



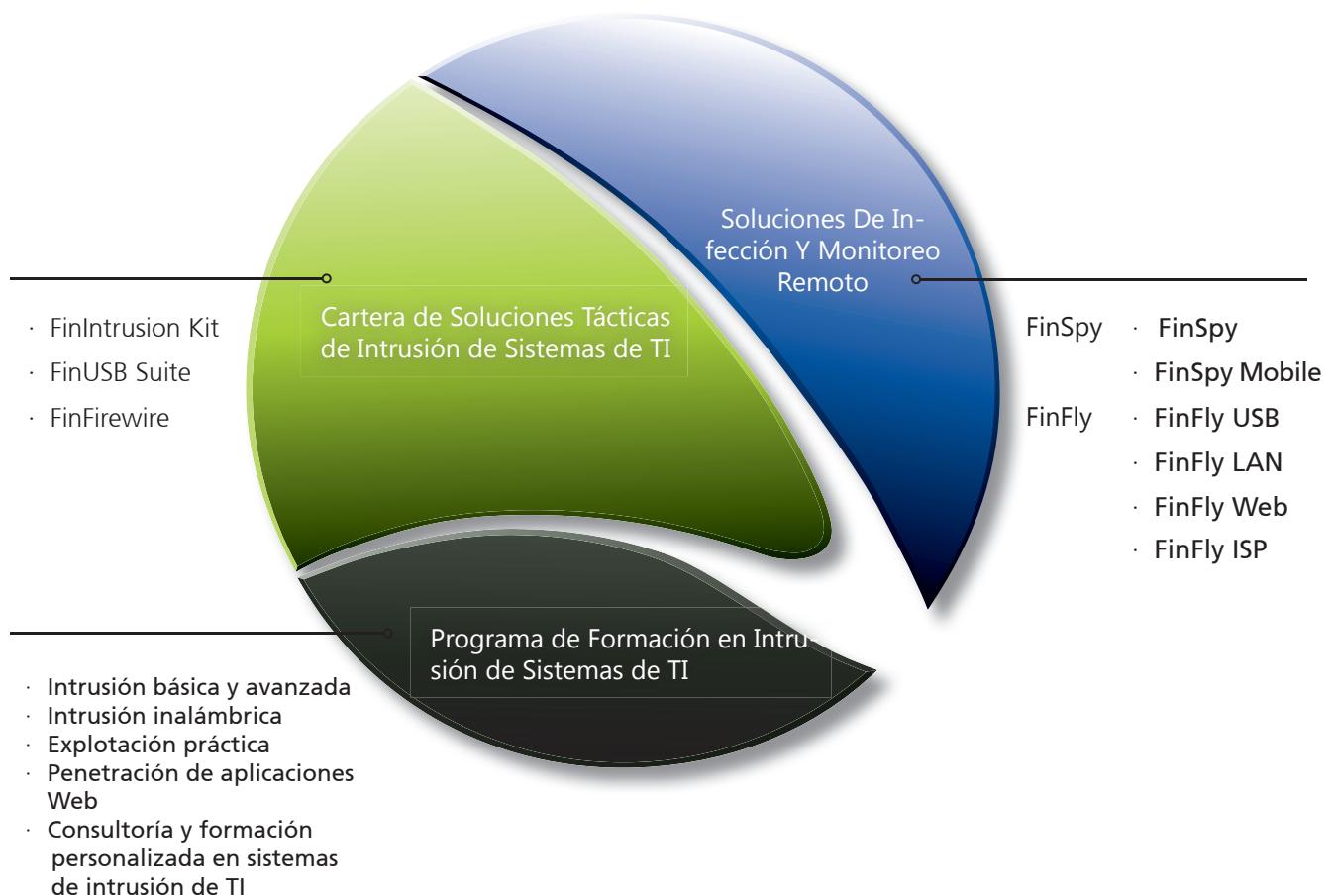
**FINFISHER™ : SOLUCIONES DE MONITOREO REMOTO
E INTRUSIÓN DE SISTEMAS DE IT
PARA GOBIERNOS**



FINFISHER™

IT INTRUSION

WWW.GAMMAGROUP.COM

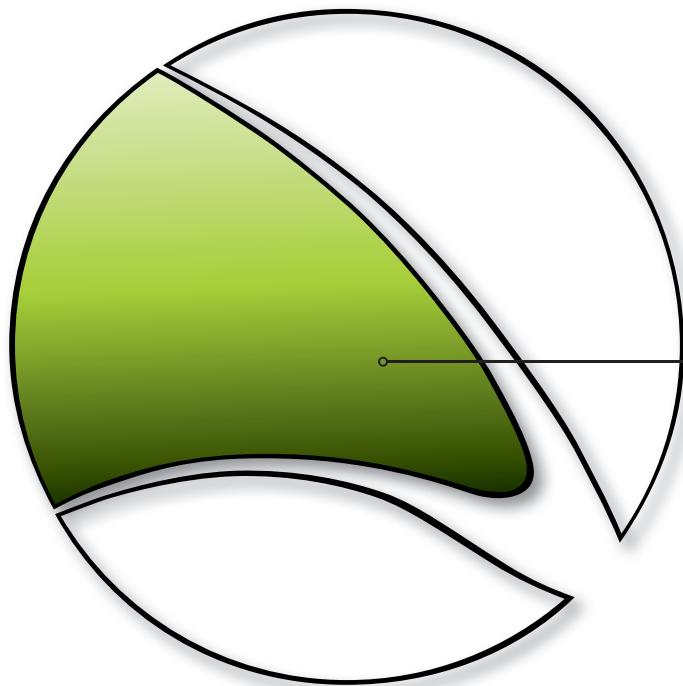


Cartera De Soluciones Tácticas De Intrusión De TI

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.



FINFISHER™
IT INTRUSION

Cartera De Soluciones Tácticas De Intrusión De TI

FININTRUSION KIT

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 el resultado de 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 hay **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 quebrantar **el cifrado WPA** de la red inalámbrica del hogar de un objetivo y para monitorear sus **credenciales de acceso al correo web (Gmail, Yahoo, etc.) y a redes sociales (Facebook, MySpace, etc.)**. lo que permitió a los investigadores **monitorizar de forma remota** estas cuentas desde los cuarteles centrales sin necesidad

DE UN VISTAZO	
Uso:	<ul style="list-style-type: none">· Operaciones estratégicas· Operaciones tácticas
Capacidades:	<ul style="list-style-type: none">· Romper cifrados WEP/WPA· Monitorizar redes (incluyendo sesiones SSL)· Ataques de intrusión de TI
Contenido:	<ul style="list-style-type: none">· Hardware/Software

de acercarse al objetivo.

Ejemplo De Uso 2: Seguridad De TI

Varios clientes han utilizado FinIntrusion Kit para **quebrantar 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 (p. ej. blogs o grupos de discusión) y monitorear sus actividades controlando, entre otros, elementos como los registros de acceso.

Descripción General De Funciones

- Descubre **redes WLAN (802.11) y dispositivos Bluetooth®**.
- Recupera contraseñas WEB (de 64 y 128 bits) en **entre 2 y 5 minutos**.
- **Descifra contraseñas WPA1 y WPA2** utilizando ataques con diccionarios.
- Monitorea de manera activa redes de LAN (por cable e inalámbricas) y **extrae nombres de usuario y contraseñas incluso en sesiones con cifrado TLS/SSL**.
- Emula **puntos de acceso inalámbrico hostiles (802.11)**.
- **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



FINFISHER™
IT INTRUSION

Cartera De Soluciones Tácticas De Intrusión De TI

FININTRUSION KIT

Componentes Del Producto



A screenshot of the FinTrack Operation Center software. The interface has a sidebar with 'FTOC' logo and 'Configuration' section. The main area shows a 'Welcome to the FinTrack Operation Center.' message and a 'Select a Category to continue.' prompt. Under the 'Network' tab, there are four items listed: 'Network' (Record Passwords in Local Area Network (LAN)), 'Wireless' (Monitor Wireless Networks and Clients), 'Bluetooth' (Common Bluetooth Intrusion Techniques), and 'E-Mail' (Remotely gain access to E-Mail Accounts). A footer bar at the bottom says 'Welcome to Finintrusion Kit 0.9'.

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 sistemas de TI .

Monitorización automática de LAN/WLAN

A screenshot of the FinTrack Operation Center software showing the 'Network' tab configuration. The sidebar has 'Updates' and 'License' sections. The main area shows 'Configuration' tab selected. It lists network parameters: Interface (eth0), IP Address (62.168.39.90), Netmask, Gateway (62.168.39.65), Broadcast (255.255.255.255), Nameserver (208.67.222.222, 208.67.220.220, 156.154.70.1, 156.154.71.1), MAC Address (0026B9008EAC), and Status (Up).

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.

Username	Password	Server	Protocol
dropbox	fr33dom	64.223.183.17	https
ftp	secret1	128.101.240.212	ftp
ftoc	password1	62.84.74.92	pop3

Start **Delete** **Save...**



Cartera De Soluciones Tácticas De Intrusión De TI

FINUSB SUITE

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

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

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, videos 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.

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 Trojan Horse. 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.

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.



FINFISHER™
IT INTRUSION

Cartera De Soluciones Tácticas De Intrusión De TI

FINUSB SUITE

Componentes Del Producto



FinUSB Suite – Unidad Móvil



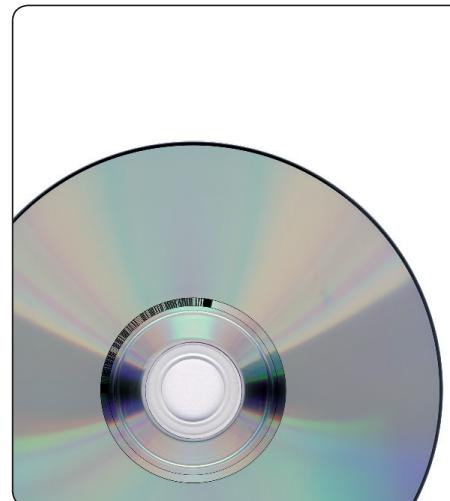
FinUSB HQ

- 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.
- Cifra datos sobre la marcha.



FinUSB – Omisión De La Contraseña De Windows

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

Cartera De Soluciones Tácticas De Intrusión De TI

FINUSB SUITE

Máxima Facilidad De Uso



1. Elegir una llave FinUSB.
2. Configurar todos 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

The screenshot shows the FINUSB HQ software interface. At the top, there's a black header bar with the 'FINUSB HQ' logo. Below it is a grey navigation bar with the title 'FinUSB Suite: Report'. The main content area is divided into several sections:

- I. Generic**:
 - Generic Information
- II. Passwords**:
 - Windows Account Hashes
 - E-Mail Accounts
 - Messenger Accounts
 - Google Chrome Passwords
 - Firefox Passwords
 - Network Passwords
 - Protected Storage
 - Internet Explorer Accounts
- III. System**:
 - Windows Product Keys
 - Windows Updates
 - LSA Secrets
 - Current Processes
- IV. Network**:
 - Network Adapters
 - Network Ports
 - Internet Explorer History
 - Mozilla Firefox History
 - Wireless Keys
 - Mozilla Firefox Cookies

At the bottom of the interface, there's a 'Generic Information' section and a status bar indicating 'Computer | Protected Mode: Off' and '75%'. The entire window has a dark theme with light-colored text and icons.



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 en ejecución**, 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:	<ul style="list-style-type: none">· Operaciones tácticas
Capacidades:	<ul style="list-style-type: none">· Omite la contraseña de usuario· Accede al sistema de forma encubierta· Recupera contraseñas de RAM· Permite la realización de análisis forenses en tiempo real
Contenido:	<ul style="list-style-type: none">· 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.



Cartera De Soluciones Tácticas De Intrusión De TI

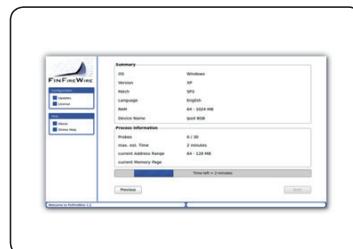
FINFIREWIRE

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.

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 técnicos o editoriales que pueda contener este documento.



GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411

Fax: +44 - 1264 - 332 422

info@gammagroup.com

Soluciones De Infección Y Monitoreo Remoto

FINSPY

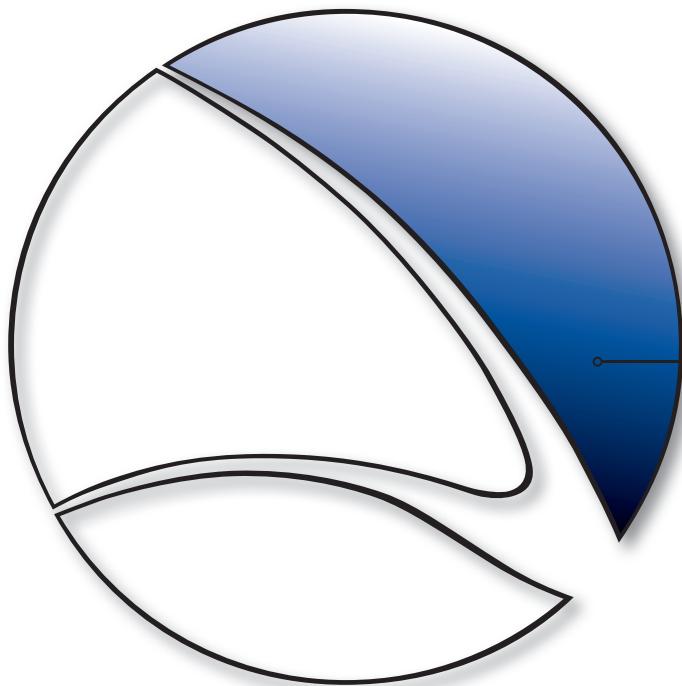
FINSPY MOBILE

FINFLY USB

FINFLY LAN

FINFLY WEB

FINFLY ISP



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.



FINFISHER™
IT INTRUSION

Soluciones De Infección Y Monitoreo Remoto

FINSPY

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 intercepción 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:

- Salteo de mas de 40 sistemas antivirus probada regularmente
- **Comunicación encubierta** con los cuarteles generales 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
- **Captura 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	
Uso:	· Operaciones estratégicas/tácticas
Capacidades:	· Monitorizar equipos remotos · Monitorizar comunicaciones cifradas
Contenido:	· Hardware/Software

Ejemplo De Uso 1: Agencia De Inteligencia

FinSpy se instaló en varios sistemas informáticos de **cibercafé en áreas críticas** para monitorearlos y detectar actividades sospechosas, especialmente **comunicaciones internacionales vía Skype**. 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 **Evidencia** (pruebas válidas de acuerdo con la **normativa europea**)
- **Administración de usuarios** según las autorizaciones de seguridad
- Comunicaciones y cifrado de datos de seguridad utilizando **RSA 2048 y AES 256**
- Oculto del público mediante **proxies anonimizantes**
- 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.



FINFISHER™
IT INTRUSION

Soluciones De Infección Y Monitoreo Remoto

FINSPY

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.

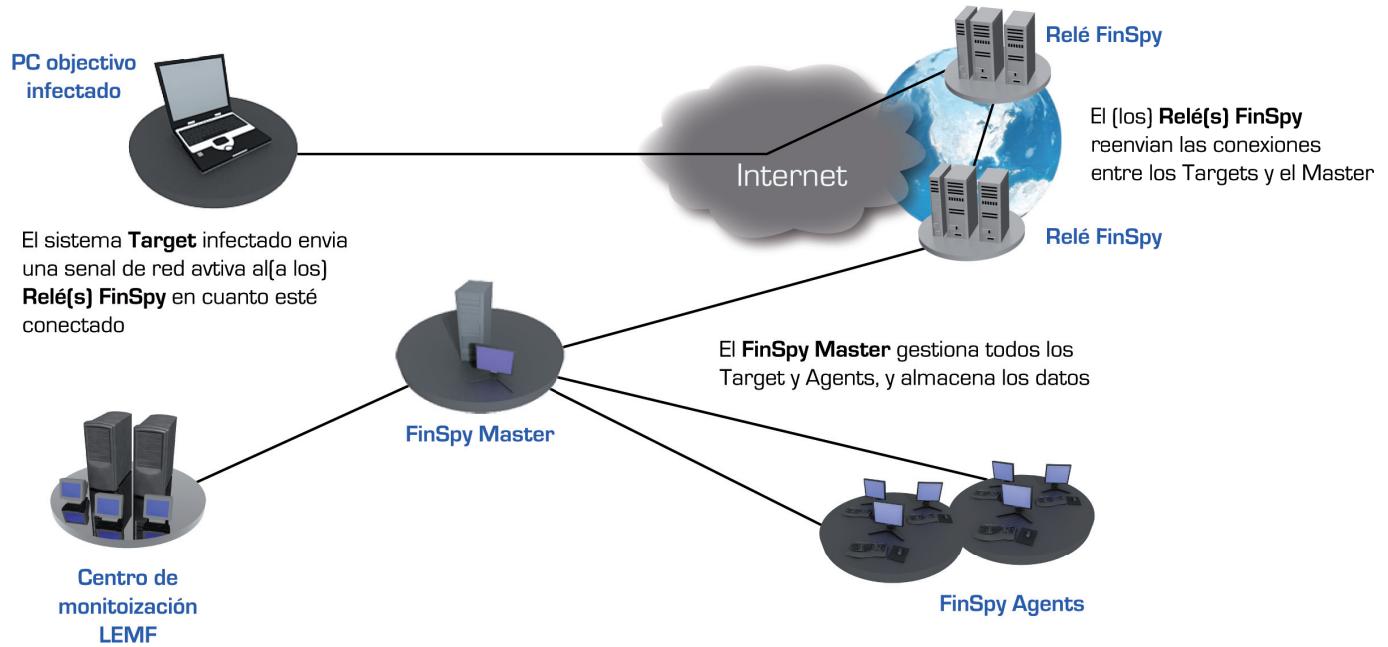
FinSpy Agent

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

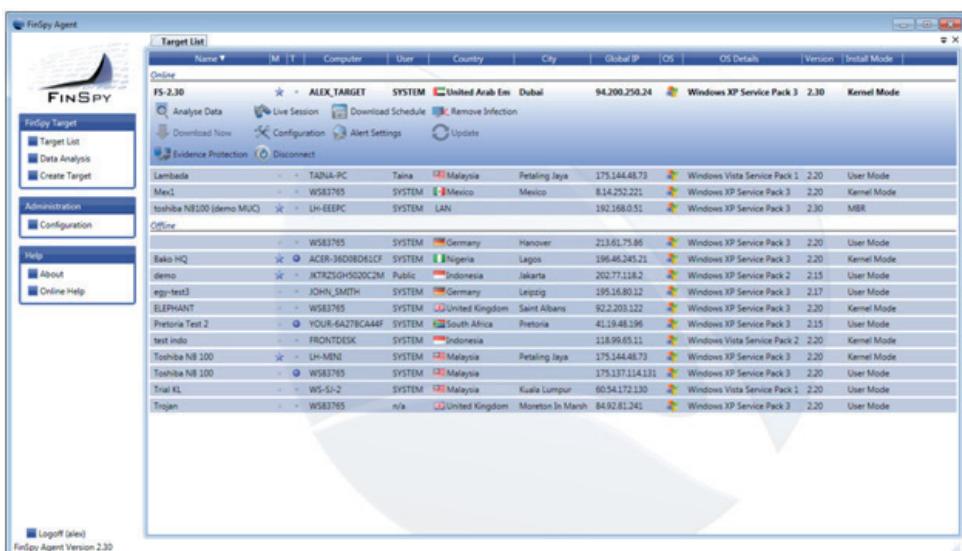
Soluciones De Infección Y Monitoreo Remoto

FINSPY

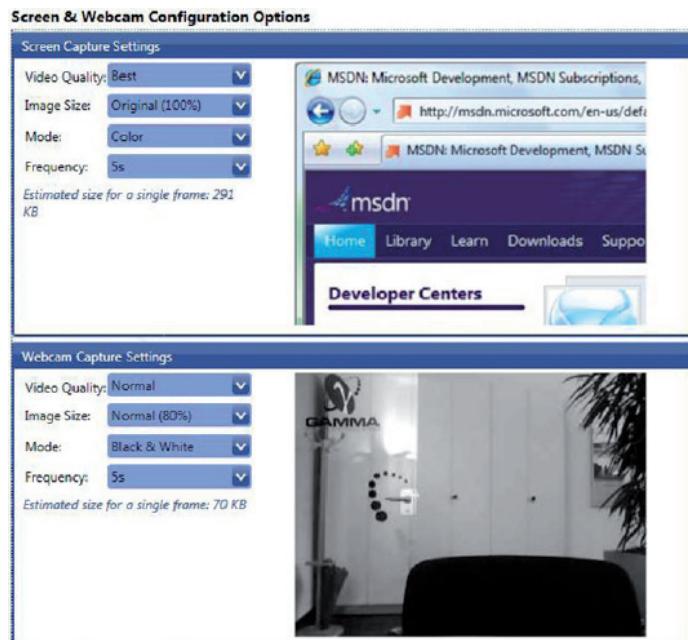
Acceso A Sistemas Informáticos De Cualquier Lugar Del Mundo



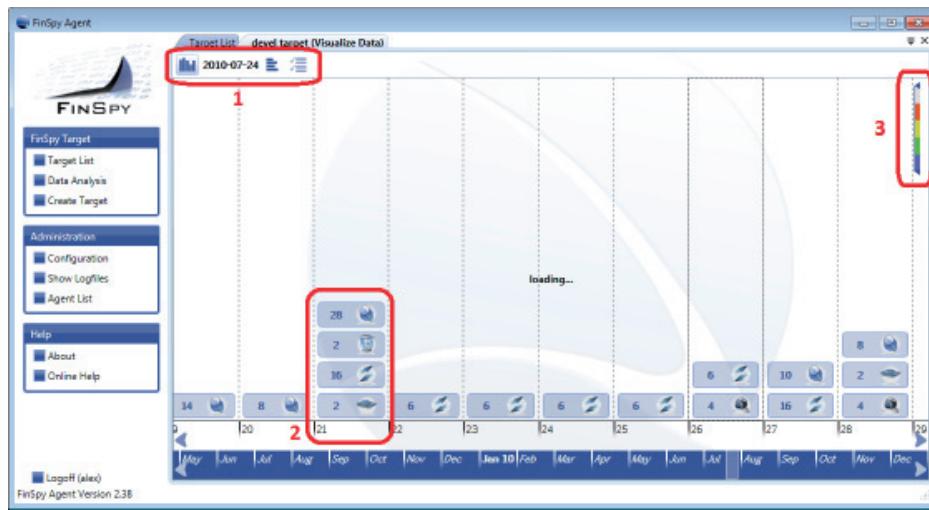
Interfaz De Usuario Fácil De Utilizar



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

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 técnicos o editoriales que pueda contener este documento.



GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422
info@gammagroup.com

FINSPY LICENSES

Descripción

La solución FinSpy contiene 3 tipos de licencia de producto:

A. Licencia de actualización

Esta licencia controla si **FinSpy** puede obtener nuevas actualizaciones del servidor de actualizaciones de Gamma. Se combina con el módulo de **Asistencia post-venta de FinFisherman™**.

Una vez que expire la licencia, el sistema **FinSpy** seguirá **funcionando**, pero ya no podrá descargar las versiones y parches más recientes del servidor de actualización de FinSpy.

B. Licencia de agente

Esta licencia controla el número de **FinSpy Agents** que pueden iniciar sesión en el **FinSpy Master** en paralelo.

Ejemplo:

Se han adquirido **5 licencias de agente**.

Las licencias de **FinSpy Agent** se pueden instalar en un número ilimitado de sistemas, pero

Solo 5 sistemas **FinSpy Agent** pueden iniciar en el **FinSpy Master** y trabajar con los **datos al mismo tiempo**

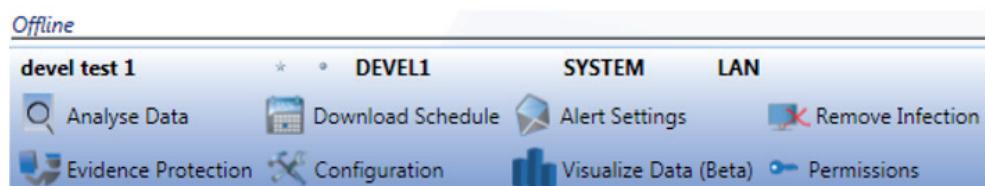
C. Licencia de objetivo

Esta licencia controla el número de **FinSpy Targets** que pueden estar activos en paralelo.

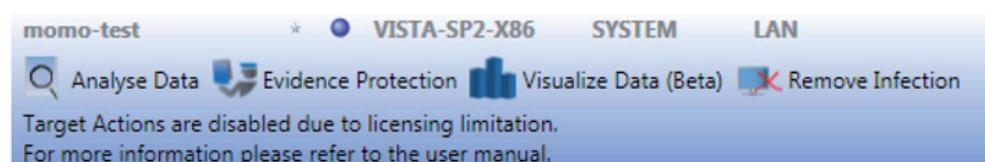
Activos se refiere a instalaciones de **FinSpy Target** activadas independientemente de que el sistema objetivo esté conectado o no.

Si se implementa FinSpy Target en un sistema objetivo y no hay ninguna licencia de objetivo disponible, el FinSpy Target se desactivará temporalmente y no se podrá ni grabar ni acceder en tiempo real. En cuanto haya una nueva licencia disponible (por ejemplo, actualizando la licencia existente o desinfectando uno de los **FinSpy Targets** activos), el objetivo recibirá una licencia libre, se activará, y empezará a grabar y a ofrecer acceso en tiempo real.

Captura de pantalla de un objetivo activo con licencia



Captura de pantalla de un objetivo inactivo sin licencia



Soluciones De Infección Y Monitoreo Remoto

FINSPY MOBILE

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

Concretamente, las organizaciones sin capacidades de **red o intercepción 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 intercepción 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 los cuarteles generales de la organización
- Grabación de las **comunicaciones comunes** por videollamada, 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 y Android**

DE UN VISTAZO

Uso:	<ul style="list-style-type: none">· Operaciones estratégicas· Operaciones tácticas
Capacidades:	<ul style="list-style-type: none">· Monitorización remota de teléfonos móviles
Contenido:	<ul style="list-style-type: none">· 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 Evidencia (pruebas válidas de acuerdo con la **normativa europea**)
- **Administración de usuarios** según las autorizaciones de seguridad
- Comunicaciones y cifrado de datos de seguridad utilizando **RSA 2048 y AES 256**
- Oculto del público mediante **proxies anonimizantes**
- 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

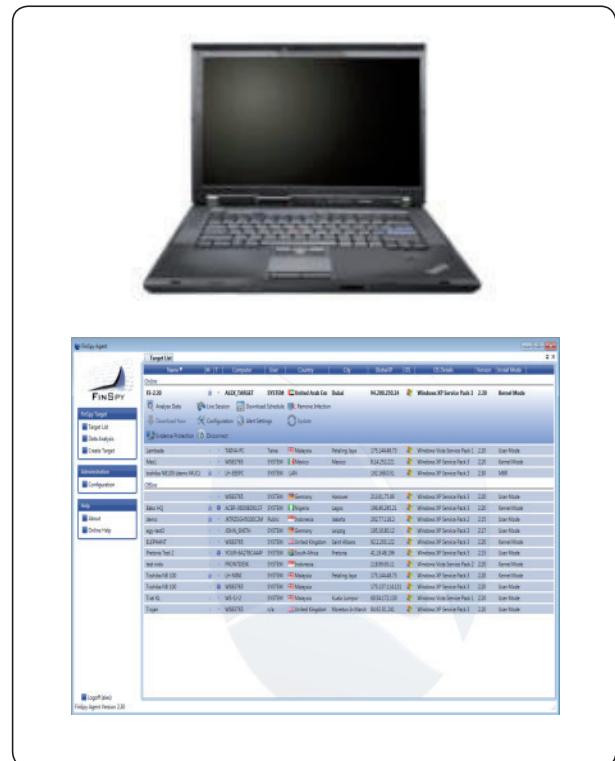


FINFISHER™
IT INTRUSION

Soluciones De Infección Y Monitoreo Remoto

FINSPY MOBILE

Componentes Del Producto



FinSpy Master y Proxy

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

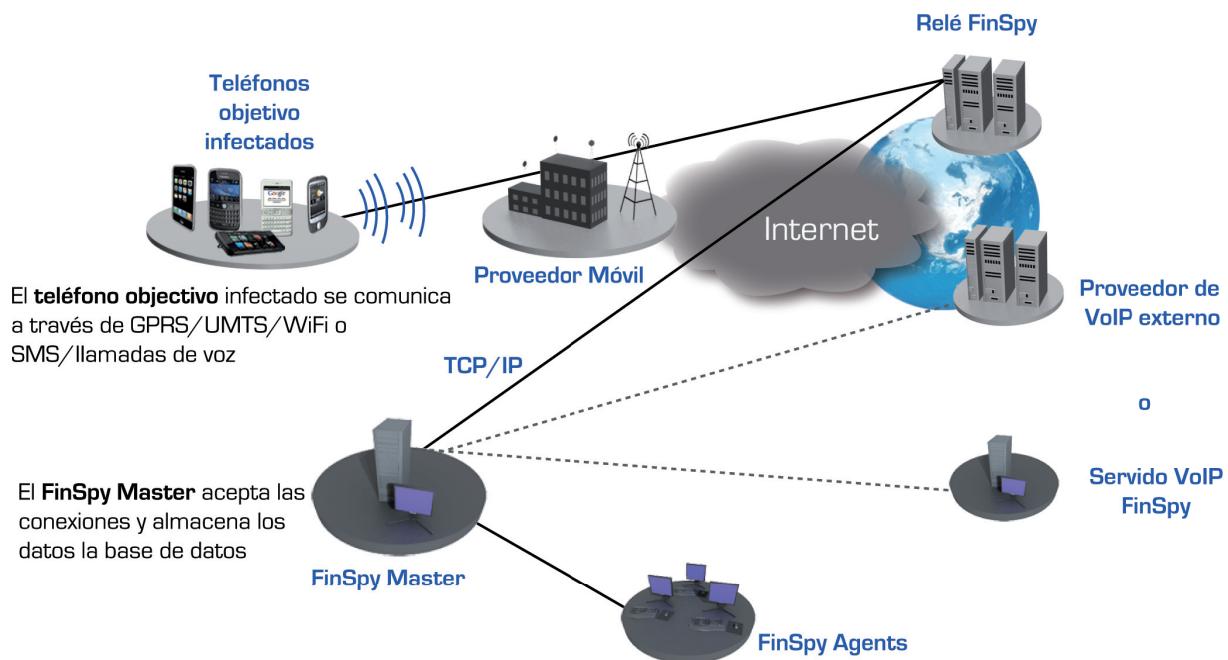
FinSpy Agent

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

Soluciones De Infección Y Monitoreo Remoto

FINSPY MOBILE

Acceso A Sistemas Informáticos De Cualquier Lugar Del Mundo



Interfaz de usuario fácil de utilizar

The screenshot shows the FINSPY MOBILE Event Report interface. The top navigation bar includes: Target Account, Configure, Event Report, Remote Command, License, Custom Report, and Logout (madmin).

The main area is titled "Event Report" and displays a table of event results. The table has columns: Select, Flag, Entry, Type, Direction, Contact, Duration, Details, Mobile Time, and Server Time.

The table data is as follows:

Select	Flag	Entry	Type	Direction	Contact	Duration	Details	Mobile Time	Server Time
	40	Im	Outgoing	User <phoenix@email.com>			Details	2010-October-06 02:28:05	2010-October-13 06:11:05
	39	Im	Outgoing	User <phoenix@email.com>			Details	2010-October-06 02:28:05	2010-October-13 06:11:05
	38	Im	Incoming	Phoenix <phoenix@email.com>			Details	2010-October-06 02:28:05	2010-October-13 06:11:05
	37	Im	Outgoing	User <phoenix@email.com>			Details	2010-October-06 02:28:05	2010-October-13 06:11:05
	36	Im	Incoming	Phoenix <phoenix@email.com>			Details	2010-October-06 02:28:05	2010-October-13 06:11:05
	35	Im	Incoming	Phoenix <phoenix@email.com>			Details	2010-October-06 02:28:05	2010-October-13 06:11:05
	34	Im	Incoming	Phoenix <phoenix@email.com>			Details	2010-October-06 02:28:05	2010-October-13 06:11:05



Soluciones De Infección Y Monitoreo Remoto

FINFLY USB

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 los cuartel generales de la agencia.

DE UN VISTAZO

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

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**.

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.

Descripción General De Funciones

- 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, videos y documentos de Officeen el dispositivo.
- Infección **del sistema objetivo apagado al arrancar desde el USB**.
- 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

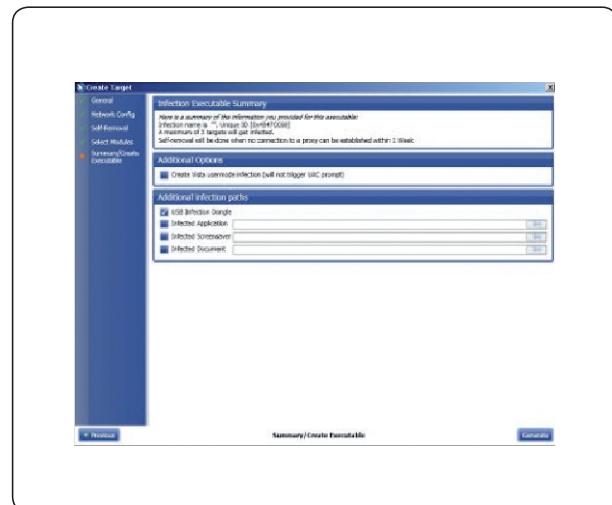


FINFISHER™
IT INTRUSION

Soluciones De Infección Y Monitoreo Remoto

FINFLY USB

Componentes Del Producto



FinFly USB

- Llave SanDisk 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

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 técnicos o editoriales que pueda contener este documento.



GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411

Fax: +44 - 1264 - 332 422

info@gammagroup.com

Soluciones De Infección Y Monitoreo Remoto

FINFLY LAN

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**.
- Disfraz 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



FINFISHER™
IT INTRUSION

Soluciones De Infección Y Monitoreo Remoto

FINFLY LAN

Componentes Del Producto



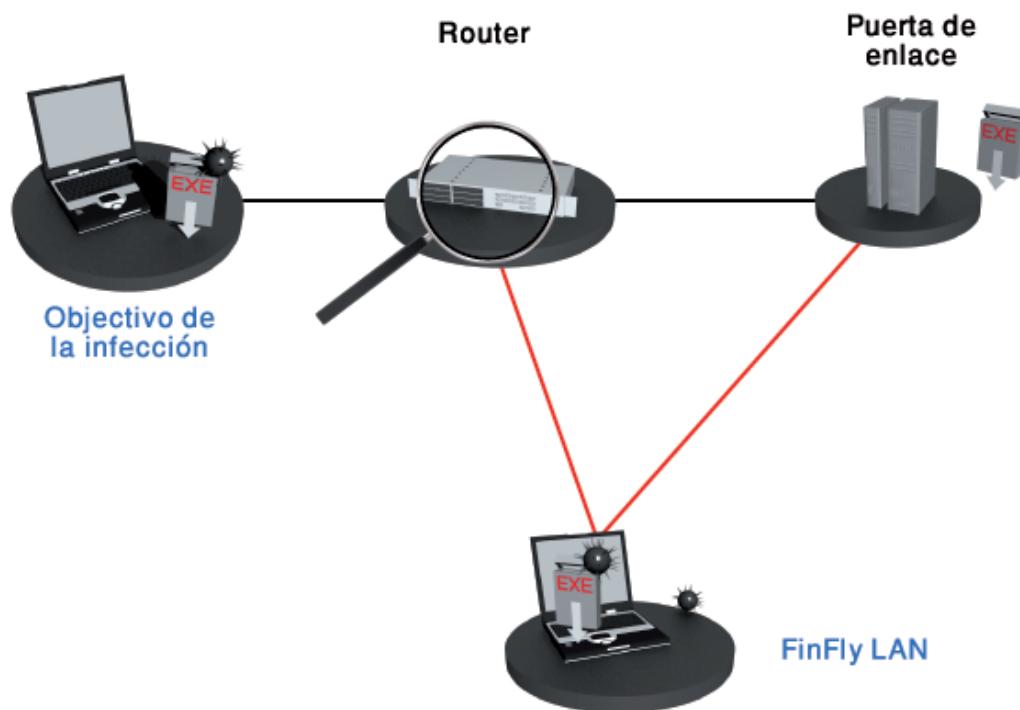
FinFly LAN

- 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)



Soluciones De Infección Y Monitoreo Remoto

FINFLY WEB

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 ha sido específicamente diseñado para permitir infectar un sistema objetivo **de manera remota y encubierta** utilizando gran variedad de **ataques basados en la web**.

FinFly Web proporciona una **interfaz interactiva** que permite que el agente **cree fácilmente un código de infección a medida** en función de los módulos seleccionados.

Los sistemas objetivo que visiten un sitio Web preparado con el código infeccioso implementado **se infectarán secretamente** con el software configurado.

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 Monitoreo remoto en el sistema objetivo, que pudo **monitorearse desde la sede central de la agencia**.

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 **FinFly ISP** en los sistemas del principal proveedor de servicios de Internet del país. Esto se combinó con **FinFly Web** para infectar de forma remota a los objetivos que visitaban sitios Web contrarios al Gobierno introduciendo secretamente el código de FinFly Web en los sitios web en cuestión.

Descripción General De Funciones

- **Módulos web totalmente personalizables.**
- Se pueden **instalar secretamente en cualquier sitio web**.
- Total integración con **FinFly LAN** y **FinFly ISP** para implementarse incluso en los sitios Web más populares, como proveedores de correo Web, portales de video, 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

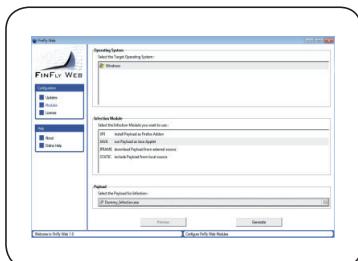


FINFISHER™
IT INTRUSION

Soluciones De Infección Y Monitoreo Remoto

FINFLY WEB

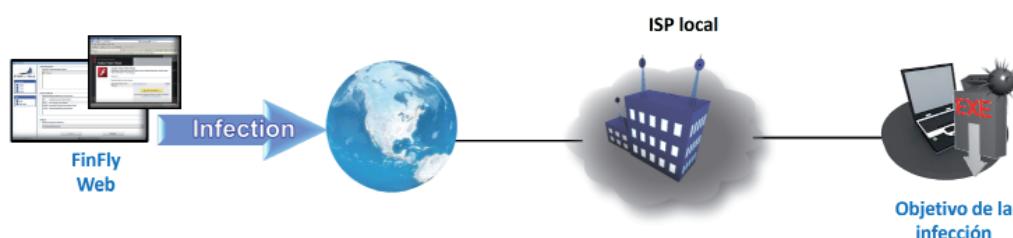
Componentes Del Producto



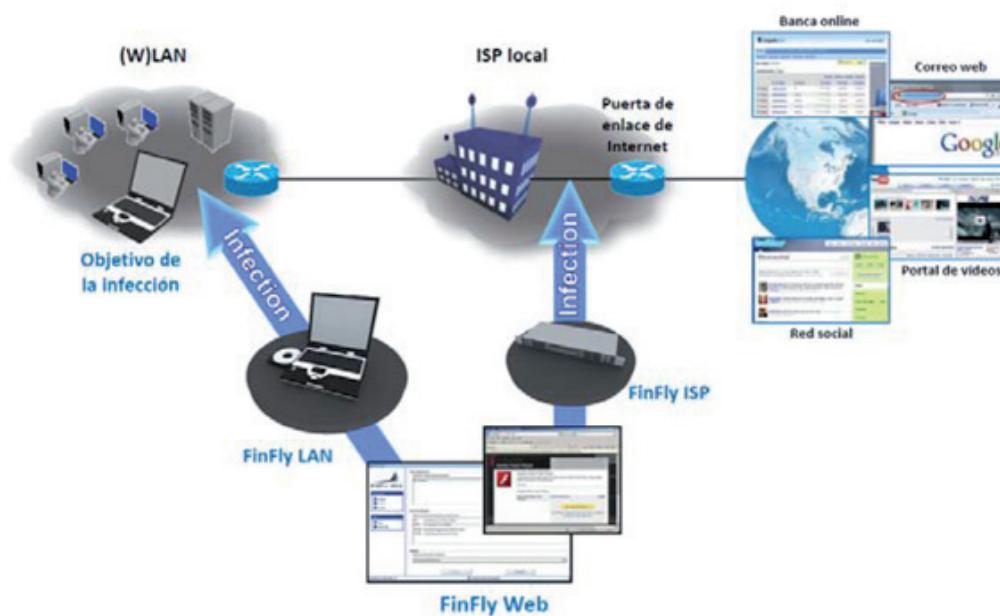
FinFly Web

- Software interactivo para crear sitios Web de infección a medida

Infección Directa Con FinFly Web



Total Integración Con FinFly LAN Y FinFly ISP



Soluciones De Infección Y Monitoreo Remoto

FINFLY WEB

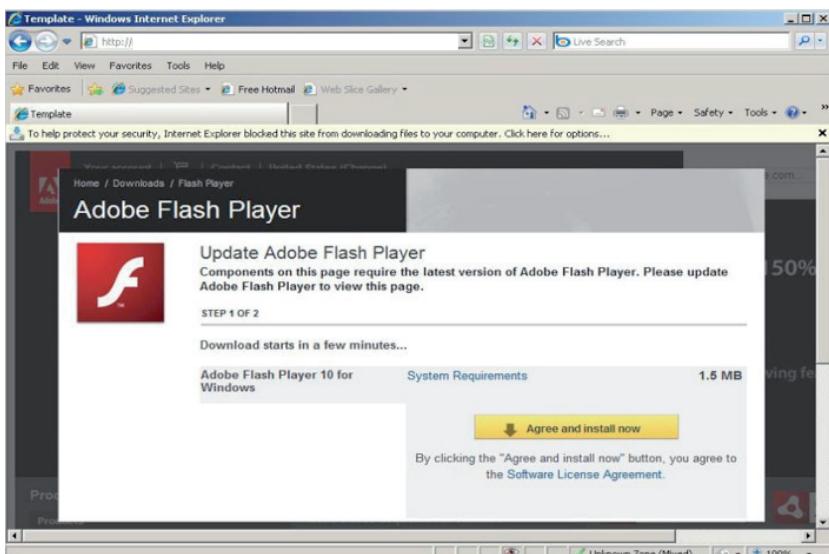
Ejemplo: Applet Java (Internet Explorer, Firefox, Opera, Safari)

El sitio web le pedirá al objetivo que acepte un complemento Java que puede ir firmado con el nombre de cualquier empresa fiable (p. ej. "Microsoft Corporation")



Ejemplo: Ausencia De Un Componente (Internet Explorer, Firefox, Opera, Safari)

El sitio web simulará que el sistema objetivo no dispone de un complemento o códec determinado, y le pedirá al usuario que lo descargue y lo instale.

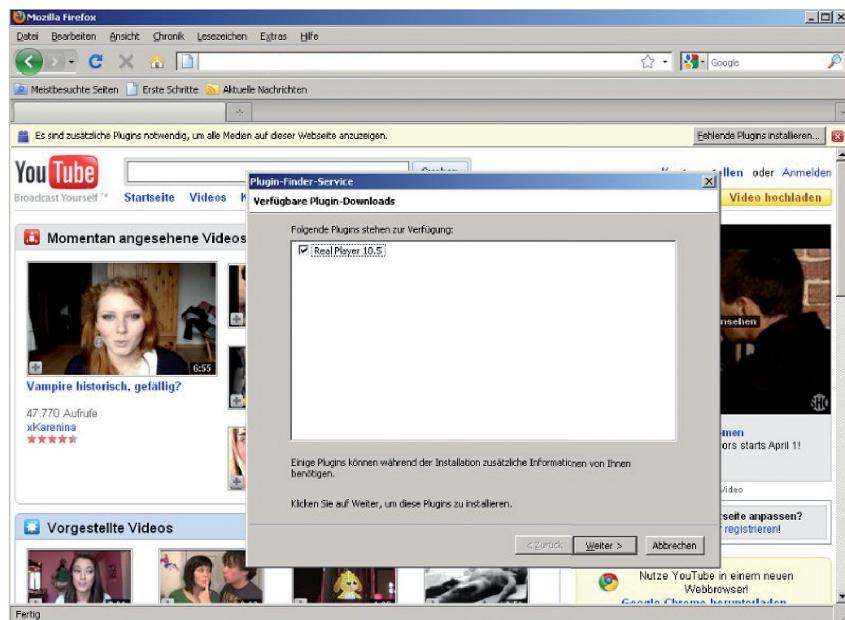


Soluciones De Infección Y Monitoreo Remota

FINFLY WEB

Ejemplo: Ausencia de un archivo XPI (sólo Firefox, todas las plataformas)

Este módulo le pedirá al objetivo que instale complementos adicionales para poder visualizar el sitio web



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 técnicos o editoriales que pueda contener este documento.



GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422
info@gammagroup.com

Soluciones De Infección Y Monitoreo Remoto

FINFLY ISP

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 monitoreo remoto para poder **monitorear el objetivo desde dentro de 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 monitoreo remoto 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 intercepción 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 infección.

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

FinFly ISP puede **infectar archivos** descargados por el objetivo **en tiempo real**, o infectar el sistema objetivo **enviando falsas actualizaciones** de aplicaciones de software populares. La nueva versión integra la potente aplicación de infección remota de Gamma **FinFly Web** para que los objetivos se infecten en tiempo real con solo **visitar cualquier sitio Web**.

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

Descripción General De Funciones

- Se puede instalar dentro de la **red de un proveedor de servicios de Internet**.
- Es compatible con **todos los protocolos más comunes**
- Selecciona e identifica los objetivos por **su dirección IP o el nombre de inicio de sesión de RADIUS**
- Oculta la solución de monitorización remota en las **descargas de los objetivos**.
- Disfrazla 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.



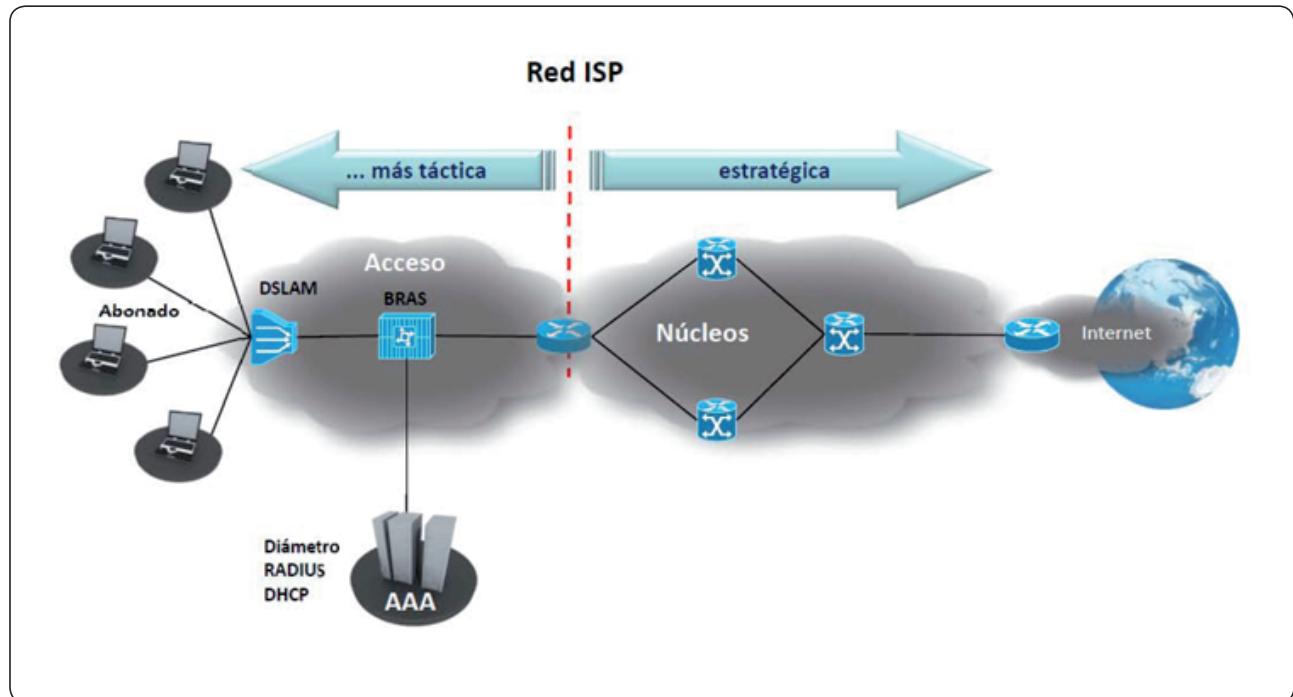
FINFISHER™
IT INTRUSION

Soluciones De Infección Y Monitoreo Remoto

FINFLY ISP

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 permite identificar e infectar de forma remota cualquier objetivo desde la sede central de la agencia gubernamental sin necesidad de que las fuerzas y cuerpos de seguridad se desplacen al lugar en cuestión.

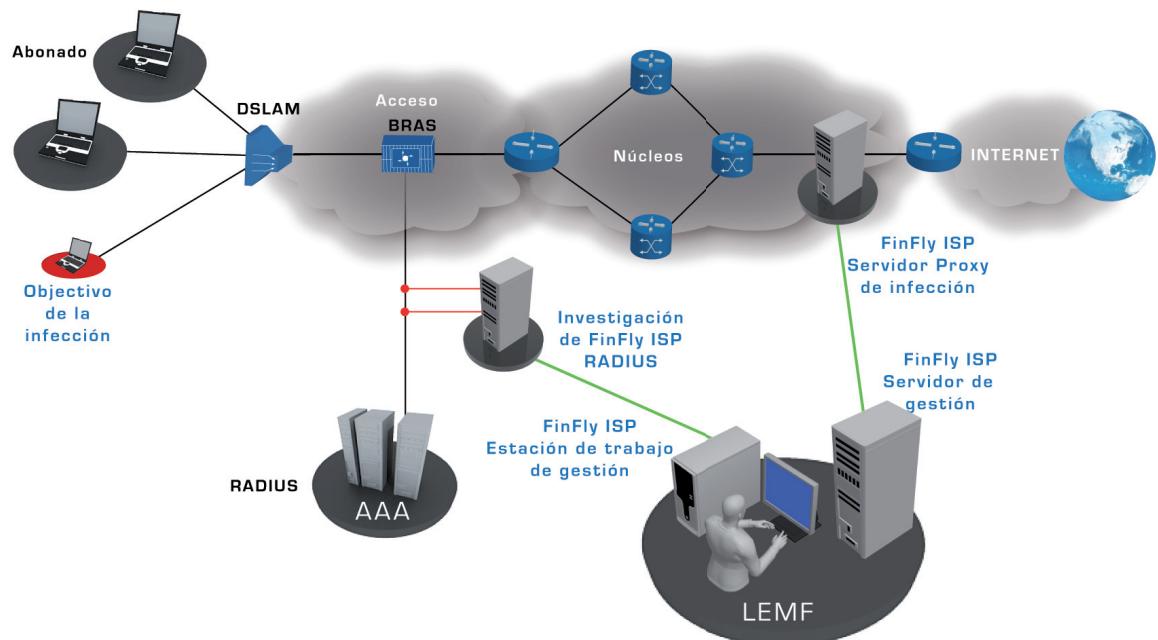
Evidentemente, es posible combinar soluciones tácticas y estratégicas para otorgar la máxima flexibilidad posible a las operaciones de infección.

Soluciones De Infección Y Monitoreo Remoto

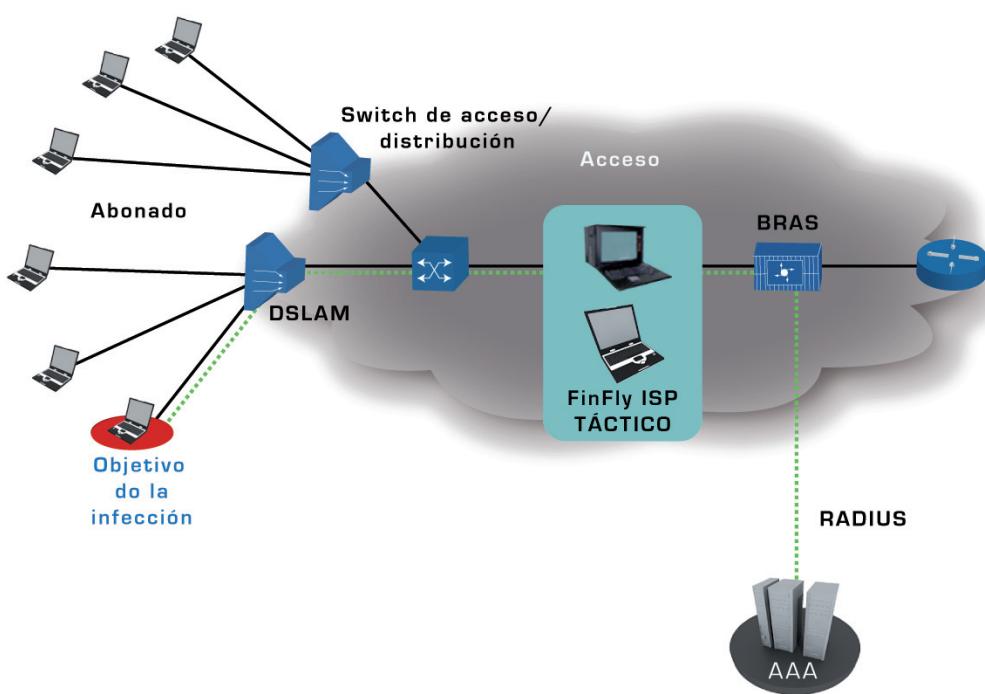
FINFLY ISP

Configuración de la red

Implementación estratégica



Implementación táctica



Soluciones De Infección Y Monitoreo Remoto

FINFLY ISP

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



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

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



Capacidad de proceso	5 Gbps
Nº máx. de NIC:	3 NIC
Interfaces:	1GE Cobre / Fibra SONET/SDH OC-3 / -12 STM-1 / -4 ATM AAL5
Procesadores:	2 Intel Core i7
Núcleos	6 núcleos / procesador
RAM:	12 GB
Capacidad de disco duro:	2 SATA de 1 TB
Unidad óptica	DVD+/-RW SATA
Monitor	1 TFT de 17"
Características	Función de conmutación de derivación para NIC
Sistema operativo	Linux GNU (Debian 5.0) reforzado

Los datos técnicos y las especificaciones están sujetos a cambios sin previo aviso.

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 técnicos o editoriales que pueda contener este documento.



GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411

Fax: +44 - 1264 - 332 422

info@gammagroup.com

Soluciones De Infección Y Monitoreo Remota

FIN SUPPORT

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
 - Sistema de solicitud de características
- 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 parcial

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 FinFisherTM y sustituciones de hardware en garantía. Además, con FinLifelineSupport, el cliente recibe automáticamente nuevas características y funciones con la versión estándar de los parches de corrección de errores.

Parches de corrección de errores

FinSupport es una organización de asistencia basada en el producto en la que un agente de asistencia postventa recibe consultas relacionadas por correo electrónico o por teléfono. El agente de asistencia postventa se encuentra en Alemania y su horario de trabajo es de 09:00 a 17:00 (CET).

Con FinLifelineSupport, dispondrá de asistencia de 09:00 a 17:00 (CET). Si se registra una solicitud de asistencia fuera del horario de trabajo estándar, esta será atendida el siguiente día laborable.

Cuando el cliente comunica un incidente, nosotros registramos un informe de incidente y documentamos la prioridad del mismo. Tras un periodo de tiempo determinado, se tomarán medidas correctivas según la prioridad asignada. El equipo de FinFisherTM es responsable de coordinar la investigación y la resolución del informe de incidente, así como de comunicar el estado y cualquier información nueva al autor de dicho informe.

Para cuestiones de alta prioridad, nos aseguramos de que el sistema siga funcionando correctamente proporcionando soluciones temporales y parches de corrección de errores probados. Cuando el equipo de FinFisherTM ofrece una solución temporal, también deriva la comunicación de problema al departamento de Investigación y desarrollo (I+D) para garantizar una resolución rápida. Estas medidas de asistencia profesional garantizan que el software responda a las más altas expectativas.

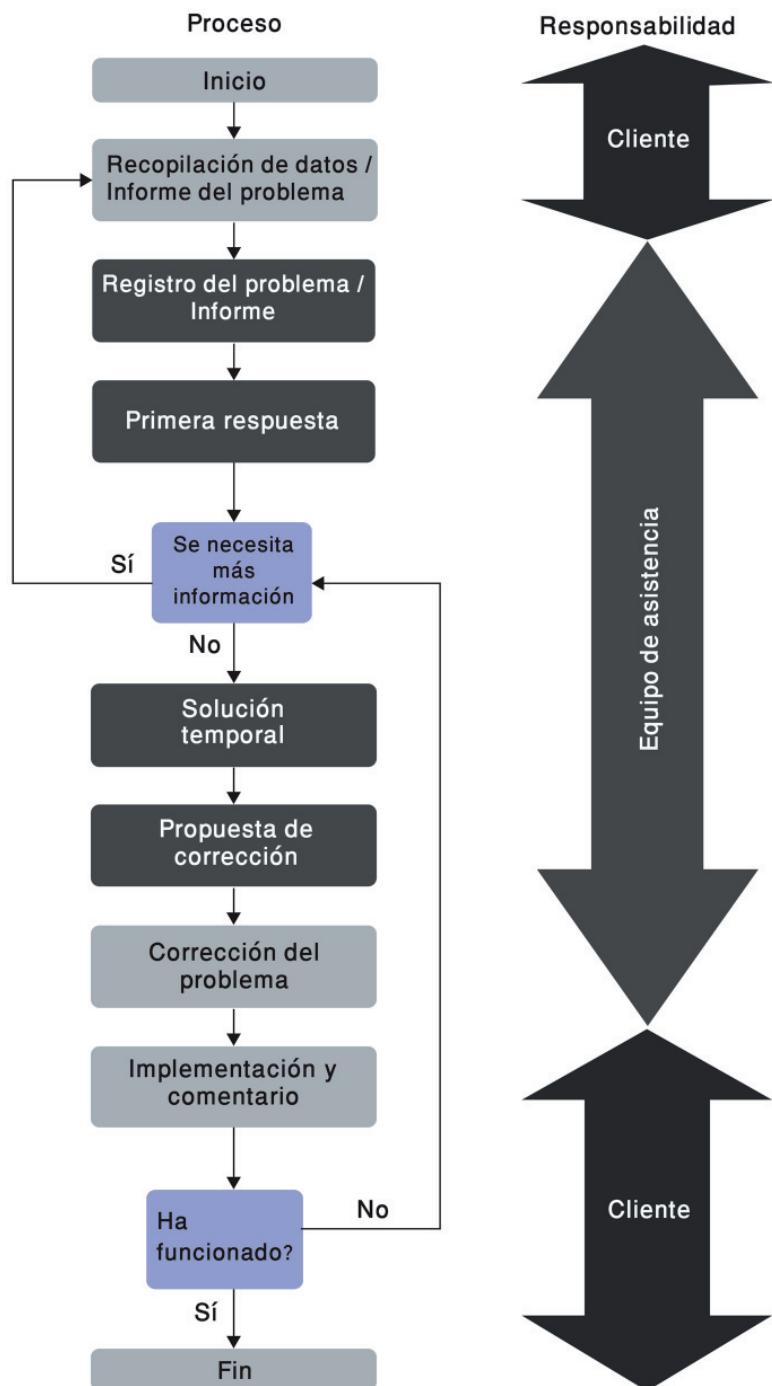


FINFISHER™
IT INTRUSION

Soluciones De Infección Y Monitoreo Remoto

FIN SUPPORT

El siguiente gráfico ofrece una visión del procedimiento operativo típico y las áreas de responsabilidad (Nota: En este gráfico, el 'cliente' representa al autor del informe del incidente):



Soluciones De Infección Y Monitoreo Remota

FIN SUPPORT

En la siguiente tabla se describe el procedimiento normal de gestión de incidentes del cliente:

Cliente	Procesamiento y tareas de informes de incidente
	FinFisher™ ofrece métodos de contacto exclusivos (correo electrónico, línea de teléfono/fax) para la comunicación de incidentes.
En el caso de un (posible) defecto de hardware/software, el cliente recibe un informe de incidente a través de los métodos de comunicación establecidos. El informe debe incluir: - identificador del contrato - nombre del cliente - tecnología/sistema afectado - descripción del defecto - prioridad (véase definición a continuación) - síntomas de error disponibles	
Si así se le solicita, el cliente colabora facilitando más síntomas de error.	En el plazo de un día laborable, el cliente recibe el número de ticket para poder confirmar la recepción y tener un seguimiento del informe de incidente, así como los resultados del análisis inicial.
	FinLifelineSupport admite la recopilación de síntomas de error si así se solicita.
	FinLifelineSupport ayuda con una solución temporal.
	Tras el análisis del incidente, FinLifelineSupport ofrece una propuesta de corrección para el informe de incidente con las medidas correctivas previstas y el tiempo de respuesta.
	Si el incidente comunicado requiere corrección, FinLifelineSupport ofrece una modificación de hardware o software.
El cliente implementa la modificación de hardware/ software proporcionada. El cliente confirma que el problema se ha corregido.	FinLifelineSupport ayuda implementando una modificación de hardware ⁽ⁱ⁾ / software.

(i) El arreglo del hardware se cobrará por separado si este no está en garantía.



Soluciones De Infección Y Monitoreo Remoto

FIN SUPPORT

Definición de la prioridad de las consultas y errores

FinLifelineSupport procesa todas las consultas e informes de problemas que recibe de acuerdo con su urgencia. Hay dos factores que miden la urgencia de un incidente y ambos se incluyen en el informe de incidente:

- 'Prioridad', que se basa únicamente en el alcance técnico del error
- 'Gravedad de cliente', que es un factor más objetivo y se basa en el impacto que tiene en el cliente

En la siguiente tabla de 'Prioridad', se ofrece una visión general del correspondiente alcance técnico:

Prioridad	Definición	Ejemplo
1	problema crítico: no funciona un aspecto fundamental del sistema	El Proxy está caído y no se puede establecer la comunicación con FinSpy Target.
2	problema importante sin solución temporal	Una actualización de antivirus detecta un RMS ya instalado que requiere una actualización inmediata para permanecer operativo en el sistema infectado.
3	problema importante con solución temporal	La función FinSpy Target no funciona correctamente, pero se puede arreglar con una solución temporal.
4	problema no crítico sin grandes consecuencias en el sistema	Aparece un ícono equivocado para un archivo descargado

Tiempos de respuesta

En el 90% de los incidentes, nuestros tiempos de respuesta son los que se indican en la siguiente tabla.

'Día(s) laborable(s)' = según el calendario alemán, por lo que se deben excluir los días festivos en Alemania.

En nuestros tiempos de respuesta existen tres fases:

- Respuesta inicial
- Respuesta con acción correctiva
- Resolución del problema (o disminución de la prioridad)

El tiempo de la 'Respuesta inicial' va desde el momento en que registramos un incidente hasta que el cliente recibe la respuesta confirmándole la recepción del incidente.

La 'Respuesta inicial' también puede solicitar información más detallada o, en los casos menos complejos, puede resolver el problema inmediatamente.

Soluciones De Infección Y Monitoreo Remota

FIN SUPPORT

Tiempos de respuesta	Respuesta inicial	Respuesta con acción correctiva	Resolución del PROBLEMA / Disminución de la PRIORIDAD
Prio 1 - problema crítico	En el mismo día laborable	1 díalaborable	2 días laborables Nota: Dependiendo del problema y la investigación necesaria, se puede tardar más en resolver el problema.
Prio 2 - problema importante sin solución temporal	En el mismo día laborable	2 días laborables	5 días laborables Nota: Dependiendo del problema y la investigación necesaria, se puede tardar más en resolver el problema.
Prio 3 - problema importante con solución temporal	En el mismo día laborable	3 días laborables	14 días laborables Nota: Dependiendo del problema y la investigación necesaria, se puede tardar más en resolver el problema.
Prio 4 - problema no critico	En el mismo día laborable	7 díaslaborables	en la próxima actualización de 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).



Programa De Capacitación En Sistemas De Intrusión De TI

FINTRAINING



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.



FINFISHER™
IT INTRUSION

Programa De Capacitación En Sistemas De Intrusión De TI

FINTRAINING

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 intercepción activa y la obtención de inteligencia a través de la **intrusión de TI** tienen cada vez más importancia en el día a día de los gobiernos, y exigen la **configuración de equipos de intrusión 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**.

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

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. Y con el fin de garantizar la utilidad de los conocimientos transmitidos, se ofrece **soporte operativo en el país del cliente** en el marco del programa.

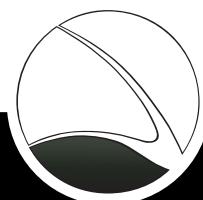
Ejemplos de los temas del curso

- **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**

Programa de asesoría

- Programa completo de **consultoría y formación** en intrusión de TI
- **Formación y configuración estructurada de equipos especializados en intrusiones de TI**
- **Evaluación completa de los miembros del equipo**
- Sesiones de formación práctica centradas en operaciones reales
- **Consultoría operativa** en el país del cliente

Encontrará la lista completa de funciones en las Especificaciones del producto



FINFISHER™
IT INTRUSION



GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

WWW.GAMMAGROUP.COM