

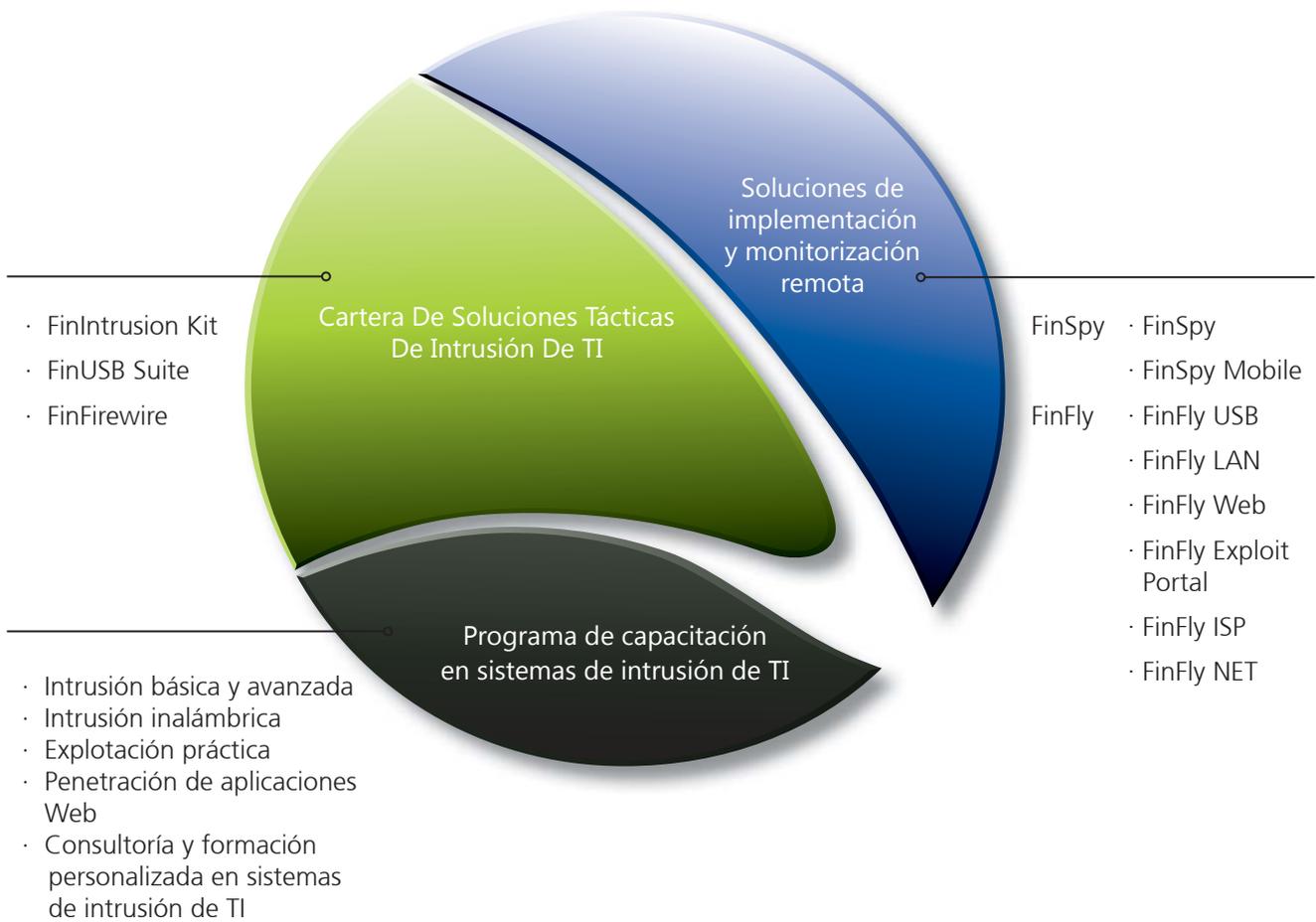


FINFISHER™ : SOLUCIONES DE MONITOREO REMOTO  
E INTRUSIÓN DE SISTEMAS DE IT  
PARA GOBIERNOS



[WWW.FINFISHER.COM](http://WWW.FINFISHER.COM)

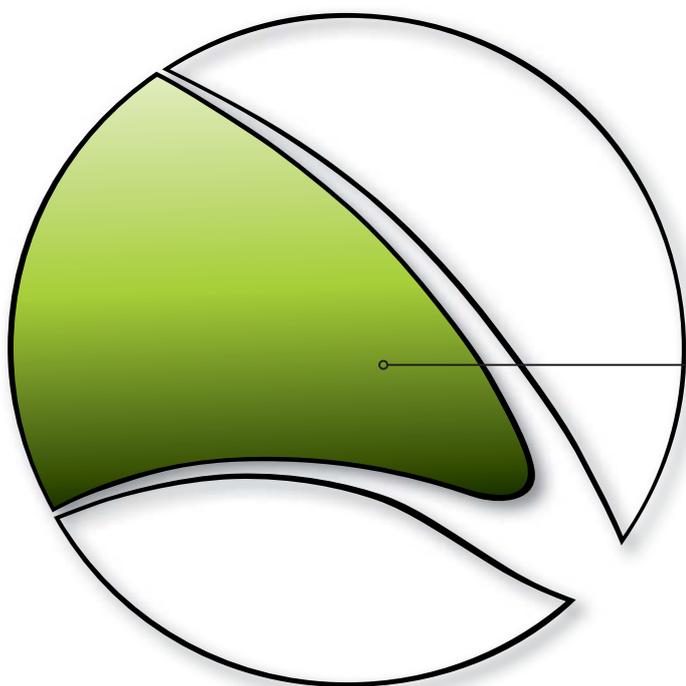
**FINFISHER™**  
IT INTRUSION



**FININTRUSION KIT**

**FINUSB SUITE**

**FINFIREWIRE**



---

Gamma hace frente a los constantes avances en el campo de las intrusiones de IT con soluciones para mejorar los recursos de nuestros clientes. Ofrece las técnicas y las soluciones más avanzadas y fáciles de utilizar, que complementan los conocimientos de los expertos en inteligencia para permitirles afrontar los retos más importantes en lo referente a la intrusión en un nivel táctico.



**FinIntrusion Kit** ha sido diseñado y desarrollado por especialistas en sistemas de intrusión de TI de primer nivel mundial, con más de 10 años de experiencia en su campo gracias a su participación en varios Tiger Teams (Red Teams), tanto del sector privado como de agencias gubernamentales, valorando la seguridad de distintas redes y organizaciones.

FinIntrusion Kit es un kit operativo **actualizado y encubierto** a la vez, que puede utilizarse en la mayoría de **operaciones de intrusión de TI**, tanto en áreas defensivas como ofensivas. Entre nuestros clientes podemos contar con **departamentos militares especializados en guerra cibernética, agencias de inteligencia, departamentos de inteligencia policial y otras fuerzas y cuerpos de seguridad.**

### Ejemplo De Uso 1: Unidad Técnica De Vigilancia

FinIntrusion Kit se utilizó para descodificar **el cifrado WPA** de la red inalámbrica del hogar de un objetivo y para monitorizar sus **credenciales de acceso al correo web (Gmail, Yahoo, ...)** y a **redes sociales (Facebook, MySpace, ...)**, lo que permitió a los investigadores **monitorizar de forma remota** estas cuentas desde la sede central sin necesidad de acercarse al objetivo.

### Descripción General De Funciones

- Descubre **redes LAN (802.11) y dispositivos Bluetooth®**
- Recupera contraseñas WEP (64 y 128 bits) **en entre 2 y 5 minutos**
- **Descifra contraseñas WPA1 y WPA2** utilizando ataques con diccionarios
- Monitorea de manera activa redes LAN (por cable e inalámbricas) y **extrae nombres de usuario y contraseñas incluso para sesiones con cifrado TLS/SSL**
- **Entra de forma Remota en cuentas de correo electrónico** utilizando técnicas de intrusión basadas en la red, el sistema y la contraseña
- **Evaluación y validación de la seguridad de la red**

Encontrará la lista completa de funciones en las Especificaciones del producto

### DE UN VISTAZO

Uso:	· Operaciones estratégicas · Operaciones tácticas
Capacidades:	· Descodifica cifrados WEP/WPA · Monitorizar redes (incluyendo sesiones SSL) · Ataques de intrusión de TI
Contenido:	· Hardware/Software

### Ejemplo De Uso 2: Seguridad De TI

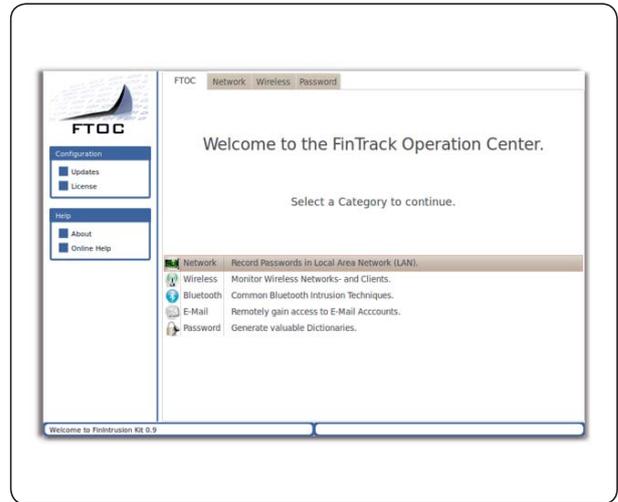
Varios clientes han utilizado FinIntrusion Kit para **saltarse con éxito la seguridad** de redes y sistemas informáticos con finalidades **ofensivas y defensivas** utilizando diversas técnicas y herramientas.

### Ejemplo De Uso 3: Casos De Uso Estratégico

FinIntrusion Kit se suele utilizar para acceder de forma remota a cuentas de correo electrónico y servidores de objetivos y monitorear sus actividades controlando, entre otros, elementos como los registros de acceso.



### Componentes Del Producto



### FinIntrusion Kit – Unidad Táctica Encubierta

Componentes básicos para la intrusión de TI :

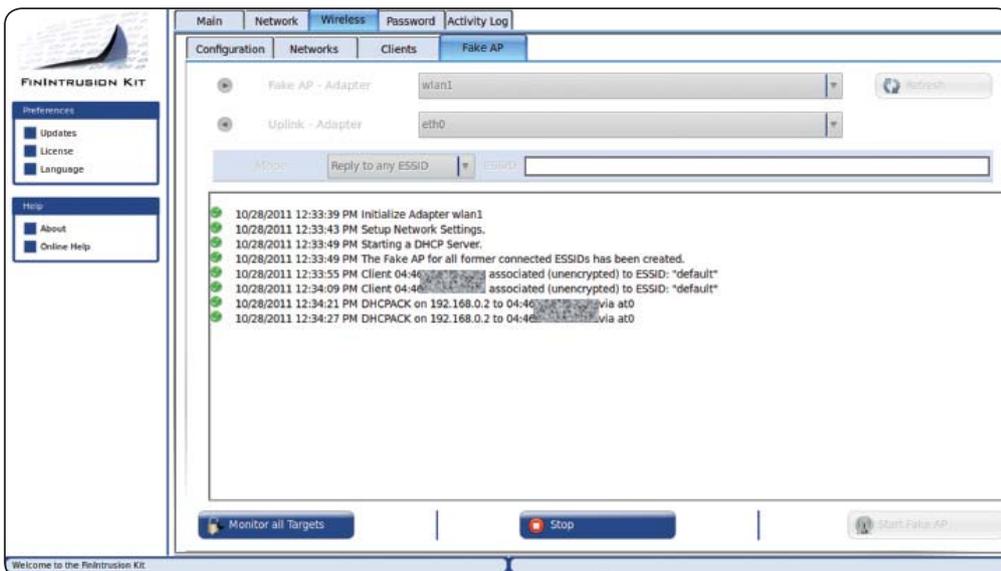
- Adaptador WLAN de gran potencia
- Adaptador Bluetooth de gran potencia
- Antenas 802.11
- Muchos dispositivos habituales de intrusión de TI

### FinTrack Operation Center

- Interfaz gráfica de usuario para automatizar ataques de intrusión de TI

### Localizador de Wi-Fi

- Localiza dispositivos WLAN cercanos y registra el tráfico y las contraseñas



**Rastreador activo de contraseñas de redes LAN y WLAN**

- Captura incluso datos con cifrado SSL de servicios como correo Web, portales de vídeo, banca en línea y muchos más

The screenshot shows the 'Passwords' tab in the FININTRUSION KIT software. The interface includes a sidebar with 'Preferences' (Updates, License, Language) and 'Help' (About, Online Help) sections. The main area displays a table of active targets with columns for Target IP, Protocol, Username, Password, IP Address, and Hostname / URL. An 'Export List' button is located at the bottom right of the table. A status bar at the bottom indicates 'Monitoring against Target 10.0.0.225 is running in the background.'

Target IP	Protocol	Username	Password	IP Address	Hostname / URL
passivesniff	ftp	ftp	bad-choice	130.89.149.226	kassia3.snt.utwente.nl
passivesniff	http	michael@yahoo.com	smith	188.125.72.80	http://mlogin.yahoo.com
passivesniff	irc	unknown	ircmobile	193.219.128.49	/PASS
all	snmp	public		192.168.0.253	SNMP
all	http	john@cnn.com	342DukE*!^31	157.166.255.80	audience.cnn.com
all	https	james@facebook.com	Parker433	69.171.228.40	www.facebook.com
10.0.0.225	ftp	anonymous	chrome@example.com	195.135.221.132	ftp.suse.de
10.0.0.225	snmp	public		192.168.0.253	SNMP
10.0.0.225	irc	unknown		140.211.167.99	irc.freenode.com
10.0.0.225	https	jacob@yahoo.com	\$\$%_BeckeR122	217.146.187.123	mail.yahoo.com

**FinUSB Suite** es un producto flexible que permite a fuerzas y cuerpos de seguridad y a agencias de inteligencia extraer información forense de sistemas informáticos de manera rápida y segura, **sin la necesidad de contar con agentes con formación específica en TI.**

Se ha utilizado con gran éxito realizadas en todo el mundo, en las que se ha recabado información importante sobre los objetivos de operaciones encubiertas y abiertas.

### Ejemplo De Uso 1: Operación Encubierta

Se entregó una llave FinUSB a una fuente infiltrada en un grupo criminal organizado (GCO) y esta persona extrajo, de manera secreta, credenciales de cuentas de correo electrónico y correo Web y documentos de Microsoft Office de los sistemas objetivo mientras el grupo criminal utilizaba el dispositivo USB **para intercambiar archivos convencionales**, como música, vídeos y documentos de Office.

Tras devolver la llave USB a la sede central de la agencia, los datos obtenidos pudieron ser descifrados, analizados y utilizados para monitorizar constantemente las operaciones del grupo de manera remota.

### Descripción General De Funciones

- Optimizado para **operaciones encubiertas**
- Máxima facilidad de uso gracias a la **ejecución automatizada**
- **Cifrado seguro** mediante RSA y AES
- Extracción de **nombres de usuario y contraseñas** para todas las aplicaciones de software más comunes, como:
  - Clientes de correo electrónico
  - Soluciones de mensajería
  - Navegadores
  - Herramientas de administración remota
- **Copia silenciosa de archivos** (busca en los discos, en la Papelera de reciclaje y en los últimos archivos abiertos, editados o creados)
- Extracción de **información de la red** (registros de chats, historial de navegación, claves WEP/WPA(2), etc.)
- Compilación de **información del sistema** (software en ejecución e instalado, información de los discos duros, etc.)

Encontrará la lista completa de funciones en las Especificaciones del producto.

DE UN VISTAZO	
Uso:	· Operaciones tácticas
Capacidades:	· Obtención de información · Acceso a sistemas · Análisis forenses rápidos
Contenido:	· Hardware/Software

### Ejemplo De Uso 2: Unidad Técnica De Vigilancia

Una unidad técnica de vigilancia (UTV) estaba siguiendo a un objetivo que visitaba a menudo cibercafés aleatorios, lo que hacía imposible monitorear sus actividades con tecnologías tipo caballo de Troya. La UTV decidió utilizar FinUSB para extraer los **datos dejados en los terminales públicos** utilizados por el objetivo una vez éste se había ido.

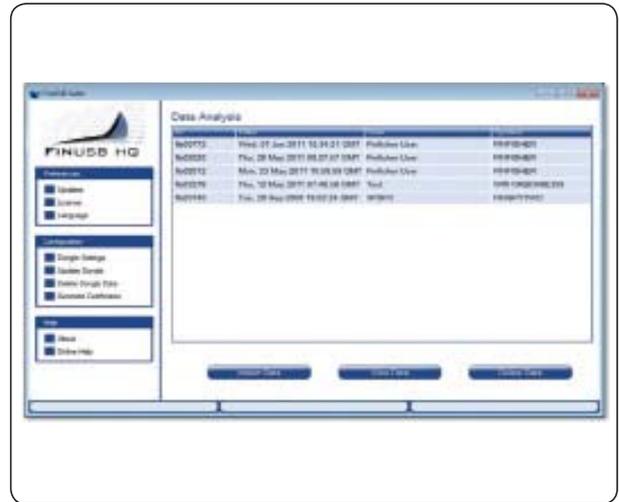
De este modo, se pudieron recuperar varios documentos abiertos por el objetivo en su correo web. La información recabada incluía archivos de Office de vital importancia, el historial de navegación a través del análisis de las cookies y mucho más.



**Componentes Del Producto**



**FinUSB Suite – Unidad Móvil**



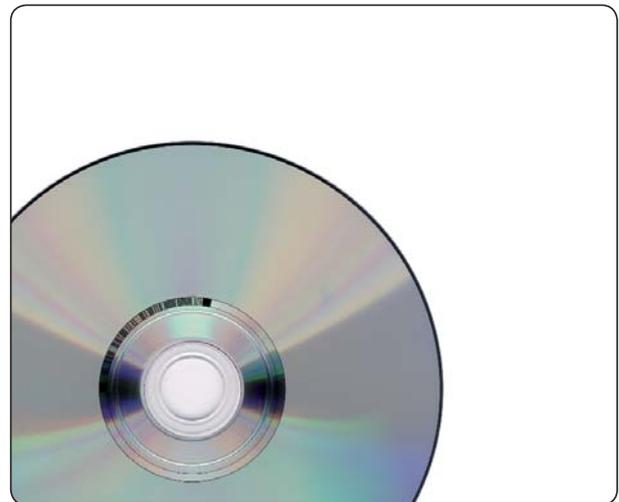
**FinUSB HQ**

- Interfaz gráfica de usuario para descifrar y analizar los datos recogidos
- Configura las opciones operativas de la llave



**10 Llaves FinUSB (U3, 16 Gb)**

- Extrae secretamente datos del sistema



**FinUSB – Omisión De La Contraseña De Windows**

- Permite saltarse el inicio de sesión de Windows sin efectuar modificaciones permanentes en el sistema



### Máxima Facilidad De Uso



1. Elegir una llave FinUSB
2. Configurar los módulos y funciones deseados, y actualizar la llave FinUSB con FinUSB HQ
3. Dirigirse al sistema objetivo
4. Conectar la llave FinUSB
5. Esperar a que se hayan transferido todos los datos
6. Volver al software FinUSB HQ
7. Importar todos los datos de la llave FinUSB
8. Generar el informe

### Informes Profesionales



Las unidades técnicas de vigilancia y los expertos forenses a menudo se encuentran con situaciones en las que tienen que acceder a un sistema informático en ejecución sin apagarlo, para así evitar la pérdida de datos o para ahorrar un tiempo vital para el éxito de la operación. En la mayoría de casos, el sistema objetivo estará protegido mediante un **salvapantallas con contraseña** o el usuario objetivo no habrá iniciado sesión y aparecerá la **pantalla de inicio de sesión**.

FinFireWire permite que el operador **se salte la pantalla protegida por contraseña** de manera rápida y encubierta, y acceda al sistema objetivo sin dejar rastros ni dañar pruebas forenses que pueden ser esenciales.

### Ejemplo De Uso 1: Operación Forense

Una **unidad forense** entró en el piso de un objetivo e intentó acceder al sistema informático. El ordenador estaba **encendido, pero la pantalla estaba bloqueada**. Dado que la unidad no estaba legalmente autorizada a utilizar una solución de Monitoreo remoto, se habrían **perdido todos los datos** apagando el sistema, ya que **el disco duro estaba íntegramente cifrado**. Se utilizó FinFireWire para **desbloquear el sistema objetivo**, lo que permitió que un agente **copiara todos los archivos** antes de apagar el ordenador y llevar toda esta información a los cuarteles centrales de la agencia.

### Descripción General De Funciones

- **Desbloquea el inicio de sesión** para todas las cuentas de usuario
- Desbloquea los **salvapantallas protegidos con contraseña**
- **Realiza un volcado de toda la RAM** para llevar a cabo un análisis forense
- Permite efectuar análisis forenses **en tiempo real** y **sin tener que reiniciar** el sistema objetivo
- La contraseña del usuario **no se modifica**
- Compatible con **sistemas Windows, Mac y Linux**
- Funciona con **FireWire/1394, PCMCIA y Express Card**

Encontrará la lista completa de funciones en las Especificaciones del producto.

DE UN VISTAZO	
Uso:	Operaciones tácticas
Capacidades:	<ul style="list-style-type: none"> <li>· Omite la contraseña de usuario</li> <li>· Accede al sistema de forma encubierta</li> <li>· Recupera contraseñas de RAM</li> <li>· Permite la realización de análisis forenses en tiempo real</li> </ul>
Contenido:	Hardware/Software

### Ejemplo de uso 2: Recuperación de contraseñas

Combinando el producto con **aplicaciones forenses tradicionales** como Encase®, las unidades forenses utilizaron la **función de volcado RAM** para tomar una instantánea de la información de la RAM actual y **recuperaron la contraseña de cifrado del disco duro** para llevar a cabo un cifrado de todo el disco de TrueCrypt.

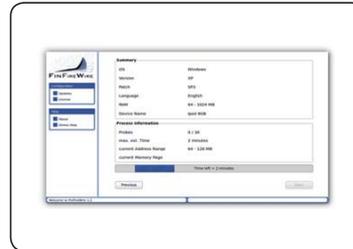


### Componentes Del Producto



**FinFireWire - Unidad táctica**

- Sistema táctico completo



**Interfaz de usuario interactiva**

- Interfaz de usuario fácil de utilizar



**Tarjetas adaptadoras de conexión**

- Adaptador PCMCIA y ExpressCard para sistemas objetivo sin puerto FireWire



**Conjunto Universal De Cables Finwire**

- De 4 pines a 4 pines
- De 4 pines a 6 pines
- De 6 pines a 6 pines

### Uso



**1. Dirigirse al sistema objetivo**



**2. Iniciar FinFireWire**



**3. Conectar el cable y el adaptador FireWire**



**4. Seleccionar un objetivo**



**5. Esperar a que el sistema se desbloquee**

**FINSPY**

**FINSPY MOBILE**

**FINFLY USB**

**FINFLY LAN**

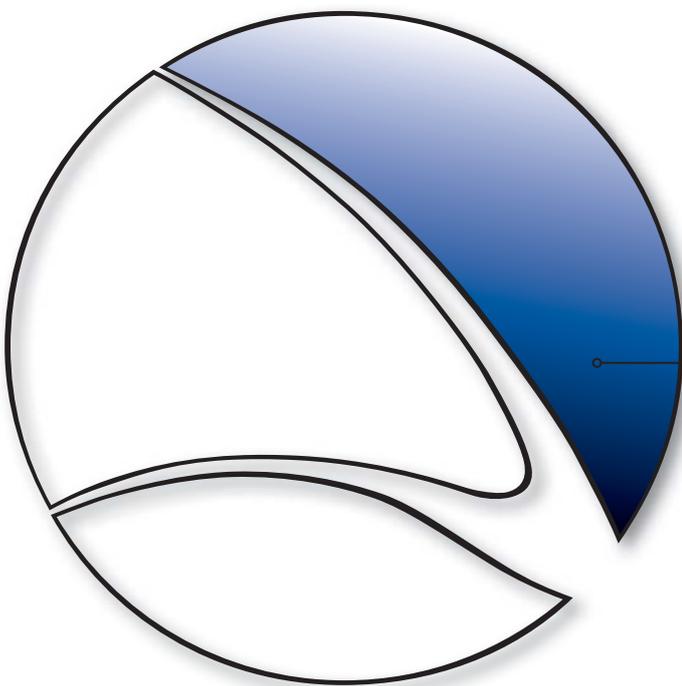
**FINFLY WEB**

**FINFLY EXPLOIT**

**PORTAL**

**FINFLY ISP**

**FINFLY NET**



---

Las soluciones de infección y monitorización remota permiten acceder a los sistemas de los sospechosos y conseguir un acceso total a la información que contienen, con la posibilidad de controlar las funciones de los sistemas objetivo hasta el punto de capturar comunicaciones y datos cifrados. En combinación con métodos de infección remota mejorados, las agencias gubernamentales que las utilicen podrán infectar de forma remota sistemas objetivo.



**FinSpy** es una solución de monitorización remota de eficacia probada que permite a los gobiernos hacer frente al reto actual de **monitorizar objetivos móviles y que adoptan medidas de seguridad**, que **cambian su ubicación** constantemente, que utilizan canales de **comunicación anónimos y cifrados**, y que **residen en el extranjero**.

Las soluciones de interceptación legal tradicionales **deben afrontar nuevos retos** que solo se pueden **solucionar utilizando sistemas activos** como FinSpy:

- Datos que no se transmiten por ninguna red
- Comunicaciones cifradas
- Objetivos residentes en países extranjeros

FinSpy **ha demostrado su éxito** en operaciones realizadas en todo el mundo **a lo largo de muchos años**, que han permitido obtener valiosa inteligencia sobre organizaciones y personas objetivo.

Cuando FinSpy se instala en un sistema informático, se puede **controlar y acceder al dispositivo de forma remota** en el mismo momento en que se conecta a Internet o a una red, **independientemente del lugar del mundo** en el que se encuentre.

### Descripción General De Funciones

Ejemplos de funciones en el ordenador objetivo:

- Indetectabilidad por 40 sistemas antivirus probada regularmente
- **Comunicación encubierta** con la sede central de la organización
- **Monitorización total de Skype** (llamadas, chats, transferencias de archivos, vídeo y lista de contactos)
- Grabación de las **comunicaciones comunes** por correo electrónico, chats y VoIP
- **Vigilancia en tiempo real** a través de Webcam y micrófono
- **Rastreo del país** en el que se encuentra el objetivo
- **Extracción silenciosa de archivos** del disco duro
- **Capturado de pulsaciones basado en procesos** para un análisis más rápido
- **Análisis forenses remotos en tiempo real** en el sistema objetivo
- **Filtros avanzados** para registrar solo la información importante
- Compatible con los sistemas operativos más comunes: **Windows, Mac OSX y Linux**

### DE UN VISTAZO

<b>Uso:</b>	· Operaciones estratégicas/tácticas
<b>Capacidades:</b>	· Monitorizar equipos remotos · Monitorizar comunicaciones cifradas
<b>Contenido:</b>	· Hardware/Software

### Ejemplo De Uso 1: Agencia De Inteligencia

FinSpy se instaló en varios sistemas informáticos de **cibercafés en áreas críticas** para monitorearlos y detectar actividades sospechosas, especialmente **comunicaciones vía Skype con extranjeros**. A través de la webcam, se tomaron fotografías de los objetivos mientras utilizaban el sistema.

### Ejemplo De Uso 2: Crimen organizado

FinSpy se **implementó secretamente en los sistemas objetivo** de varios miembros de un grupo criminal organizado. Gracias al **rastreo del país y al acceso remoto al micrófono**, se recopiló información fundamental sobre **todas las reuniones** de este grupo.

Ejemplos de funciones en la sede central:

- Protección de **pruebas** (pruebas válidas de acuerdo con la **normativa Europea**)
- **Administración de usuarios** según las autorizaciones de seguridad
- Oculto del público mediante **proxies anonimantes**
- Se puede **integrar plenamente** con la función de monitorización de las fuerzas y cuerpos de seguridad

Encontrará la lista completa de funciones en las Especificaciones del producto.



### Componentes Del Producto



#### FinSpy Master y Proxy

- Control total de los sistemas objetivo
- Protección de pruebas para registros de actividad y datos
- Almacenamiento seguro
- Administración de usuarios y objetivos en función de las autorizaciones de seguridad

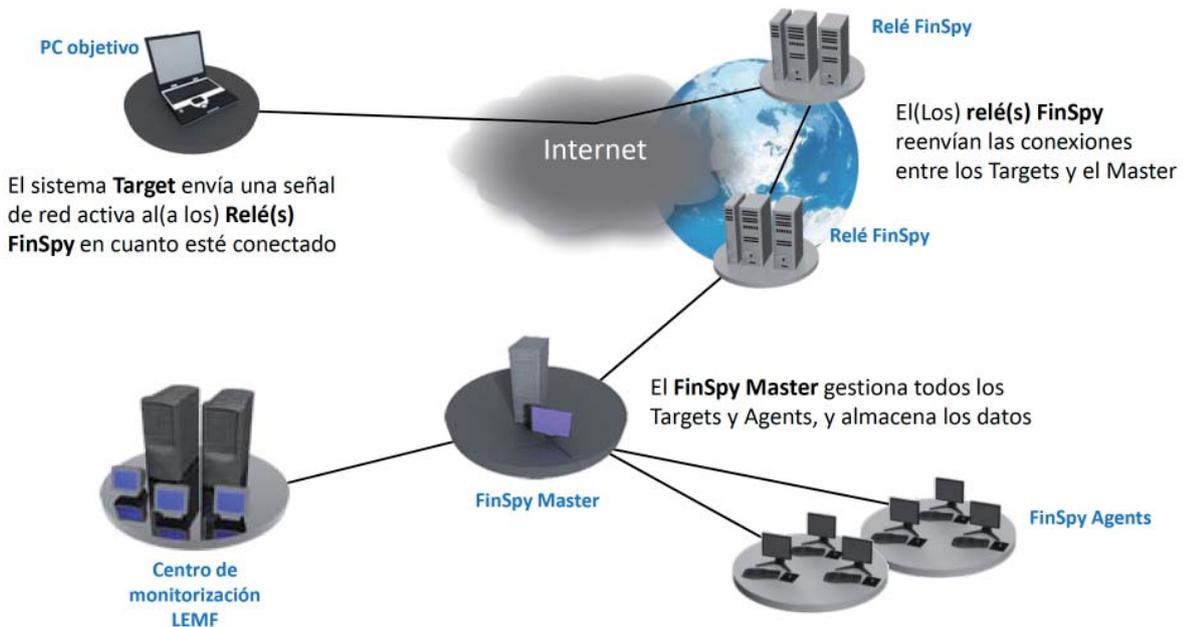


#### FinSpy Agent

- Interfaz gráfica de usuario para programar y abrir sesiones
- configurar y analizar datos de los objetivos en tiempo real



### Acceso A Sistemas Informáticos De Cualquier Lugar Del Mundo



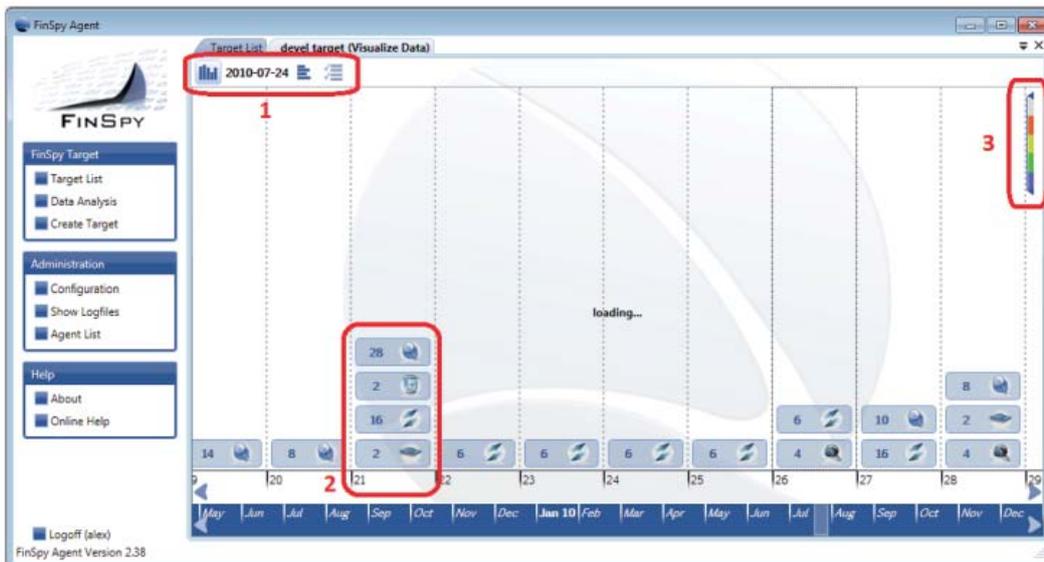
### Interfaz De Usuario Fácil De Utilizar



### Configuración del objetivo con y sin conexión



### Inteligencia completa en sistema objetivo



1. Múltiples vistas de datos
2. Análisis de datos estructurado
3. Niveles de importancia para todos los archivos registrados

**FinSpy Mobile** cierra la brecha de las capacidades de interceptación de los gobiernos para las **plataformas de Smartphone** más comunes.

Concretamente, las organizaciones sin capacidades de **red o interceptación fuera del canal de conversación** pueden acceder a teléfonos móviles e interceptar los dispositivos con capacidades mejoradas. Además, la solución ofrece **acceso a comunicaciones cifradas y almacenamiento en los dispositivos de los datos** que no se transmiten.

Las soluciones de interceptación táctica o estratégica tradicionales **deben afrontar nuevos retos** que solo se pueden **solucionar utilizando sistemas ofensivos** como FinSpy Mobile:

- Los datos no se transmiten a través de ninguna red y se mantienen en el dispositivo.
- Comunicaciones cifradas en la interfaz del canal de conversación, lo que evita el uso de sistemas tácticos activos o pasivos fuera del canal de conversación.
- Cifrado de extremo a extremo desde el dispositivo, como mensajes de PIN, de soluciones de mensajería o de correo electrónico.

**FinSpy Mobile** ha dado muy buenos resultados a las agencias gubernamentales que recopilan información **de forma remota de teléfonos móviles objetivo**.

Cuando FinSpy Mobile se instala en un teléfono móvil, se puede **controlar y monitorizar de forma remota** independientemente del lugar del mundo en el que se encuentre el objetivo.

### Descripción General De Funciones

Ejemplos de funciones en el ordenador objetivo:

- **Comunicaciones encubiertas con la sede central de la organización**
- Grabación de las **comunicaciones comunes** por video llamada, SMS/MMS y correo electrónico
- **Vigilancia en tiempo real** mediante llamadas silenciosas
- **Descarga de archivos** (contactos, calendario, imágenes, archivos)
- **Rastreo del país** en el que se encuentra el objetivo (GPS y ID celular)
- Grabación completa de todas las **comunicaciones a través de BlackBerry Messenger**
- Compatible con los sistemas operativos más comunes: **Windows Mobile, iOS (iPhone), BlackBerry OS, Android y Symbian**

### DE UN VISTAZO

Uso:	· Operaciones estratégicas · Operaciones tácticas
Capacidades:	· Monitorización remota de teléfonos móviles
Contenido:	· Hardware/Software

### Ejemplo de uso 1: Agencia de inteligencia

FinSpy Mobile se implementó en los **teléfonos móviles BlackBerry** de varios objetivos para monitorizar todas sus comunicaciones, incluyendo **SMS/MMS, correo electrónico y BlackBerry Messenger**.

### Ejemplo de uso 2: Crimen organizado

FinSpy se **implementó secretamente en los teléfonos móviles** de varios miembros de un grupo criminal organizado. Gracias a los datos de **rastreo GPS** y a las **llamadas silenciosas**, se recopiló información fundamental sobre **todas las reuniones** de este grupo.

Ejemplos de funciones en la sede central:

- Protección de pruebas (pruebas válidas de acuerdo con la **normativa Europea**)
- **Administración de usuarios** según las autorizaciones de seguridad
- Oculto del público mediante **proxies anonimantes**
- Se puede **integrar plenamente** con la función de monitorización de las fuerzas y cuerpos de seguridad

Encontrará la lista completa de funciones en las Especificaciones del producto.



### Componentes Del Producto



#### FinSpy Master y Proxy

- Control total de los teléfonos objetivo
- Protección de pruebas para registros de actividad y datos
- Almacenamiento seguro
- Administración de usuarios y objetivos en función de las autorizaciones de seguridad

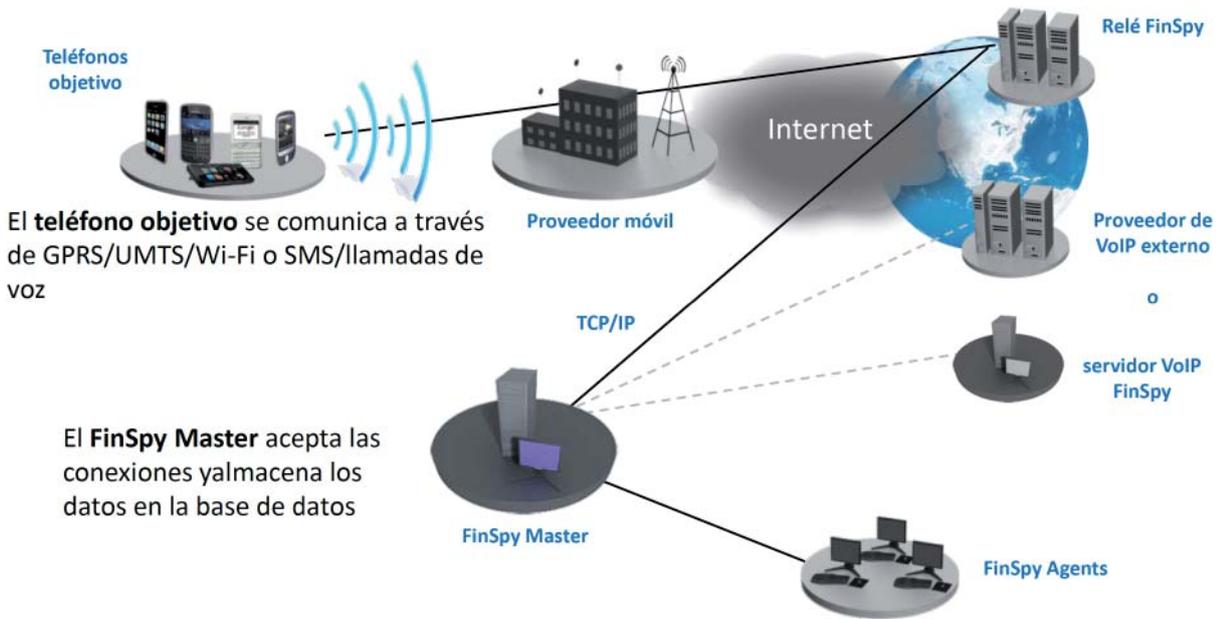


#### FinSpy Agent

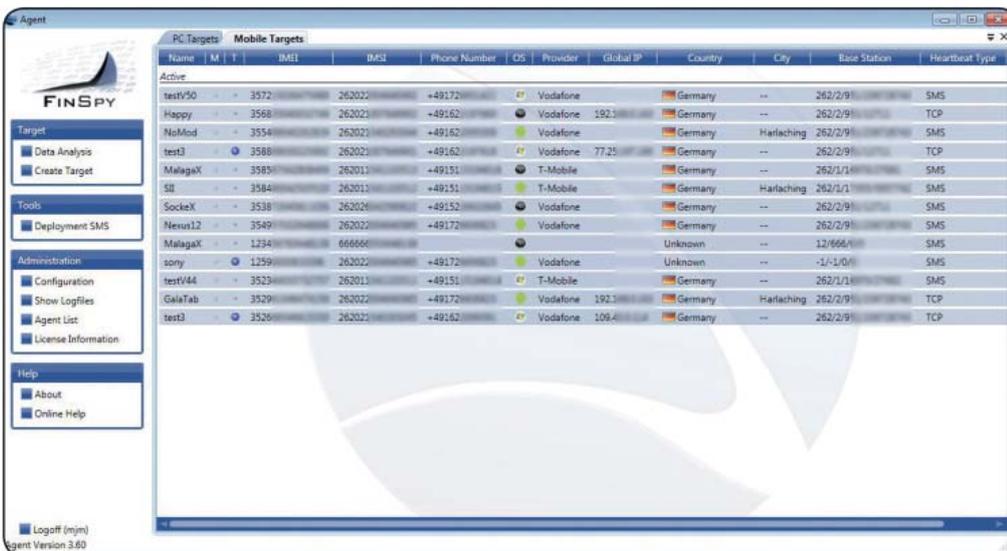
- Interfaz gráfica de usuario para programar y abrir sesiones, configurar y analizar datos de los objetivos en tiempo real



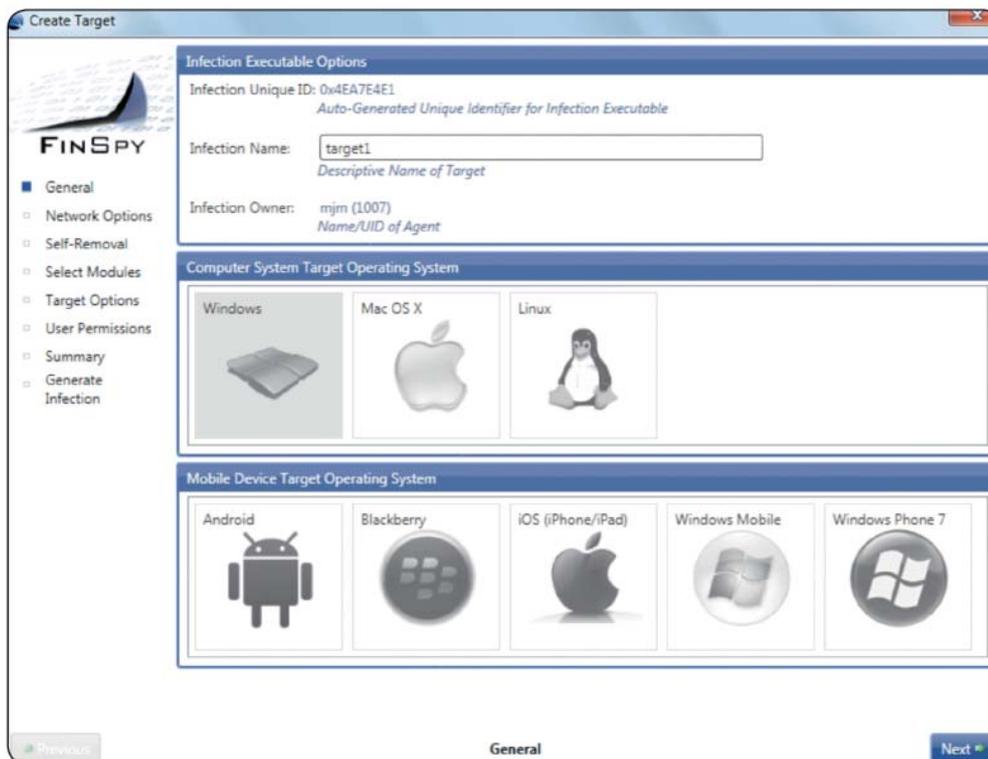
### Acceso A Los Teléfonos Móviles De Objetivos De Todo El Mundo



### Interfaz De Usuario Fácil De Utilizar



### Compatible Con Todas Las Plataformas Móviles Habituales



**FinFly USB** es una forma sencilla y fiable de instalar soluciones de monitorización remota en sistemas informáticos a los que se puede acceder físicamente.

Al insertar FinFly USB en un ordenador, **instala automáticamente el software configurado** con muy poca o nada de interacción por parte del usuario, lo que implica que **no será necesario que la operación se confíe a agentes con formación específica en TI**. FinFly USB se puede utilizar en **múltiples sistemas** antes de devolverlo a la sede central de la agencia.

### Ejemplo De Uso 1: Unidad técnica de vigilancia

FinFly USB ha sido utilizado con éxito por **unidades técnicas de vigilancia** en varios países para implementar una solución de monitorización remota en los sistemas objetivo que se **apagaban** con solo **iniciar el sistema desde el dispositivo FinFly USB**. Esta técnica funcionó incluso para sistemas objetivo con un **cifrado completo del disco duro** y productos como TrueCrypt habilitados.

### Descripción General De Funciones

- Se puede implementar incluso en **sistemas apagados con un cifrado completo del disco duro** (p. ej., TrueCrypt)
- **Instala secretamente una solución de monitorización remota** al insertarse en el sistema objetivo
- **Requiere muy poca o nada de interacción** por parte del usuario
- Su funcionalidad puede **ocultarse copiando archivos convencionales** como música, vídeos y documentos de Office en el dispositivo
- El hardware es un **dispositivo USB totalmente común y aparentemente inocuo, que no levanta sospechas**

Encontrará la lista completa de funciones en las Especificaciones del producto.

DE UN VISTAZO	
Uso:	Operaciones tácticas
Capacidades:	Implementa una solución de monitorización remota en el objetivo
Contenido:	Hardware

### Ejemplo De Uso 2: Agencia de Inteligencia

Una fuente infiltrada en un grupo terrorista recibió un FinFly USB que **instaló secretamente una solución de monitorización remota** en varios ordenadores del grupo mientras los terroristas utilizaban el dispositivo para intercambiarse documentos. Los sistemas objetivo **se monitorizaron de forma remota desde la sede central de la agencia gubernamental** y la fuente devolvió el FinFly USB al terminar la operación.



### Componentes Del Producto



#### FinFly USB

- Llave USB
- Implementa una solución de monitorización remota al insertarse en los sistemas objetivo
- Implementa una solución de monitorización remota durante el proceso de inicio



#### Total integración con FinSpy

- Generación y activación automática a través de FinSpy Agent

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, **enviando falsas actualizaciones** para aplicaciones de software populares o introducir **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 mientras este utilizaba un **punto de conexión inalámbrica público** (Hotspot) en una cafetería.

### 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 de forma remota soluciones de monitorización remota a través de los **sitios Web que visita el objetivo**

Encontrará la lista completa de funciones en las Especificaciones del producto

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.



### Componentes Del Producto



#### FinFly LAN

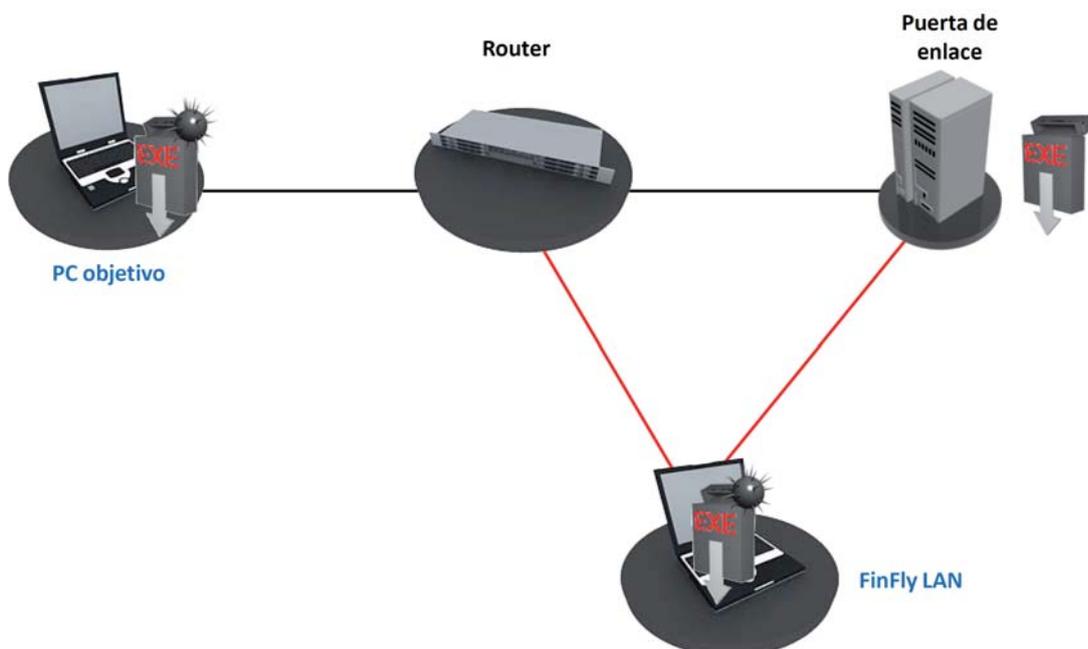
- Software basado en Linux con una interfaz de usuario fácil de utilizar.



#### FinIntrusion Kit - Integración (opcional)

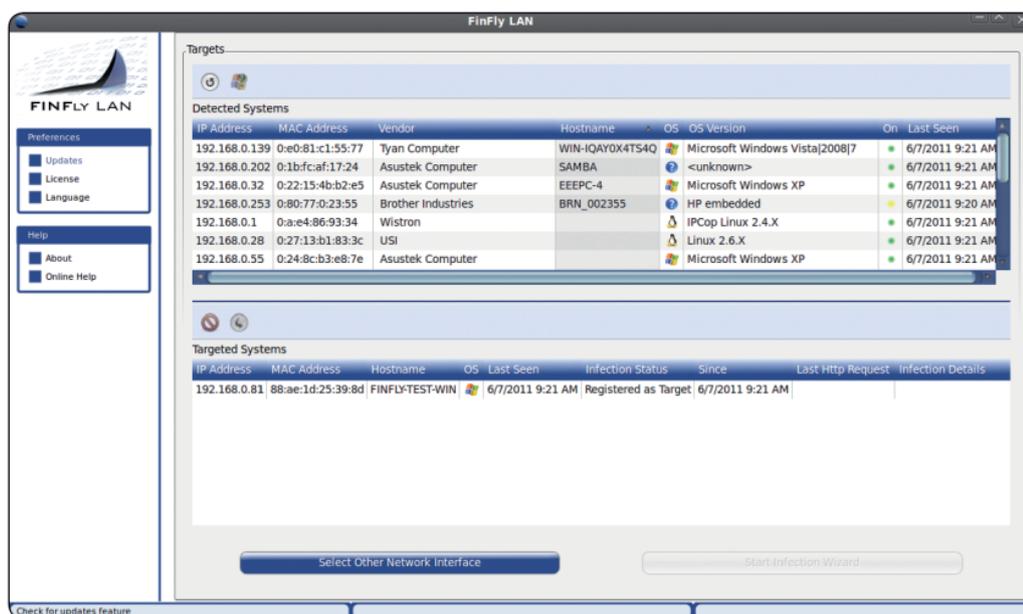
- FinFly LAN se puede cargar como un módulo en el FinIntrusion Kit.

### Implementación a Través de Redes Lan



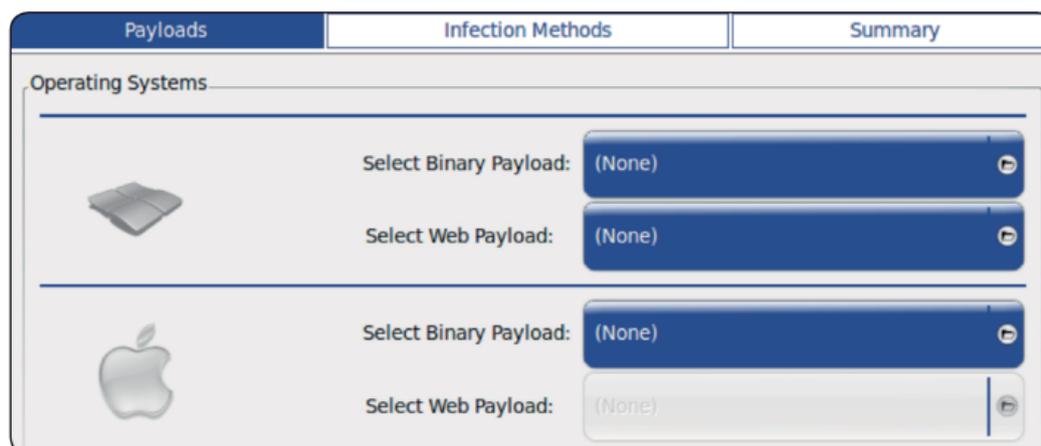
### Interfaz de Usuario Automatizada

- Fácil de utilizar sin recibir mucha formación específica



### Compatibilidad Con Múltiples Objetivos Y Cargas

- Se pueden añadir varios ejecutables para cada objetivo



Uno de los principales retos ligados al uso de una solución de monitorización remota es instalarla en el sistema objetivo, sobre todo cuando se dispone de muy poca información, como una simple **dirección de correo electrónico**, y cuando resulta imposible **acceder físicamente al sistema**.

FinFly Web está diseñado para ofrecer la implementación **remota y encubierta** de un sistema objetivo utilizando gran variedad de **ataques basados en la Web**.

FinFly Web proporciona una **interfaz interactiva** que permite que el agente **pueda crear fácilmente un código de implementación personalizado** en función de los módulos seleccionados.

La carga se implementará cuando el sistema objetivo visite el sitio Web preparado con el código personalizado.

### Ejemplo De Uso 1: Unidad Técnica De Vigilancia

Tras estudiar el perfil del objetivo, la unidad creó un **sitio Web de interés** para esta persona y le envió el **enlace por medio de un panel de discusión**. Al abrir el enlace, se instaló una solución de monitorización remota en el sistema objetivo, que pudo **monitorearse desde la sede central de la agencia**.

### Descripción General De Funciones

- Módulos Web **totalmente personalizables**
- Se pueden **instalar secretamente en cualquier sitio Web**
- Total integración con **FinFly LAN, FinFly NET y FinFly ISP** para implementarse incluso en los sitios Web más populares, como proveedores de correo Web, portales de vídeo, etc.
- Instala soluciones de monitorización remota **incluso si sólo se conoce la dirección de correo electrónico del objetivo**
- Posibilidad de dirigir las actividades de monitorización a todos los visitantes de **determinados sitios Web**

Encontrará la lista completa de funciones en las Especificaciones del producto.

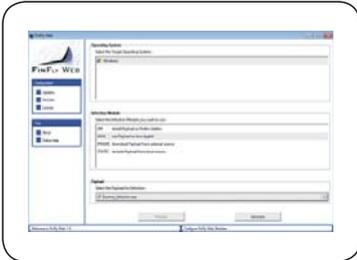
DE UN VISTAZO	
Uso:	· Operaciones estratégicas
Capacidades:	· Implementa una solución de monitorización remota en el sistema objetivo a través de sitios Web
Contenido:	· Software

### Ejemplo De Uso 2: Agencia De Inteligencia

El cliente implementó el producto **FinFly ISP en los sistemas del principal proveedor de servicios de Internet (ISP) del país**. Se **combinó con FinFly Web** para **implementar de forma remota la carga cuando el objetivo visitó un sitio Web de confianza**.



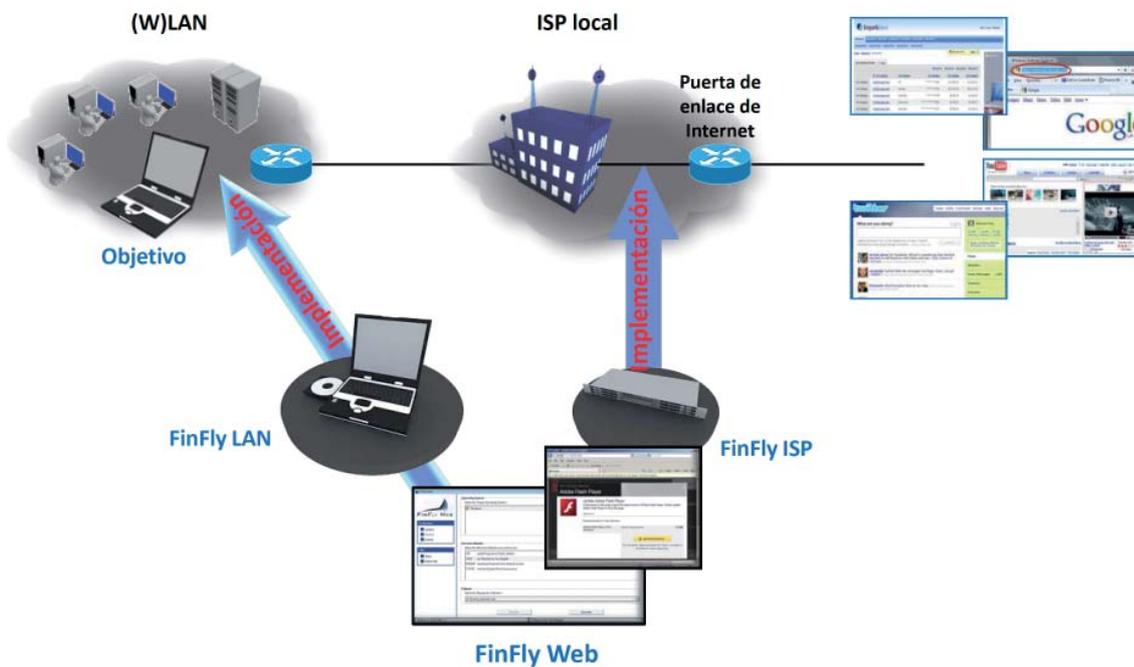
### Componentes Del Producto



#### FinFly Web

- Generador de sitios WebWeb personalizados

### Total integración con FinFly LAN y FinFly ISP



En muchas ocasiones, **no se pueden utilizar** métodos de implementación estándar para soluciones de monitorización remota cuando se trata con **objetivos muy experimentados y extremadamente cuidadosos**, ya que conocen las técnicas y herramientas de implementación habituales.

En la mayoría de los casos, las **explotaciones de tipo "Zero Day"** ofrecen una forma extremadamente potente y **fiable de implementar soluciones de monitorización remota** aprovechando **vulnerabilidades aún sin solucionar** en el software que utiliza el cliente.

El Portal de explotaciones de FinFly permite acceder a **una amplia biblioteca** de explotaciones de "Zero Day" y de "One Day" para aplicaciones de software populares como Microsoft® Office, Internet Explorer, Adobe Acrobat Reader, y muchas más.

### Ejemplo De Uso 1: Unidad de Delitos Tecnológicos

Una unidad de delitos tecnológicos estaba **investigando un delito cibernético** y necesitaba implementar una solución de monitorización remota en un sistema objetivo. Utilizaron una explotación de tipo Zero Day de Adobe Acrobat Reader y enviaron un archivo PDF preparado por correo electrónico al objetivo. La solución de monitorización remota se implementó automáticamente en cuanto el objetivo abrió el archivo.

### Descripción General De Funciones

- Acceso completo al **portal Web y generador de explotaciones**
- **Explotaciones de Zero Day de categoría gubernamental** que funcionan en varios sistemas y niveles de parche **sin modificación posterior**
- Al menos **4 explotaciones principales** (software habitual de navegador/correo/visor de archivos) disponible permanentemente
- **Garantía de 30 días** para todas las explotaciones del portal
- **Explotaciones de One Day** permanentemente actualizadas para distintas aplicaciones de software

Encontrará la lista completa de funciones en las Especificaciones del producto

DE UN VISTAZO	
Uso:	· Operaciones estratégicas
Capacidades:	· Implementa una solución de monitorización remota en el sistema objetivo a través de sitios Web
Contenido:	· Software

### Ejemplo De Uso 2: Agencia De Inteligencia

Se identificó a un objetivo **en un panel de discusión**, pero el contacto por correo electrónico no era posible. La Agencia creó un servidor Web con una **explotación de "Zero Day" de Internet Explorer** que implementó la carga en el sistema objetivo **una vez que el objetivo abrió la URL** que se le envió a través de un mensaje privado en el panel de discusión.



### Componentes Del Producto



#### Portal de explotaciones de FinFly

- Biblioteca de explotaciones de interfaz Web

### Ejemplo del portal de explotaciones de FinFly

#### ■ Microsoft Internet Explorer 9-8-7-6 Remote Code Execution Exploit

A use-after-free vulnerability exists in Microsoft Internet Explorer when processing certain JavaScript and HTML data, which could be exploited to compromise a vulnerable system via a specially crafted web page.

The vulnerability affects Microsoft Internet Explorer 9, 8, 7 and 6, on Windows 7 SP1 and prior, Windows Vista SP2 and prior, and Windows XP SP3 and prior.

The provided code execution exploit bypasses ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention) and works on all Windows systems.

- [More Information and Details](#) (Exploit updated on 2011-10-14. Exploit first released on 2011-08-06)

#### ■ Microsoft Internet Explorer 9-8 Remote Sandbox Bypass Exploit

A vulnerability exists in Microsoft Internet Explorer's sandbox (Protected Mode) when processing certain data from a Low integrity process, which could be exploited to achieve code execution in Medium integrity and bypass Protected Mode.

The vulnerability affects Microsoft Internet Explorer 9 and 8 on Windows 7 SP1 and prior and Windows Vista SP2 and prior (Windows XP SP3 and prior do not include a sandbox).

The provided exploit must be combined to another IE code and must be used as a second stage shellcode.

- [More Information and Details](#) (Exploit updated on 2011-10-14. Exploit first released on 2011-03-02)

#### ■ Adobe Acrobat & Reader 9.x PDF Processing Code Execution Exploit

A buffer overflow vulnerability exists in Adobe Acrobat and Reader when processing certain data within a PDF document, which could be exploited to compromise a vulnerable system by tricking a user into opening a malicious PDF file.

The provided code execution exploit bypasses ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention) and works on all Windows systems.

- [More Information and Details](#) (Exploit updated on 2011-09-02. Exploit first released on 2011-07-15)

En muchas operaciones reales, es posible que no se pueda tener acceso físico a los sistemas objetivo del propio país y que sea necesaria la **instalación remota encubierta** de una solución de monitorización remota para poder **monitorizar el objetivo desde la sede central de la agencia gubernamental**.

FinFly ISP es una solución (móvil) **estratégica y táctica de escala nacional** que se puede **integrar en la red de núcleo y/o de acceso de un proveedor de servicios de Internet** para instalar de forma remota la solución de monitorización remota en los sistemas objetivo seleccionados.

Los componentes de FinFly ISP se basan en la **tecnología de servidores de nivel de operador** y proporcionan la máxima **fiabilidad y escalabilidad** para hacer frente a casi cualquier reto relacionado con las topologías de redes. Hay una gran variedad de interfaces de red disponibles, todas ellas **protegidas con funciones de omisión**, para la conectividad de red activa.

Los múltiples métodos, activos y pasivos, de identificación de objetivos, **desde la monitorización en línea** mediante interceptación pasiva hasta la **comunicación interactiva** entre FinFly ISP y los servidores AAA, garantizan la identificación de todos los objetivos y el suministro de canales adecuados para el proceso de implementación.

FinFly ISP puede **modificar archivos** descargados por el objetivo **en tiempo real o enviar falsas actualizaciones** para aplicaciones de software populares. La nueva versión incluye la potente aplicación de implementación remota de Gamma **FinFly Web**, que permite introducir una carga en cualquier sitio web que visite el objetivo.

### Descripción General De Funciones

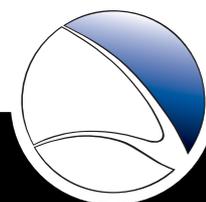
- Se puede instalar dentro de la **red de un proveedor de servicios de Internet (ISP)**
- Es compatible con **todos los protocolos más comunes**
- Objetivos seleccionados por **dirección IP, nombre de inicio de sesión de RADIUS, DHCP y MSISDN**
- Oculta la solución de monitorización remota en las **descargas de los objetivos**
- Disfraza la solución de monitorización en forma de **actualizaciones de software**
- Instala de forma remota soluciones de monitorización remota a través de los sitios **Web que visita el objetivo**

Encontrará la lista completa de funciones en las Especificaciones del producto.

DE UN VISTAZO	
Uso:	· Operaciones estratégicas
Capacidades:	· Implementa una solución de monitorización remota en el sistema objetivo a través de una red ISP
Contenido:	· Hardware/Software

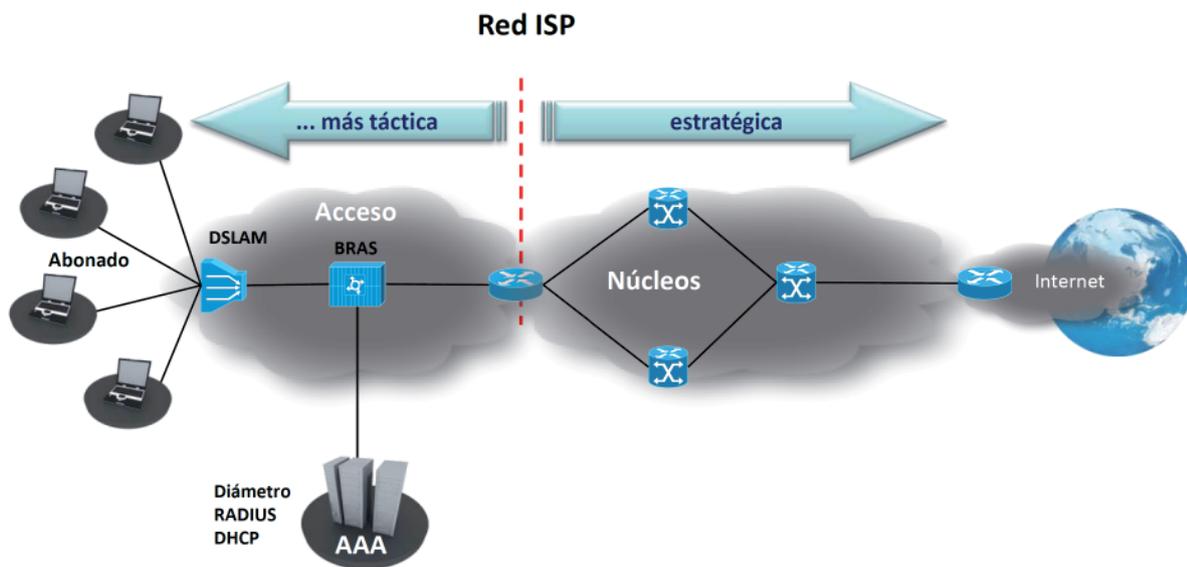
### Ejemplo De Uso: Agencia De Inteligencia

FinFly ISP se implementó en las redes del principal proveedor de servicios de Internet del país y se usó activamente para implementar de forma remota una solución de monitorización remota en los sistemas objetivo. Dado que los objetivos tienen conexiones DSL con IP dinámica, se identifican mediante su nombre de inicio de sesión de RADIUS.



### Varias posibilidades de ubicación

- FinFly ISP se puede utilizar como solución táctica o estratégica en redes ISP



Una solución táctica es de naturaleza móvil, y el hardware se dedica a las tareas de infección dentro de la red de acceso, cerca de los puntos de acceso de los objetivos. Se puede implementar a corto plazo para satisfacer requisitos tácticos centrados en un objetivo específico o un número reducido de objetivos en un área determinada.

Una solución estratégica sería, por el contrario, permanente. La instalación de FinFly ISP en los sistemas de un

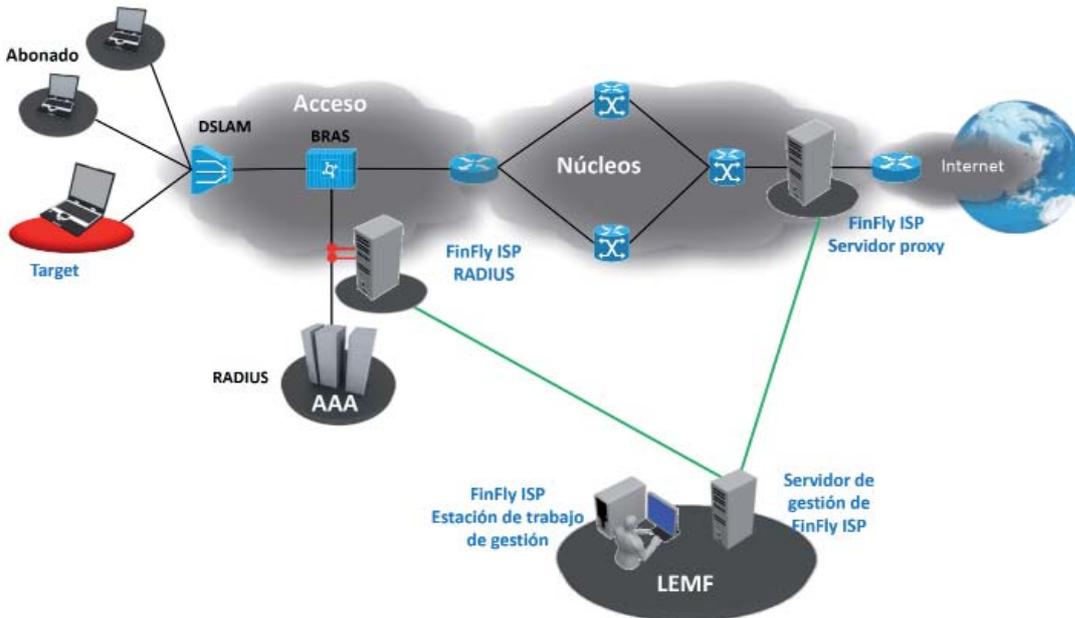
proveedor de servicios de Internet o a escala de todo el país para seleccionar objetivos e implementar de forma remota cargas desde la sede central de la agencia gubernamental sin necesidad de que las fuerzas y cuerpos de seguridad se desplacen al lugar en cuestión.

Evidentemente, es posible combinar soluciones tácticas y estratégicas para otorgar la máxima flexibilidad posible a las operaciones de infección.

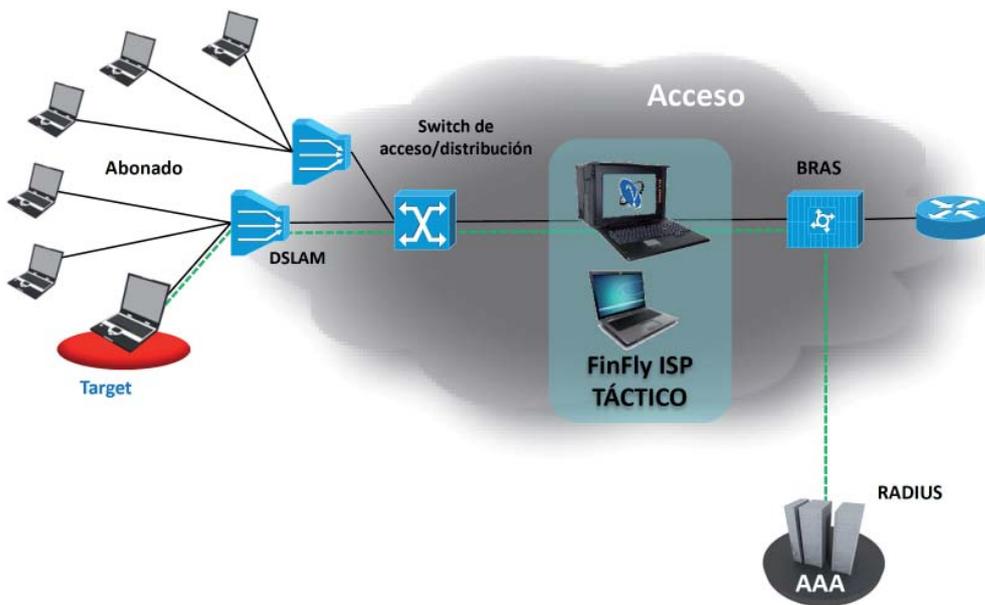


Configuración de la red

Implementación estratégica



Implementación táctica



### Componentes Del Producto

#### FinFly ISP Estratégico

Una implementación estratégica de FinFly ISP consta al menos de lo siguiente:

- Sistema de administración en el LEMF
- Servidor(es) de identificación de objetivo en el sistema AAA de la red
- Servidor(es) proxy de infección en la(s) puerta(s) de enlace de Internet, por ejemplo



#### FinFly ISP Táctico

Un sistema FinFly ISP táctico consta de lo siguiente:

- Servidor proxy portátil de identificación de objetivos e infección
- Ordenador portátil del sistema de gestión



<b>Capacidad de proceso</b>	> 20 Gbps
<b>Nº máx. de NIC:</b>	2-8 NIC
<b>Interfaces:</b>	1 GE Cobre / Fibra 10 GE Cobre / Fibra SONET/SDH OC-3 / -192 STM-1 / -64 ATM AAL5
<b>Procesadores:</b>	De 1 a 8 Intel XEON
<b>Núcleos</b>	2 – 8 núcleos / procesador
<b>RAM:</b>	12 GB – 1 TB
<b>Capacidad de disco duro:</b>	3 SAS de 146 GB – 4,8 TB
<b>Características</b>	HP iLO 3 Alimentación redundante Ventiladores redundantes Función de conmutación de derivación (si existe)
<b>Sistema operativo</b>	Linux GNU (Debian 5.0) reforzado

<b>Capacidad de proceso</b>	6 Gbps
<b>Nº máx. de NIC:</b>	3 NIC
<b>Interfaces:</b>	1x 1000BASE-T (cobre; 2 puertos) 1x 1000BASE-SX (fibra MM; 2 puertos) 1x 1000BASE-LX (fibra SM; 2 puertos) Otros bajo petición
<b>Procesadores:</b>	1 Intel Core i7 Intel Xeon bajo petición
<b>Núcleos</b>	4 núcleos / procesador
<b>RAM:</b>	Mínimo de 12 GB
<b>Capacidad de disco duro:</b>	2 SATA de 1 TB
<b>Unidad óptica</b>	DVD+/-RW SATA
<b>Monitor</b>	1 TFT de 17", teclado, panel táctil
<b>Características</b>	Función de conmutación de derivación para NIC
<b>Sistema operativo</b>	Linux GNU (Debian 5.0) reforzado Windows 7 Prof. (portátil de gestión)

En muchas operaciones reales, es posible que no se pueda tener acceso físico a los sistemas objetivo del propio país.

Para resolver esto, es necesaria una **solución de monitorización remota encubierta para poder monitorizar el objetivo desde la sede central de la agencia gubernamental.**

**FinFly NET** es una solución **táctica** (portátil) que se debe implementar en un **entorno de LAN "amigable"** (como hoteles, puntos de conexión inalámbrica, empresas, con la asistencia del dueño de la red) con poca antelación, para instalar de forma remota la Solución de monitorización remota en los sistemas objetivo seleccionados.

FinFly NET se basa en un **equipo portátil de alto rendimiento** combinado con un **ordenador portátil de gestión** para ofrecer máxima movilidad y flexibilidad en las redes objetivo. Una amplia variedad de tarjetas de interfaz de red disponibles, todas ellas **protegidas con funciones de omisión**, para la conectividad de red activa.

El usuario final puede elegir entre diversos y **sofisticados métodos pasivos de identificación de objetivos y tráfico**. Estos van desde la monitorización DHCP/RADIUS (direcciones MAC, nombres de usuario) y la monitorización de flujos hasta la identificación remota de un sistema operativo (fingerprinting). Cada uno de los métodos se puede usar de forma independiente o combinada para ofrecer la máxima eficacia a la hora de identificar los objetivos de interés. Sumado a ello también se pueden utilizar direcciones IP fijas.

Puede **modificar archivos descargados** por el objetivo en tiempo real, **enviar falsas actualizaciones** para aplicaciones de software populares o introducir la carga en sitios Web visitados.

### Descripción General De Funciones

- Se puede instalar en un **entorno de LAN** (hotel, punto de conexión inalámbrica, empresa, etc.)
- Ethernet 1000Base-T, 1000Base-SX, 1000Base-LX
- Identifica los objetivos utilizando distintos **métodos pasivos de identificación y definición de perfiles**
- Oculta una solución de monitorización remota en las **descargas de los objetivos**
- Disfraza la solución de monitorización en forma de **actualizaciones de software**
- Instala una solución de monitorización remota a través de los **sitios web que visita el objetivo**

Encontrará la lista completa de funciones en las Especificaciones del producto.

DE UN VISTAZO	
Uso:	· Operaciones tácticas
Capacidades:	· Implementa una solución de monitorización remota en el sistema objetivo en un entorno de LAN "amigable"
Contenido:	· Hardware/Software

### Ejemplo de uso de LAN: Agencia De Inteligencia

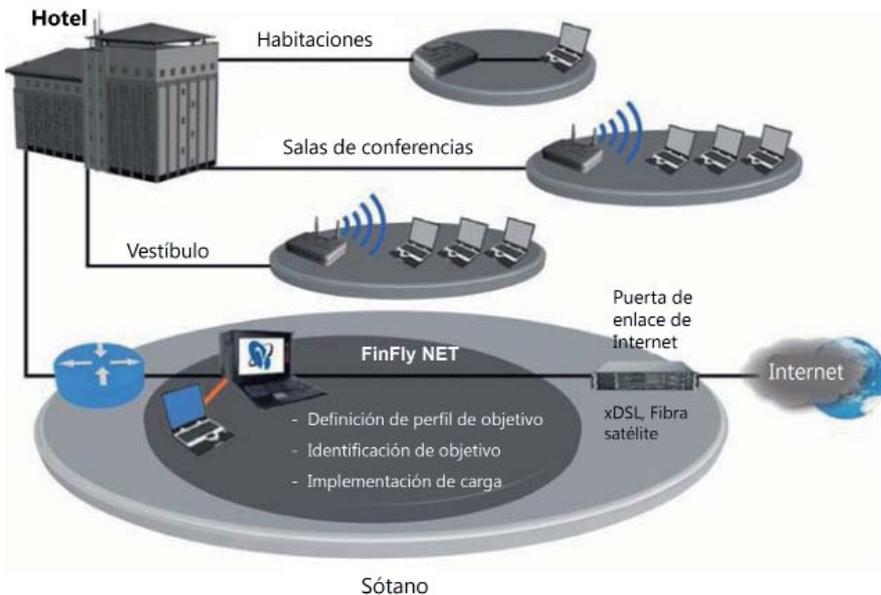
FinFly NET se implementa, por ejemplo, en la red LAN de un hotel por delante del módem DSL antes de que el tráfico IP se transmita a la red de un proveedor de servicios de Internet (ISP).

Gracias a distintos métodos pasivos de identificación y definición de perfiles, se identifican los objetivos de interés en el tráfico IP y luego se implementará una solución de monitorización remota en los sistemas objetivos identificados positivamente.

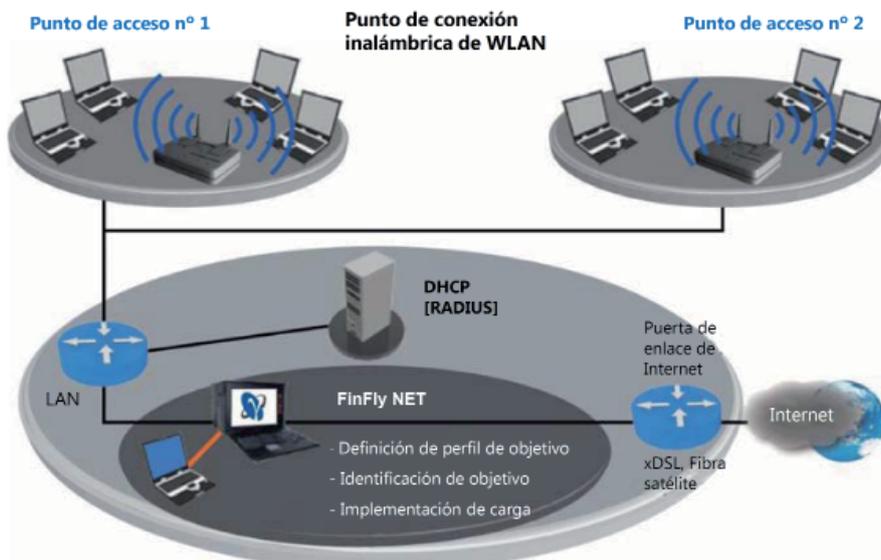


### DISTINTAS POSIBILIDADES DE IMPLEMENTACIÓN

#### Implementación en la LAN de un hotel



#### Implementación en la LAN de un punto de conexión inalámbrica de WLAN



FinFly NET se implementará en el lugar adecuado dentro de la instalación. Tras conectar la línea de entrada portátil al(a los) enlace(s) facilitado(s), el usuario puede empezar a analizar el tráfico eligiendo entre distintos métodos para identificar los objetivos de interés y su tráfico IP. Los métodos que se deben utilizar para la identificación del objetivo dependen considerablemente de la configuración de la red, de las funciones, y de los servicios facilitados y usados.



### **DEFINICIÓN DE PERFILES E IDENTIFICACIÓN DE OBJETIVO**

---

#### **Módulo rastreador de HTTP**

Tipos y versiones de navegador y sistema operativo, historial, idiomas

#### **Módulo rastreador de correo electrónico**

POP3, SMTP

#### **Módulo rastreador de inicio de sesión**

FTP, HTTP, IMAP, IRC, NNTP, POP, SMTP

#### **Módulo rastreador de TCP/UDP**

IP de origen/destino, puertos de origen/destino

#### **Módulo rastreador de DHCP/RADIUS**

MAC, nombre de host, inicio/fin de sesión IP

### **MÉTODOS DE IMPLEMENTACIÓN DE OBJETIVO**

---

#### **Binario/Descarga**

Modificación de archivos ".exe" y/o ".scr"

#### **Introducción de actualización**

Falsas actualizaciones para distintas aplicaciones

#### **Implementación en sitio Web**

Utilizar FinFly Web para la implementación durante la navegación



### Componentes Del Producto

FinFly NET consta de lo siguiente:

- Definición de perfiles de objetivo, identificación e implementación de servidor proxy
- (Portátil)
- Sistema de gestión (portátil)



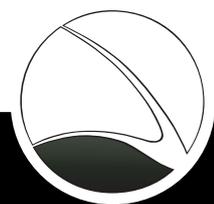
<b>Capacidad de proceso</b>	6 Gbps
<b>Nº máx. de NIC:</b>	3 NIC
<b>Interfaces:</b>	1x 1000BASE-T (cobre; 2 puertos) 1x 1000BASE-SX (fibra MM; 2 puertos) 1x 1000BASE-LX (fibra SM; 2 puertos) Otros bajo petición
<b>Procesadores:</b>	1 Intel Core i7 Intel Xeon bajo petición
<b>Núcleos</b>	4 núcleos / procesador
<b>RAM:</b>	Mínimo de 12 GB
<b>Capacidad de disco duro:</b>	2 SATA de 1 TB
<b>Unidad óptica</b>	DVD+/-RW SATA
<b>Monitor</b>	1 TFT de 17", teclado, panel táctil
<b>Características</b>	Función de conmutación de derivación para NIC
<b>Sistema operativo</b>	Linux GNU (Debian 5.0) reforzado Windows 7 Prof. (portátil de gestión)

### Nota importante:

Gamma ofrece junto a FinFly NET las mismas capacidades de inteligencia integradas en la solución FinFly ISP, mientras que las capacidades de identificación de objetivos se implementan en una solución ISP fija o portátil. Esta solución se caracteriza por una tecnología de servidor de alto rendimiento que se personalizará e integrará en el entorno ISP relevante y según las necesidades relacionadas.



El programa de formación en intrusiones de TI incluye cursos sobre nuestros productos, y sobre técnicas y métodos prácticos de intrusión. Este programa formativo transmite años de experiencia y conocimientos acumulados a los usuarios finales, maximizando así su capacidad para operar en este campo.



La capacitación en materia de seguridad es **esencial para cualquier gobierno** que quiera **preservar la seguridad** de las tecnologías de la información y evitar las amenazas a las que están expuestas sus infraestructuras, que podrían poner en jaque la confidencialidad, integridad y disponibilidad de los datos que contienen.

Por otra parte, temas como la **guerra cibernética**, la interceptación activa y la obtención de inteligencia a través de la **intrusión de sistemas de TI** tienen cada vez más importancia en el día a día de los gobiernos, y exigen la **configuración de equipos de intrusión de sistemas de TI** para **hacer frente a estos nuevos retos**.

Los docentes de los cursos de FinTraining son **expertos de primer orden mundial en el campo de las intrusiones de TI** y en los cursos se abordan **escenarios eminentemente prácticos**, centrados en las **operaciones reales** que el usuario final necesita aprender a resolver para poder solucionar los **problemas a los que deben hacer frente día tras día**.

**Gamma** integra los cursos de formación individualizada en un **programa de consultoría y formación profesional** que permite configurar o mejorar las capacidades de un equipo de especialistas en intrusiones de TI. Estos cursos de formación son **totalmente personalizados** en base a las necesidades y las particularidades operativas a las que deba enfrentarse el usuario final.

### Ejemplos de los temas del curso

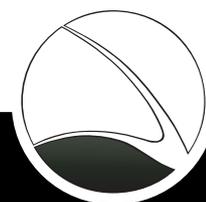
- **Definición de perfiles** de sitios Web y personas objetivo
- Seguimiento de correos **electrónicos anónimos**
- **Acceso remoto** a cuentas de correo Web
- **Evaluación de seguridad** de servidores y servicios Web
- **Explotación práctica de software**
- **Intrusión de TI inalámbrica** (WLAN/802.11 y Bluetooth)
- Ataques a **infraestructuras críticas**
- Rastreo de **datos y credenciales de usuarios** de redes
- **Monitorización de puntos de acceso inalámbrico**, cibercafés y redes de hoteles
- **Intercepción y grabación de llamadas** (VoIP y DECT)
- **Rotura de funciones hash de contraseñas**

DE UN VISTAZO	
Uso:	· <b>Transferencia de conocimientos</b>
Capacidades:	· <b>Conocimientos en materia de intrusiones de TI</b> · <b>Capacitación en guerra cibernética</b>
Contenido:	· <b>Formación</b>

### Programa de asesoría

- Programa completo de **consultoría y formación** en intrusión de TI
- **Formación y configuración estructurada de equipos especializados en intrusiones de TI**

Encontrará la lista completa de funciones en las Especificaciones del producto



Cursos personalizados en instalaciones de formación avanzadas de todo el mundo



### FinSupport

FinSupport ofrece mejoras y actualizaciones de la línea de productos FinFisher™ en combinación con un contrato de asistencia anual.

La página Web y el equipo de asistencia de FinFisher™ ofrecen los siguientes servicios a nuestros clientes:

- Acceso en línea a:
  - Manual de usuario más reciente
  - Especificaciones más recientes del producto
  - Diapositivas de formación sobre el producto más recientes
  - Sistema de comunicación de errores
  - Último informe de comprobación de antivirus
  - Sistema de solicitud de características
  - Feature Request Frontend
- Actualizaciones regulares de software:
  - Parches de corrección de errores
  - Nuevas características
  - Nuevas versiones importantes
- Asistencia técnica a través de Skype:
  - Corrección de errores
  - Asistencia operativa

### FinLifelineSupport

FinLifelineSupport ofrece asistencia administrativa profesional para resolución de problemas y consultas técnicas. También ofrece asistencia administrativa remota para corrección de errores de software de FinFisher™ y sustituciones de hardware dentro de la garantía. Además, con FinLifelineSupport, el cliente recibe automáticamente nuevas características y funciones con la versión estándar de los parches de corrección de errores.

#### DE UN VISTAZO

Uso:	· Solución general y asistencia operativa
Capacidades:	· Solución de errores, actualización de funciones y capacidades
Contenido:	· Hardware/Software

### Actualizaciones de software

FinLifelineSupport incluye actualizaciones regulares de software y garantiza mejoras automáticas del sistema existente con parches de software que se suministran a través del sistema de actualización.

Estas mejoras incluyen nuevas características, nuevas mejoras y nuevas funciones según las necesidades del cliente (excluyendo el hardware).



**WWW.FINFISHER.COM**

La información contenida en el presente documento es confidencial y puede sufrir cambios sin previo aviso.  
Gamma Group International no se responsabiliza de las omisiones o los errores



**GAMMAGROUP**

GAMMA INTERNATIONAL  
United Kingdom

Tel : +44 - 1264 - 332 411  
Fax : +44 - 1264 - 332 422