

Algunos de los principales retos a los que deben enfrentarse las fuerzas y cuerpos de seguridad son los **objetivos móviles**, cuando **no es posible acceder físicamente** al sistema informático y aquellos objetivos que **no abren ninguno de los archivos infectados** enviados por correo electrónico a sus cuentas.

En concreto, resulta **casi imposible infectar** a este tipo de objetivos, ya que mantienen sus sistemas **actualizados** y ni la **explotación de vulnerabilidades** ni otras técnicas de intrusión básicas tienen éxito con ellos.

FinFly LAN ha sido desarrollado para implementar secretamente soluciones de monitorización remota en sistemas objetivo conectados a redes LAN (con cable e inalámbricas/802.11). Puede **infectar archivos descargados** por el objetivo en tiempo real, infectar el sistema objetivo **enviando falsas actualizaciones** para aplicaciones de software populares o infectar el sistema objetivo **introduciendo la carga en sitios Web visitados**.

Ejemplo De Uso 1: Unidad Técnica De Vigilancia

Una unidad técnica de vigilancia estuvo siguiendo a un objetivo durante semanas sin poder acceder físicamente al ordenador. Los agentes utilizaron FinFly LAN para instalar la solución de monitorización remota en el ordenador del objetivo este utilizaba un **punto de conexión inalámbrica público** en una cafetería.

| DE UN VISTAZO | |
|---------------|---|
| Uso: | · Operaciones tácticas |
| Capacidades: | · Implementa una solución de monitorización remota en un sistema objetivo conectado a una red LAN |
| Contenido: | · Software |

Ejemplo De Uso 2: Anticorrupción

FinFly LAN se utilizó para instalar de forma remota una solución de monitorización remota en el ordenador de un objetivo mientras lo utilizaba **desde una habitación de hotel**. Los agentes se encontraban en otra habitación del hotel **conectados a la misma red** y manipularon el sitio Web que estaba visitando el objetivo para activar la instalación.

Descripción General De Funciones

- **Descubre todos los sistemas informáticos** conectados a una red LAN.
- Funciona tanto en **redes con cable como inalámbricas (802.11)**.
- Se puede combinar con FinIntrusion Kit y sus funcionalidades de **acceso encubierto a redes**.
- Oculta la solución de monitorización remota en las **descargas de los objetivos**.
- Disfraza la solución de monitoreo remoto en forma de **actualizaciones de software**.
- Instala remotamente soluciones de monitoreo remoto a través de los sitios web que visita el objetivo.

Encontrará la lista completa de funciones en las Especificaciones del producto



Componentes Del Producto



FinFly LAN

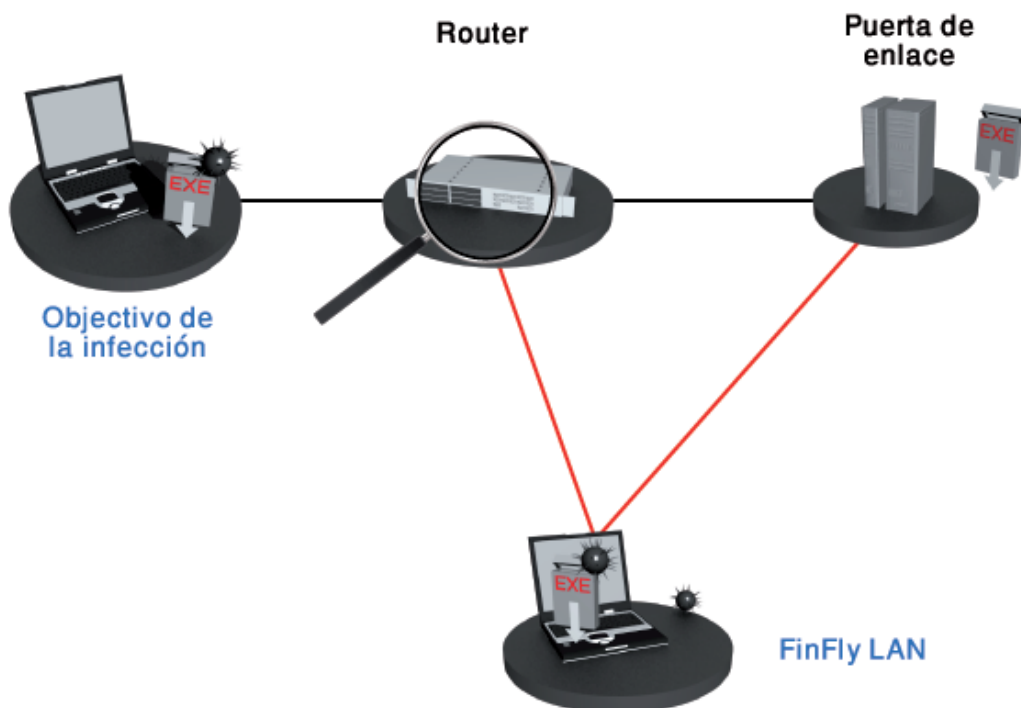
- Software basado en Linux con una interfaz de usuario fácil de utilizar.



FinIntrusion Kit - Integración (opcional)

- FinFly LAN se puede cargar como un módulo en el FinIntrusion Kit.

Infección A Través De Redes LAN



Interfaz De Usuario Automatizada

- Fácil de utilizar sin recibir mucha formación específica

| Systems Infected | | | |
|-------------------|-------------------|-----------------|---------------------|
| Target identifier | Payload | InfectionMethod | Infected at |
| testuser5 | test_trojan_1.exe | Binary | 20:30:12 27/08/2010 |
| 10.0.0.52 | test_trojan_2.exe | Update | 16:12:37 23/08/2010 |

Compatibilidad Con Múltiples Objetivos Y Cargas

- Se pueden añadir varios ejecutables para cada objetivo

Infection Techniques

☒ Binary Infection(.exe,.scr)

Operation mode: Do not Infect

www.microsoft.com

enter a website's address
(eg. www.microsoft.com)

