “uniforme” y sea más difícil de detectar
- Cifrado
  - Así pase por HTTPS

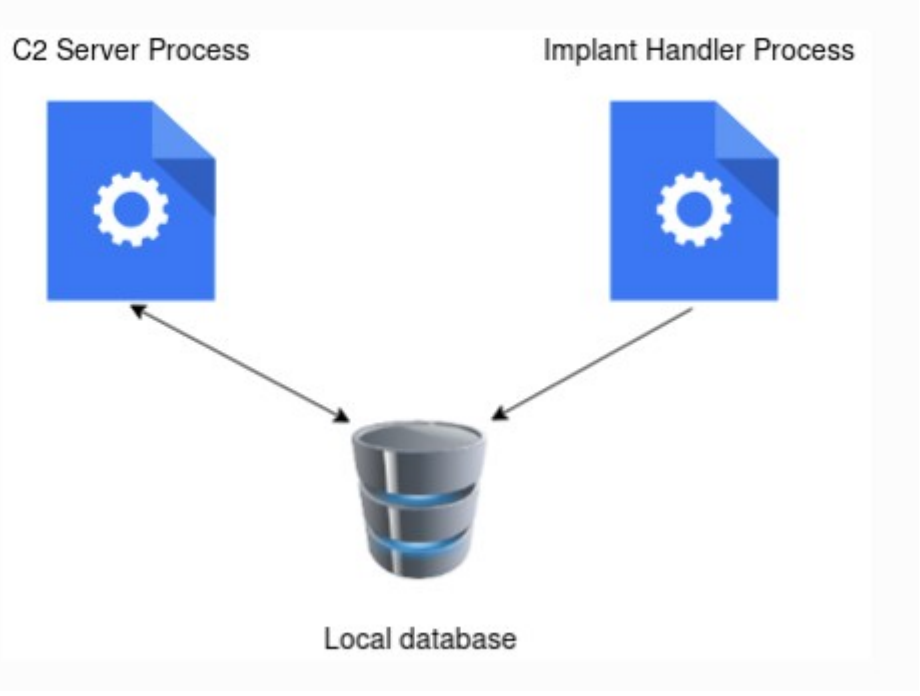
Lista Corta de C2

- Cobalt Strike
  - El más usado
- PoshC2
  - El más maduro de los Open Source
- Covenant
- Koadic
- Empire
  - Vale la pena mencionarlo aunque ahora este sin soporte
    - Una oportunidad!!!
- Tener en cuenta que mientras más usados y menos personalizables, más fáciles de detectar para los blue teamers

PoshC2

- Características que destacar
  - Módulos en C#, Powershell y Python
    - Altamente extensible
  - Payloads en PowerShell v2 y v4, C++ y C#, ejecutables y DLLs, código fuente de shellcode y Python3 para funcionalidad básica de C2 en Linux y MacOS.
  - Características para trabajo en equipo
    - En la versión actual no es tan adecuado como en la primera
  - Reportes de las actividades
  - Alto ratio de éxito en las campañas de red teaming
    - También, reconocido en los APT > Hay que personalizar más
- El Server Puede ejecutar en forma interactiva o como servicio

PoshC2 Arquitectura Interna



https://poshc2.readthedocs.io/en/latest/install_and_setup/architecture.html

PoshC2 : IoCs

- URLS comúnes
  - Cambiar en Config.sys y el oldurls.txt
- UserAgent
  - Cambiar en Config.sys
- El Domain Fronting
  - Usar dominios del rubro de salud
- Proceso usado por default para migración (netsh.exe)
  - Usar migrate con -RtlCreateUserThread y una mejor selección de proceso destino
- Change Default Persistence Methods
  - No provisto, pero, personalizable
- Template Files
  - Otra más en manos de los red teamers para personalizar