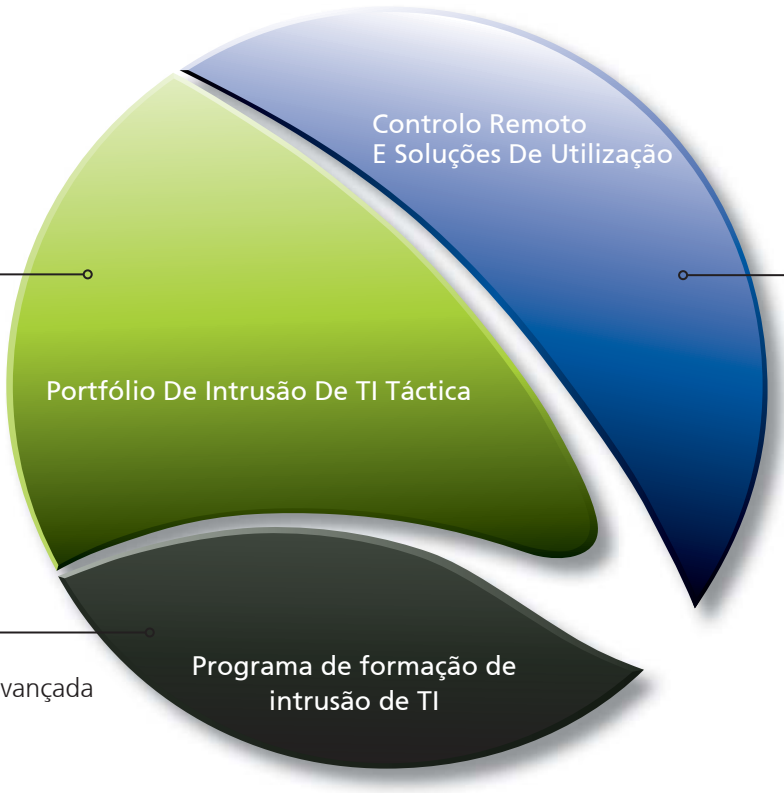
# FINFISHER™ : SOLUÇÕES DE CONTROLO REMOTO E INTRUSÃO DE TI GOVERNAMENTAL

WWW.FINFISHER.COM

FINFISHER™
IT INTRUSION




- FinIntrusion Kit
- FinUSB Suite
- FinFirewire

FinSpy
- FinSpy
- FinSpy Mobile

FinFly
- FinFly USB
- FinFly LAN
- FinFly Web
- FinFly Exploit Portal
- FinFly ISP
- FinFly NET

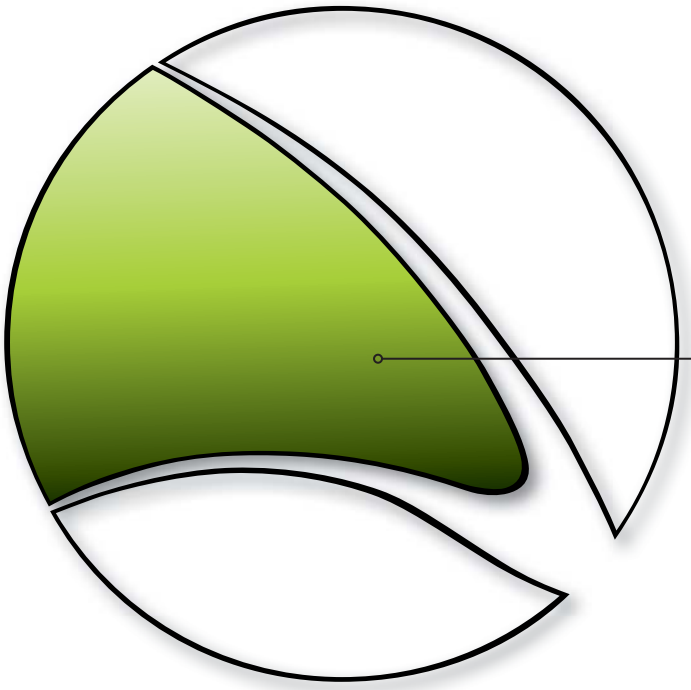
- Intrusão básica e avançada
- Intrusão sem fios
- Exploração prática
- Penetração de aplicação de Web
- Formação e consultoria personalizada de intrusão de TI

Portfólio De Intrusão De TI Táctica

# **FIN**INTRUSION KIT

# **FIN**USB SUITE

# **FIN**FIREWIRE



A Gamma desenvolve esforços permanentes no campo da intrusão de TI com soluções para melhorar as capacidades dos nossos clientes. As técnicas e soluções mais recentes fáceis de utilizar, complementam os conhecimentos da comunidade de serviços secretos, permitindo-lhe enfrentar os desafios de intrusão relevantes ao nível táctico.

FINFISHER™
IT INTRUSION

WWW.FINFISHER.COM

# FINKIT DE INTRUSÃO

O Kit FinIntrusion foi concebido e desenvolvido pelos especialistas de classe mundial de intrusão de TI, com mais de 10 anos de experiência nesta área pelo trabalho em várias Tiger Teams (Red Teams) no sector público e privado, avaliando a segurança das diferentes redes e organizações.

O Kit FinIntrusion é um kit operacional de **actualização e dissimulação** que pode ser utilizado para as **Operações de intrusão de TI** mais comuns nas áreas defensiva e ofensiva. Os clientes actuais incluem **Departamentos militares de ciber-guerra, Agências de serviços secretos, Serviços secretos da polícia e outras Agências policiais.**

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operações estratégicas/tácticas** |
| **Capacidades:** | · **Descodifica WEP/WPA**<br>· **Controlo de rede (incluindo sessões SSL)**<br>· **Ataques de intrusão de TI** |
| **Conteúdo:** | · **Hardware/Software** |

**Exemplo 1 de utilização: Unidade de vigilância técnica**

O Kit FinIntrusion foi utilizado para quebrar **a encriptação WPA** de uma rede sem fios doméstica do Alvo e, em seguida, para controlar o seu **Webmail (Gmail, Yahoo, ...) e as credenciais de Rede social (Facebook, MySpace,...)**, o que permitiu que os investigadores **controlassem remotamente** estas contas a partir das sedes sem necessidade de estarem perto do Alvo.

**Exemplo 2 de utilização: Segurança de TI**

Vários clientes utilizaram o kit FinIntrusion para ignorarem com **êxito a segurança** de redes e sistemas informáticos para objectivos de **ataque e defesa,** utilizando várias ferramentas e técnicas.

**Exemplo 3 de utilização: Casos de utilização de estratégicas**

O kit FinIntrusion é largamente utilizado tendo em vista o acesso remoto às contas de e-mail do alvo e servidores de web do alvo e o controlo das suas actividades, incluindo registos de acesso e muito mais.

**Resumo das funcionalidades**

- Detecta **LANs sem fios (802.11) e dispositivos Bluetooth®**
- Recupera palavras-passe WEP (64 e 128 bits) **no prazo de 2 a 5 minutos**
- **Quebra palavras-passe WPA1 e WPA2**, utilizando ataques do dicionário
- Controla activamente LAN (com e sem fios) e **extrai Nomes de utilizador e Palavras-passe mesmo de sessões encriptadas TLS/SSL**
- Quebra remotamente **Contas de e-mail**, utilizando técnicas de intrusão baseadas em rede, sistema e palavra-passe
- **Avaliação de segurança de rede** e validação

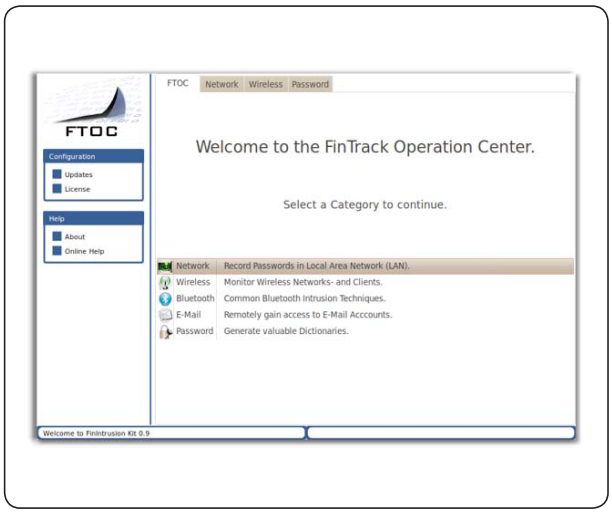
Para obter uma lista completa de funcionalidades, consulte as especificações do produto.

# FINKIT DE INTRUSÃO

## Componentes do produto

**Kit FinIntrusion – Unidade táctica dissimulada**

Componentes básicos de intrusão de TI:
- Adaptador de WLAN de alta potência
- Adaptador de Bluetooth de alta potência
- Antenas 802.11
- Dispositivos de Intrusão de TI mais comuns

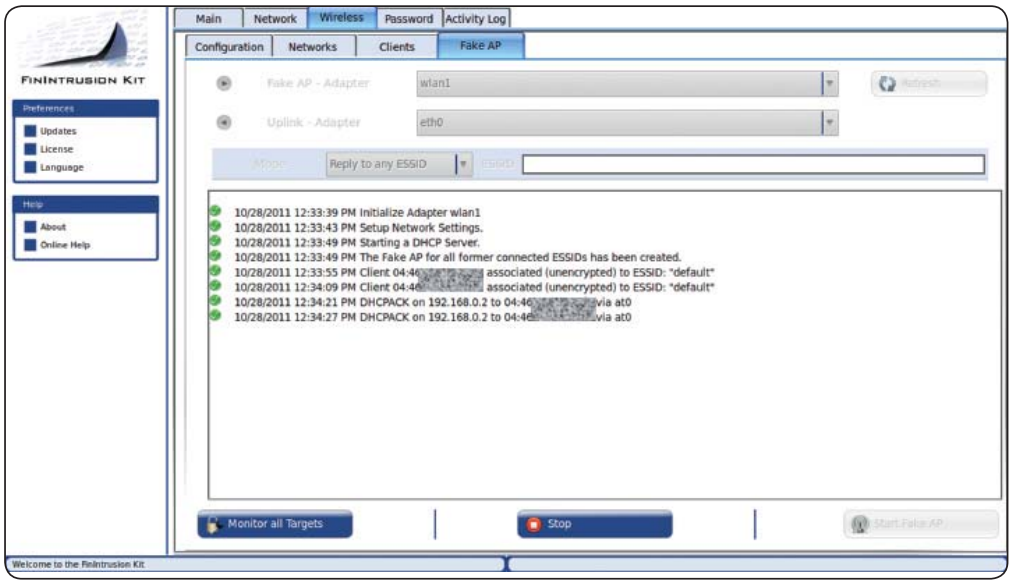



**Centro de operações de FinTrack**

- Interface gráfica de utilizador para ataques automatizados de intrusão de TI

## Catcher Wi-Fi

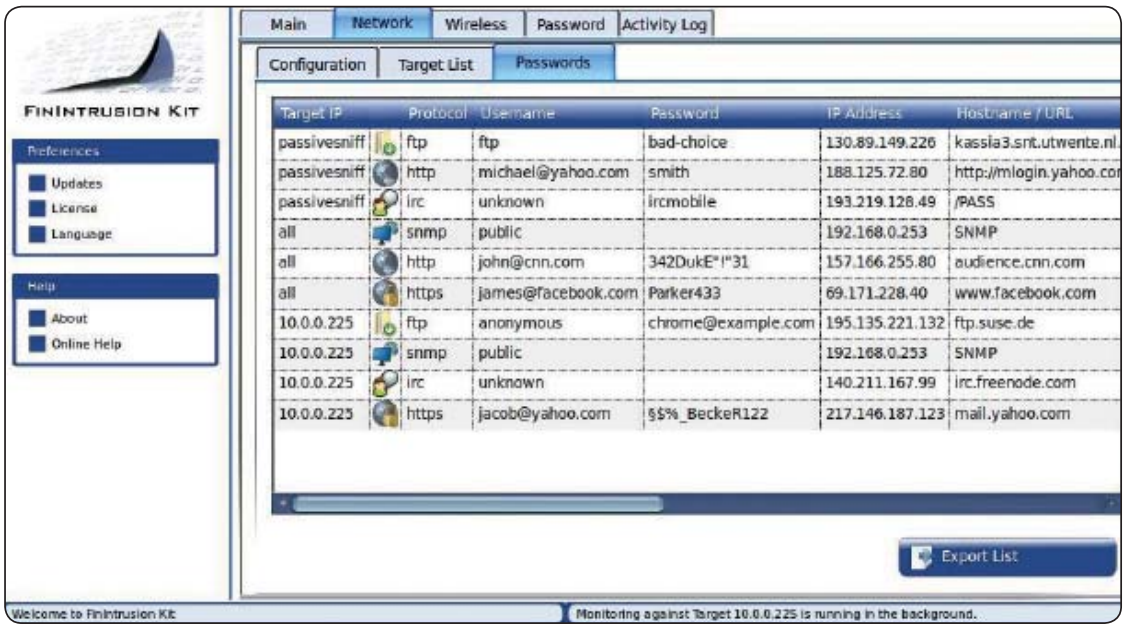
- Acesso junto de dispositivos WLAN e grava tráfego e palavras-passe.



# **FIN**KIT DE INTRUSÃO

## Farejador de palavras-passe activo de LAN/WLAN

· Captura mesmo os dados encriptados SSL como Webmail, Portais de vídeo, Banca on-line, e muito mais








GAMMAGROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# FINUSB SUITE

O FinUSB Suite é um produto flexível que permite que as forças policiais e agências de serviços secretos extraiam, de forma rápida e segura, informações forenses dos sistemas informáticos sem o requisito de agentes formados de TI.

Ele foi utilizado com êxito em operações em todo o mundo, onde os serviços secretos valiosos foram encontrados em alvos, em operações dissimuladas e abertas.

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operações tácticas** |
| **Capacidades:** | · **Obtenção de informações**<br>· **Acesso do sistema**<br>· **Forense rápida** |
| **Conteúdo:** | · **Hardware/Software** |

### Exemplo 1 de utilização: Operação dissimulada

Uma fonte num Grupo de crime organizado (GCO) recebeu um dongle FinUSB que extraiu secretamente credenciais de conta de contas de Web e E-mail e documentos do Microsoft Office a partir dos sistemas alvo, enquanto o GCO utilizou o dispositivo USB para **trocar ficheiros regulares** como música, vídeo e documentos do Office.

Depois de devolver o dispositivo USB à sede, os dados recolhidos puderam ser descodificados, analisados e utilizados para controlar o grupo, de forma constante e remota.

### Exemplo 2 de utilização: Unidade de vigilância técnica

Uma unidade de vigilância técnica (UVT) estava a seguir um alvo que visitava com frequência e de forma aleatória cafés de Internet, o que tornou impossível o controlo com tecnologia do tipo cavalo de tróia. O FinUSB foi utilizado para extrair os **dados deixados nos terminais públicos** utilizados pelo alvo depois de ter saído.

Vários documentos que o alvo abriu no seu correio da Web puderam ser recuperados deste forma. As informações recolhidas incluíam ficheiros cruciais do Office, histórico de navegação através da análise cookie, e muito mais.

### Visão geral da funcionalidade

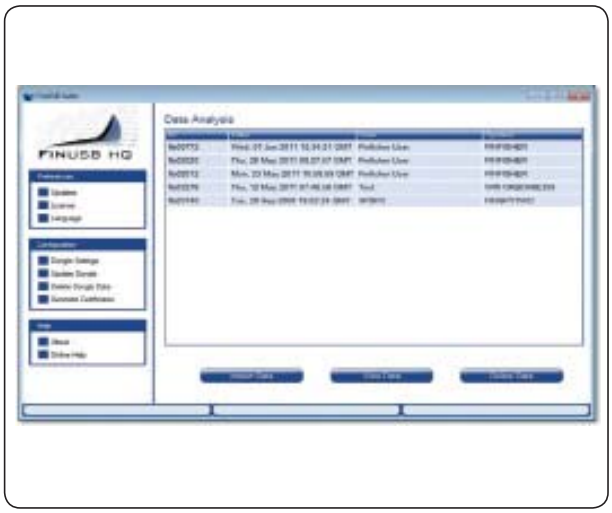
- Optimizado para **Operações dissimuladas**
- Usabilidade fácil através da **execução automatizada**
- Extracção dos **Nomes de utilizador e palavras-passe** para todo o software comum, como:
  - Clientes de e-mail
  - Mensageiros
  - Navegadores
  - Ferramentas de administração remota
- **Cópia silenciosa de ficheiros** (pesquisa de disco, caixote do lixo, última abertura/edição/criação)
- Extracção **das Informações da rede** (Registos de chat, histórico de navegação, chaves de WEP/WPA(2), ...)
- Compilação das **Informações do sistema** (Execução/software instalado, informações do disco rígido, …)

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

# **FIN**USB SUITE

## Componentes do produto

**FinUSB Suite - Unidade móvel**




**FinUSB HQ**

- Interface gráfica de utilizador para descodificar e analisar os dados recolhidos
- Configurar opções operacionais do dongle

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

- Extrai dissimuladamente os dados do sistema

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

- Ignorar início de sessão do Windows sem modificações permanentes do sistema

# FINUSB SUITE

## Utilização fácil

1. Obtenha um dongle FinUSB

2. Configure todos os Módulos/Funcionalidades e actualize o dongle FinUSB com FinUSB HQ

3. Aceda ao sistema alvo

4. Ligue o dongle FinUSB

5. Aguarde que todos os dados sejam transferidos

6. Regresse ao FinUSB HQ

7. Importe todos os dados do dongle FinUSB

8. Gerar relatório

## Relatórios profissionais






GAMMAGROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# FINFIREWIRE

As unidades de vigilância técnica e os especialistas forenses enfrentam, frequentemente, uma situação e que necessitam de aceder a um sistema em execução, sem o desligar, para evitar perda de dados ou economizar tempo essencial durante uma operação. Na maioria dos casos, o sistema alvo está protegido com uma **Protecção de ecrã com palavra-passe** ou o utilizador alvo não iniciou sessão e o **Ecrã de acesso** está activo.

O FinFireWire permite que o Operador **ignore o ecrã protegido por palavra-passe,** de forma rápida e dissimulada, e que aceda ao sistema alvo sem deixar rasto e sem danificar e evidência forense essencial.

**INFORMAÇÕES RÁPIDAS**

| | |
|---|---|
| **Utilização:** | · **Operaciones tácticas** |
| **Capacidades:** | · **Ignora palavra-passe do utilizador**<br>· **Acede dissimuladamente ao sistema**<br>· **Recupera palavras-passe a partir da RAM**<br>· **Permite dados forenses directos** |
| **Conteúdo:** | · **Hardware/Software** |

**Exemplo 1 de utilização: Operação forense**

Uma **Unidade forense** entrou no apartamento de um alvo e tentou aceder ao sistema informático. O computador estava **ligado mas o ecrã bloqueado**.
Como não era permitido, por razões legais, utilizar uma solução de controlo remoto, eles teriam **perdido todos os dados** se desligassem o sistema, pois o **disco rígido estava totalmente encriptado**. O FinFireWire foi utilizado para **desbloquear o sistema alvo em execução** permitindo que o Agente **copie todos os ficheiros** antes de desligar o computador e levá-lo para a sede.

**Exemplo 2 de utilização: Recuperação da palavra-passe**

ombinando o produto com as **aplicações forenses tradicionais** como Encase®, as unidades forenses utilizaram a **funcionalidade de cópia da RAM** para efectuar um instantâneo das informações actuais da RAM e **recuperaram a palavra-passe de encriptação do disco rígido** para encriptação de disco completo TrueCrypt.

**Visão geral da funcionalidade**

- **Desbloqueia o início de sessão do utilizador** para todas as contas de utilizador
- Desbloqueia **a protecção de ecrã com palavra-passe**
- **Copia a RAM completa** para análise Forense
- Permite actividades forenses directas **sem reinicializar** o sistema alvo
- A palavra-passe de utilizador **não é alterada**
- Suporta **Windows, Mac OSX** e **Linux**
- Funciona com **FireWire/1394, PCMCIA e Express Card**

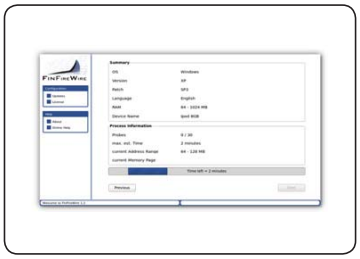
**Para obter uma lista completa de funcionalidades, consulte as especificações do produto.**

# **FIN**FIREWIRE

## Componentes do produto

**FinFireWire - Unidad táctica**

· Sistema táctico completo



**Interface de utilizador apontar-e-clicar**

· Interface de utilizador fácil de utilizar

**Placas de adaptador de ligação**

· Adaptador de PCMCIA e Express-Card para os sistemas alvo sem porta FireWire

**Conjunto de cabos FinWire universal**

· 4 pinos para 4 pinos
· 4 pinos para 6 pinos
· 6 pinos para 6 pinos

## Utilização

**1. Aceda ao sistema alvo**

**2. Inicie o FinFireWire**

**3. Ligue o adaptador e o cabo FireWire**

**4. Seleccione um alvo**

**5. Aguarde até o sistema estar desbloqueado**





GAMMAGROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

**FIN**SPY

**FIN**SPY MOBILE

**FIN**FLY USB

**FIN**FLY LAN

**FIN**FLY WEB

**FIN**FLY EXPLOIT PORTAL

**FIN**FLY ISP

**FIN**FLY NET

O controlo remoto e as soluções de infecção são utilizados para aceder aos sistemas alvo, proporcionando o acesso total às informações armazenadas, com a possibilidade de assumir o controlo das funções dos sistemas alvo para capturar comunicações e dados encriptados. Quando utilizado juntamente com os métodos aperfeiçoados de infecção remota, as agências governamentais terão a capacidade de infectar remotamente os sistemas alvo.

# FINSPY

O FinSpy é uma solução de controlo remoto provada de campo que permite que os governantes enfrentem os desafios actuais do **controlo móvel e dos alvos alertados para a segurançaque** regularmente **mudam de local**, usam canais **de comunicações encriptados e anónimos e residem em países estrangeiros.**

As soluções tradicionais de intercepção legal **enfrentam novos desafios** que só podem ser **resolvidos utilizando sistemas activos** como o FinSpy:

- Dados não transmitidos através de qualquer rede
- Comunicações encriptadas
- Alvos em países estrangeiros

O FinSpy tem tido um **êxito provado** em operações em todo o mundo **durante muitos anos**, e as informações secretas valiosas foram obtidas sobre indivíduos e organizações alvo.

Quando o FinSpy está instalado num computador, pode ser **controlado e acedido remotamente** desde que esteja ligado à Internet/rede, **independentemente do lugar do mundo** e, que o sistema alvo se encontrar.

**Visão geral da funcionalidade**

Computador alvo – Exemplo de funcionalidades:

- Ignorar 40 dos sistemas de anti-vírus regularmente testados
- **Comunicações dissimuladas** com a sede
- **Controlo de Skype** total (Chamadas, Chats, Transferências de ficheiros, Vídeo, Lista de contactos)
- Gravação de **comunicações comuns**, como E-mail, Chats e Voice-over-IP
- **Vigilância directa** através de webcam e microfone
- **Rastreio do país** do alvo
- **Extracção silenciosa de ficheiros** da unidade de disco rígido
- **Registador de chaves baseado no processo** para uma análise mais rápida
- **Dados forenses remotos directos** no sistema alvo
- **Filtros avançados** para registar apenas as informações importantes
- Suporta os sistemas operativos mais comuns: **Windows, Mac OSX** e **Linux**

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operaciones estratégicas/tácticas** |
| **Capacidades:** | · **Controlo remoto do computador**<br>· **Controlo das comunicações encriptadas** |
| **Conteúdo:** | · **Hardware/Software** |

**Exemplo 1 de utilização: Agência de serviços secretos**

O FinSpy foi instalado em vários sistemas existentes em **cyber-cafés em áreas críticas** para os controlar relativamente a actividade suspeita, especialmente as **comunicações de Skype** para pessoas estrangeiras. Utilizando a Webcam, foram tiradas fotografias dos alvos enquanto estavam a utilizar o sistema.

**Exemplo 2 de utilização: Crime organizado**

O FinSpy foi **colocado dissimuladamente nos Sistemas alvo** de vários membros de um Grupo de crime organizado. Utilizando o **controlo de país e o acesso de microfone remoto**, as informações essenciais puderam ser obtidas a partir de **todas as reuniões levadas a cabo** por este grupo.

Ejemplos de funciones en la sede central:

- Protecção de evidência (Evidência válida de acordo com os **Padrões europeus**)
- **Gestão do utilizador** de acordo com as autorizações de segurança
- Oculto do público através de **Proxies anónimos**
- Pode ser **totalmente integrado** com a funcionalidade de controlo das forças policiais

**Para obter uma lista completa de funcionalidades, consulte as especificações do produto.**

## Componentes do produto

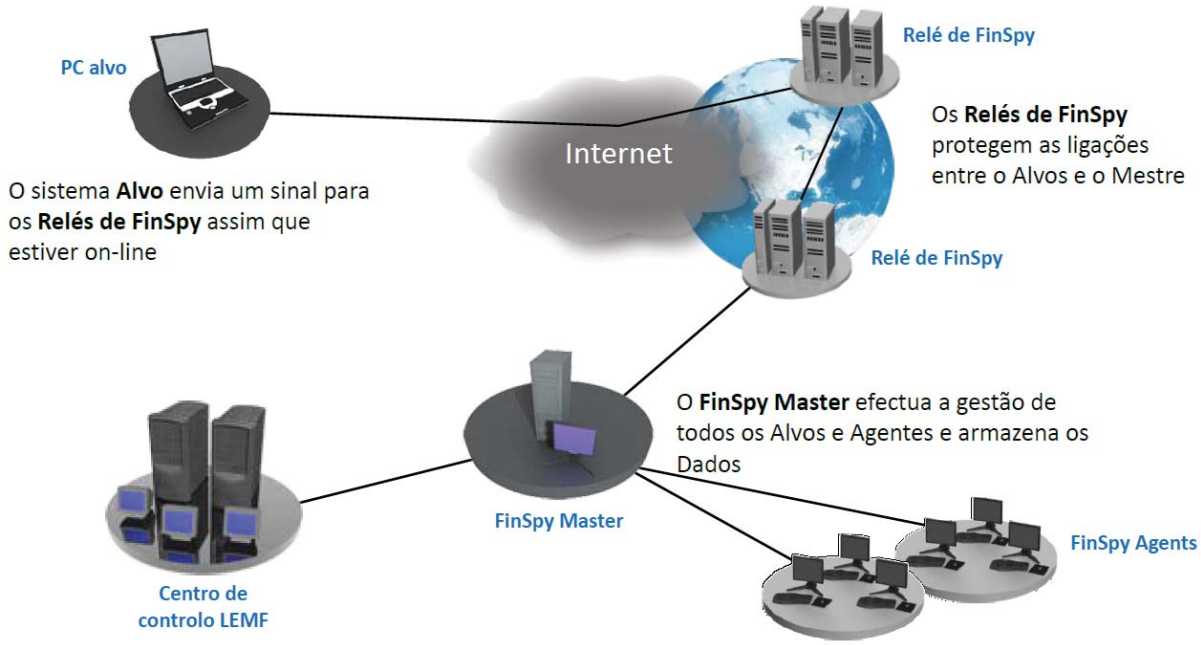
**FinSpy Master e Proxy**

- Controlo total dos sistemas alvo
- Protecção de evidência para registos de actividade e dados
- Armazenamento seguro
- Autorização de segurança com base na gestão de utilizadores e alvos

**FinSpy Agent**

- Interface gráfica de utilizador para sessões directas
- Configuração e análise de dados dos alvos

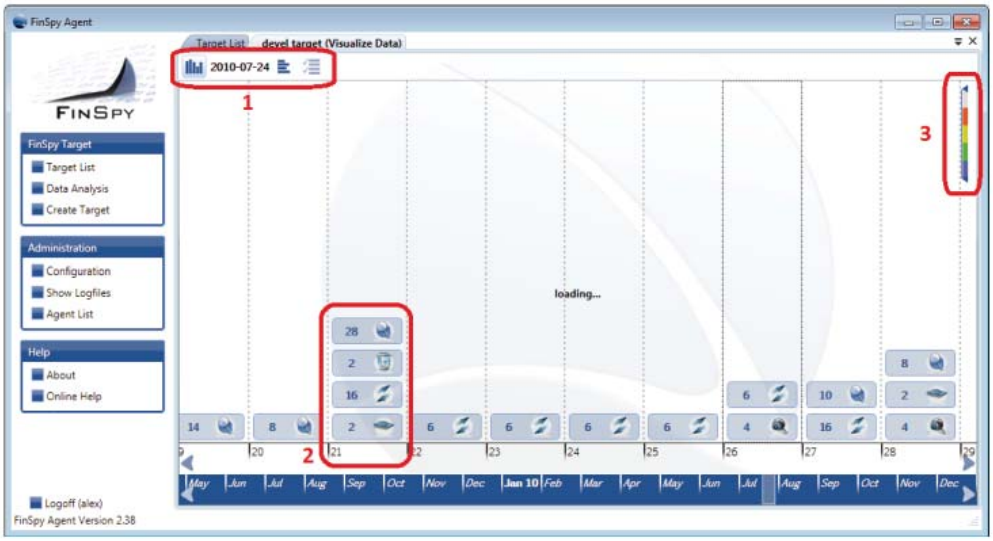
## Acesso aos sistemas informáticos alvo em todo o mundo




## Interface de utilizador fácil de utilizar

## Configuração do alvo directa e off-line


## Inteligência total no sistema alvo




1. Visualizações múltiplas dos dados
2. Análise dos dados estruturados
3. Níveis de importância de todos os ficheiros gravados





GAMMAGROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# FINSPY MOBILE

O FinSpy Mobile está a preencher a brecha das capacidades de intercepção dos Governos para as **plataformas de telefones inteligentes** mais comuns.

Especificamente, as organizações **sem capacidades de intercepção de rede ou não baseadas em ar** podem aceder aos telemóveis e interceptarem os dispositivos com capacidades avançadas. Além disso, a solução oferece **acesso a comunicações encriptadas**, bem como a dados **armazenados no dispositivo** que não está transmitido.

As soluções tradicionais tácticas ou estratégicas **enfrentam desafios** que só podem ser **resolvidos utilizando sistemas ofensivos** como o FinSpy Mobile:

- Dados não transmitidos através de qualquer rede e mantidos no dispositivo
- Comunicações encriptadas no Air-Interface, o que evita a utilização de sistemas aéreos passivos ou activos tácticos
- Encriptação terminal-para-terminal a partir do dispositivo como Messengers, E-mails ou mensagens PIN

O FinSpy Mobile tem proporcionado resultados com êxito às Agências governamentais que recolhem informações **remotamente a partir de telemóveis alvo**.

Quando o FinSpy Mobile é instalado num telemóvel pode ser **controlado e monitorizado remotamente**, independente da parte do mundo onde o alvo estiver localizado.

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operações estratégicas/tácticas** |
| **Capacidades:** | · **Controlo remoto do telemóvel** |
| **Conteúdo:** | · **Hardware/Software** |

**Exemplo 1 de utilização: Agência de serviços secretos**

O FinSpy Mobile foi colocado em **telemóveis BlackBerry** de vários alvos para monitorizar todas as comunicações, incluindo SMS/MMS, E-mail e BlackBerry Messenger.

**Exemplo 2 de utilização: Crime organizado**

O FinSpy Mobile foi **colocado dissimuladamente em telemóveis** de vários membros de um Grupo de crime organizado (GCO). Utilizando os dados de **controlo de GPS e chamadas silenciosas**, as informações essenciais podem ser obtidas a partir de **todas as reuniões efectuadas** por este grupo.

**Visão geral da funcionalidade**

Telefone alvo – Exemplo de funcionalidades:

- **Comunicações dissimuladas** com a sede
- Gravação de **comunicações comuns**, como Chamadas de voz, SMS/MMS e E-mails
- **Vigilância directa** através de chamadas silenciosas
- **Descarregamento de ficheiros** (Contactos, Calendário, Imagens, Ficheiros)
- Controlo de país do alvo (ID de GPS e célula)
- Gravação total de todas as **comunicações do BlackBerry Messenger**
- Suporta os sistemas operativos mais comuns: **Windows Mobile, iOS (iPhone), BlackBerry OS, Android e Symbian**

Sede – Funcionalidades de exemplo:

- Protecção de evidência (Evidência válida de acordo com os **Padrões europeus**)
- **Gestão do utilizador** de acordo com as autorizações de segurança
- Oculto do público através de **Proxies anónimos**
- Pode ser **totalmente integrado** com a funcionalidade de controlo das forças policiais

**Para obter uma lista completa de funcionalidades, consulte as especificações do produto.**

# FINSPY MOBILE

## Componentes do produto

**FinSpy Master e Proxy**

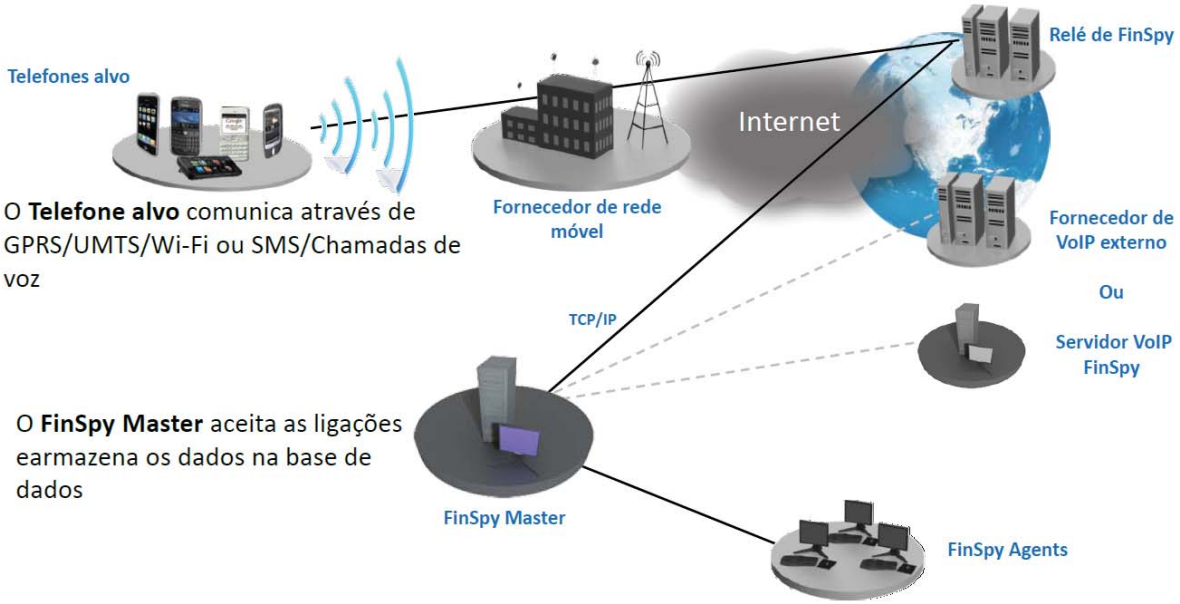
- Controlo total dos telefones alvo
- Protecção de evidência para registos de actividade e dados
- Armazenamento seguro
- Autorização de segurança com base na gestão de utilizadores e alvos

**FinSpy Agent**

- Interface gráfica de utilizador para sessões directas
- Configuração e análise de dados dos alvos

# FINSPY MOBILE

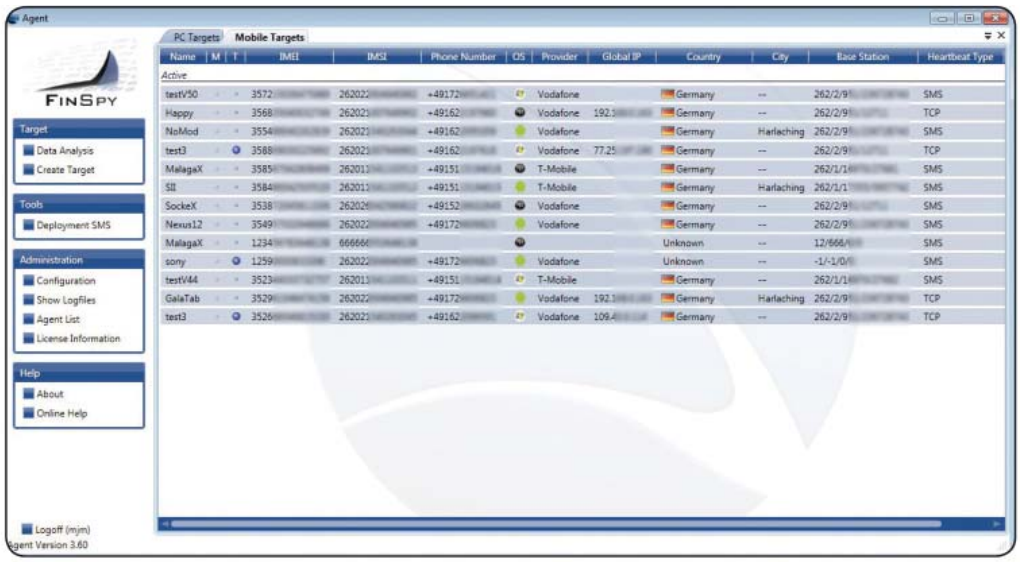
## Acesso aos telemóveis alvo em todo o mundo




O **Telefone alvo** comunica através de GPRS/UMTS/Wi-Fi ou SMS/Chamadas de voz

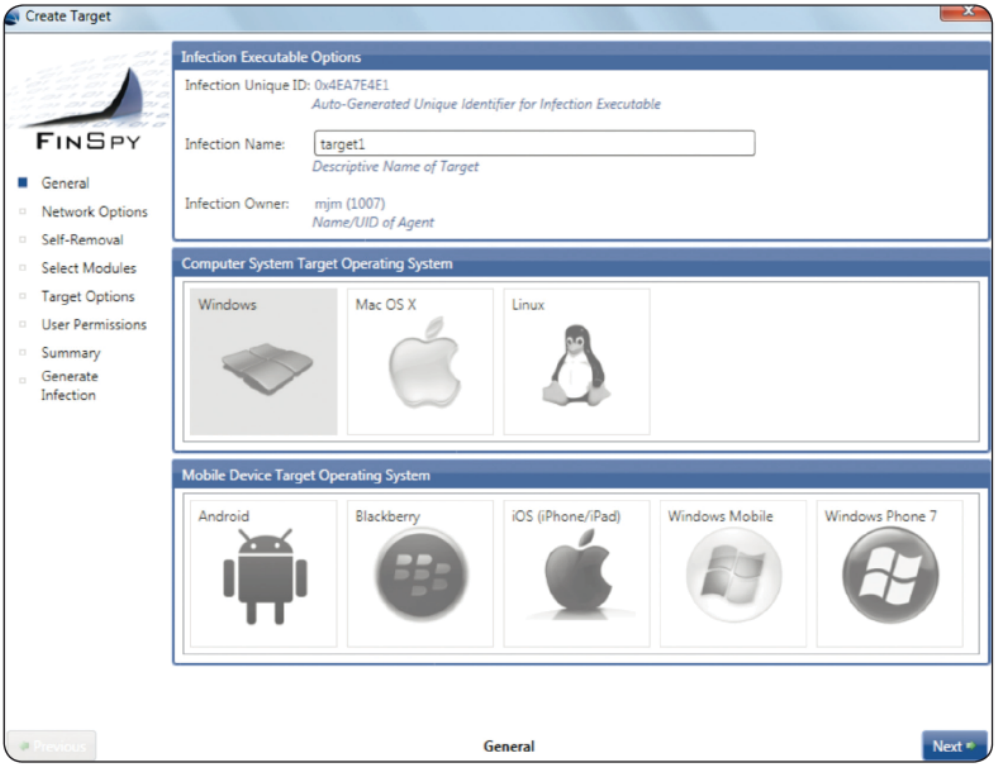
O **FinSpy Master** aceita as ligações earmazena os dados na base de dados

## Interface de utilizador fácil de utilizar



# FINSPY MOBILE

## Suporta todas as plataformas portáteis comuns






GAMMA GROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# FINFLY USB

O FinFly USB proporciona um modo fácil de utilizar e fiável de instalar soluções de controlo remoto em sistemas quando o acesso físico está disponível.

Depois do FinFly USB ter sido inserido num computador, ele **instala automaticamente o software configurado** com pouca ou nenhuma interacção do utilizador e **não requer agentes com formação de TI** quando está a ser utilizado em operações. O FinFly USB pode ser utilizado em **vários sistemas** antes de ser devolvido à sede.

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operaciones tácticas** |
| **Capacidades:** | · **Disponibiliza uma solução de monitorização remota no alvo** |
| **Conteúdo:** | · **Hardware** |

**Exemplo 1 de utilização: Unidade de vigilância técnica**

O FinFly USB foi utilizado com êxito pelas **Unidades de vigilância técnica** em vários países para colocar uma solução de monitorização remota nos sistemas alvo que foram **desligados**, através da simples **inicialização do sistema a partir do dispositivo FinFly USB**. Esta técnica trabalhou mesmo para os Sistemas alvo que tinham **codificação total de disco rígido** com produtos como TrueCrypt activado.

**Exemplo 2 de utilização: Agência de serviços secretos**

Uma fonte num grupo terrorista doméstico recebeu um FinFly USB que **instalou secretamente uma solução de controlo remoto** em vários sistemas do grupo, quando eles estavam a utilizar o dispositivo para trocarem documentos entre eles. Os sistemas alvo foram, então, **monitorizados remotamente a partir da sede** e o FinFly USB foi devolvido posteriormente pela fonte.

**Visão geral da funcionalidade**

- Pode utilizar mesmo em **sistemas desligados com codificação de disco rígido** (por exemplo, TrueCrypt)
- **Instala dissimuladamente a solução de monitorização remota** ao ser inserido no sistema alvo
- É necessária **pouca ou nenhuma interacção do utilizador**
- A funcionalidade pode ser **dissimulada colocando ficheiros normais** como músicas, vídeos e documentos do Officeno dispositivo
- O hardware é **um dispositivo USB, comum e não suspeito**

**Para obter uma lista completa de funcionalidades, consulte as especificações do produto.**

# **FIN**FLY USB

## Componentes do produto


**FinFly USB**

- Dongle USB
- Utiliza uma solução de monitorização remota ao ser inserido nos sistemas alvo
- Utiliza uma solução de monitorização remota durante o processo de arranque

**Integração completa de FinSpy**

- Criação e activação automática através do FinSpy Agent





GAMMAGROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# FINFLY LAN

Alguns dos maiores desafios que as forças policiais enfrentam são os **alvos móveis**, onde **não se consegue aceder fisicamente** a um sistema informático e onde os alvos **não abrem ficheiros** que tenham sido enviados por e-mail para as suas contas.

Em particular, os alvos alertados para a segurança são **quase impossíveis de controlar**, porque eles mantêm os sistemas **actualizados e nenhuma instalação** ou outra técnica básica de intrusão terá sucesso.

O FinFly LAN foi desenvolvido para dissimular uma solução de monitorização remota nos sistemas alvo em LANs (com e sem fios/802.11). Consegue **alterar ficheiros que tenham sido descarregados** pelo alvo directamente, **envia actualizações de software malicioso** do software popular ou **injecta carga explosiva nos sítios da Internet visitados.**

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operações tácticas** |
| **Capacidades:** | · **Coloca a solução de monitorização remota no sistema alvo na rede de área local** |
| **Conteúdo:** | · **Software** |

### Exemplo 1 de utilização: Unidade de vigilância técnica

Uma unidade de vigilância técnica estava a seguir um alvo há semanas sem conseguir aceder fisicamente ao computador. Eles utilizaram o FinFly LAN para instalarem a solução de controlo remoto no computador alvo quando ele estava a utilizar um **ponto de acesso público** num café.

### Exemplo 2 de utilização: Anti-corrupção

O FinFly LAN foi utilizado para instalar remotamente a solução de controlo remoto no computador de um alvo, enquanto ele estava a utilizá-lo **no quarto do hotel**. Os agentes estavam no outro quarto, **efectuaram a ligação à mesma rede** e manipularam os sítios que o alvo estava a visitar para accionarem a instalação.

### Visão geral da funcionalidade

- **Descobre todos os sistemas** ligados à LAN
- Funciona em redes **com e sem fios (802.11)**
- Pode ser combinado com o kit FinIntrusion para **cobrir o acesso de rede**
- Oculta a solução de controlo remoto em Descarregamentos de alvos
- Injecta solução de controlo remoto como actualizações de software
- Instala, remotamente, a solução de controlo remoto através dos sítios visitados pelo alvo

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

# FINFLY LAN

## Componentes Do Producto

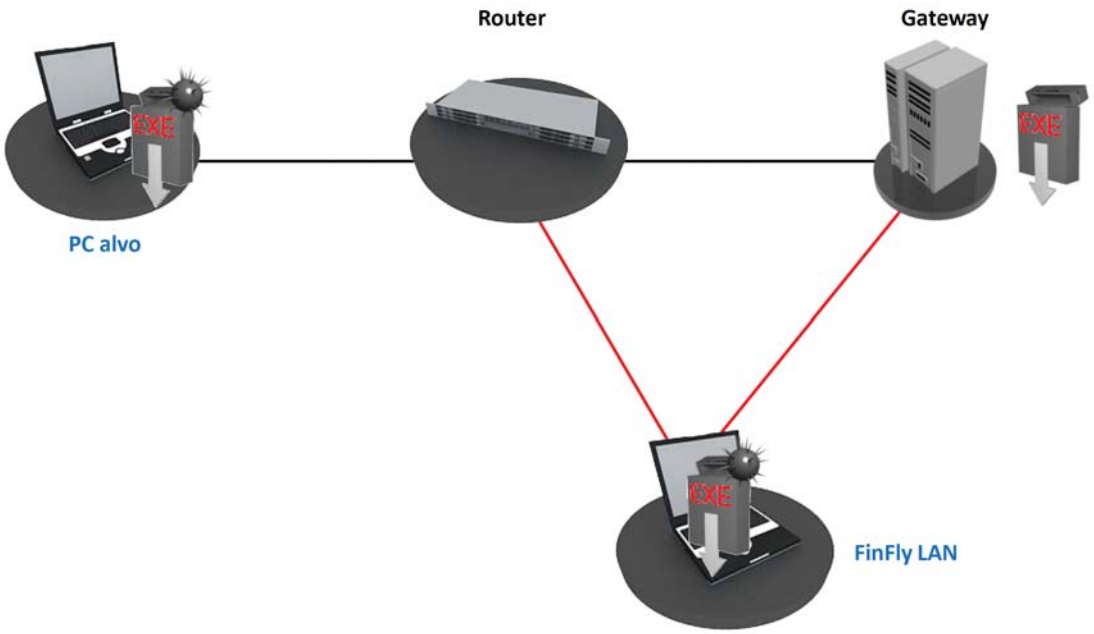
**FinFly LAN**

· Software baseado em Linux com interface fácil de utilizador

**Kit FinIntrusion - Integração (opcional)**

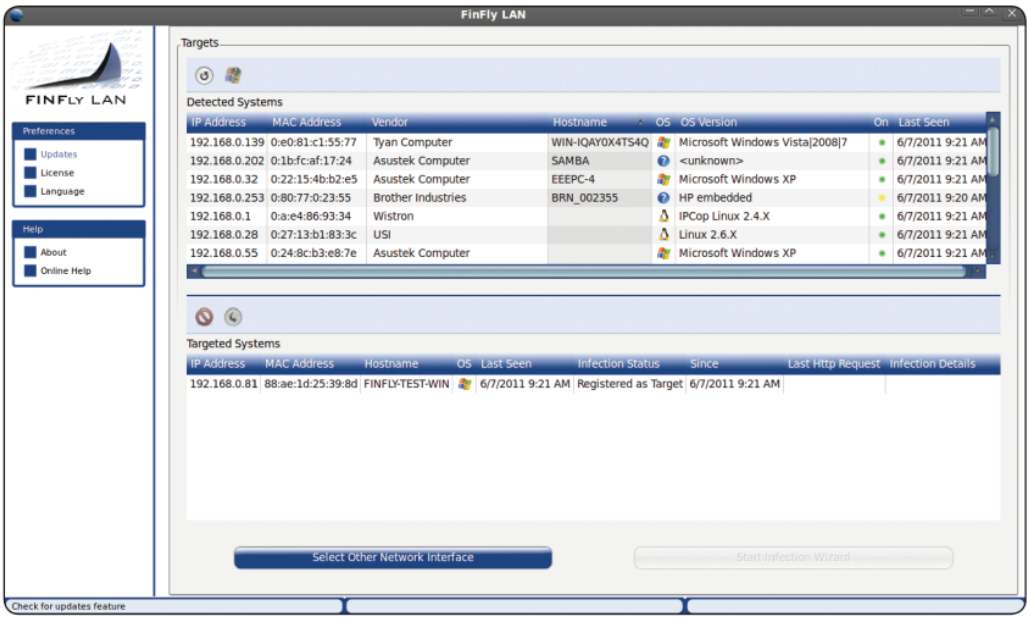
· O FinFly LAN pode ser carregado como um módulo para o Kit FinIntrusion

## Utilização através de LANs



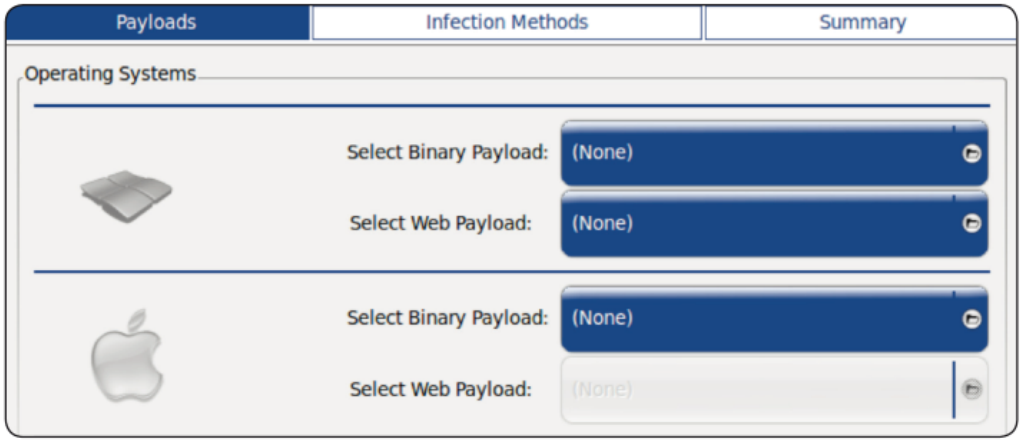
## Interface de utilizador automatizada

· Fácil de utilizar sem formação extensa




## Suporte de carga e vários alvos

· Podem ser adicionados diferentes executáveis para cada alvo








GAMMAGROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# FINFLY WEB

Um dos maiores desafios na utilização de uma solução de controlo remoto é a instalação no sistema alvo, especialmente quando apenas estão disponíveis poucas informações, como um **endereço de e-mail** e não se consegue obter **qualquer acesso físico**.

O FinFly Web foi concebido para fornecer utilização **remota e dissimulada** de um sistema alvo, utilizando uma vasta gama de **ataques baseados na web**.

O FinFly Web proporciona uma **interface do tipo apontar e clicar**, permitindo que o agente **crie um código de utilização personalizado** simples, de acordo com os módulos seleccionados.

A Carga explosiva será utilizada quando o Sistema alvo visitar o sítio da Web preparado com o código personalizado.

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operações estratégicas** |
| **Capacidades:** | · **Coloca uma solução de monitorização remota no sistema alvo através de sítios da Web** |
| **Conteúdo:** | · **Software** |

**Exemplo 1 de utilização: Unidade de vigilância técnica**

Depois de ter traçado o perfil de um alvo, a unidade criou um **sítio da Web de interesse** para o alvo e enviar-lhe a **ligação através de uma quadro de discussão**. Depois de abrir o link para o site da unidade, uma solução de controlo remoto foi instalada no sistema alvo e o alvo foi **controlado a partir da sede**.

**Exemplo 2 de utilização: Agência de serviços secretos**

O cliente instalou o **FinFly ISP no ISP principal** do seu país. Ele foi **combinado com FinFly Web** para **utilizar remotamente a carga explosiva quando o Alvo visitou um sítio da Web de confiança**.

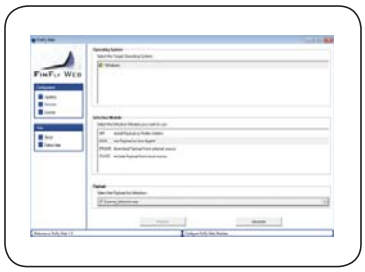
**Visão geral da funcionalidade**

- Módulos da Web **totalmente personalizáveis**
- Podem ser **instalados dissimuladamente em cada sítio da Web**
- Integração total com **FinFly LAN, FinFly NET e FinFly ISP** para instalação mesmo dentro dos sítios da Web populares, como Webmail, Video Portals e muito mais
- Instala a solução de controlo remoto, **mesmo se só for conhecido o endereço de e-mail**
- Possibilidade de marcar todas as pessoas que visitem **sítios da Web configurados**

**Para obter uma lista completa de funcionalidades, consulte as especificações do produto.**

# FINFLY WEB

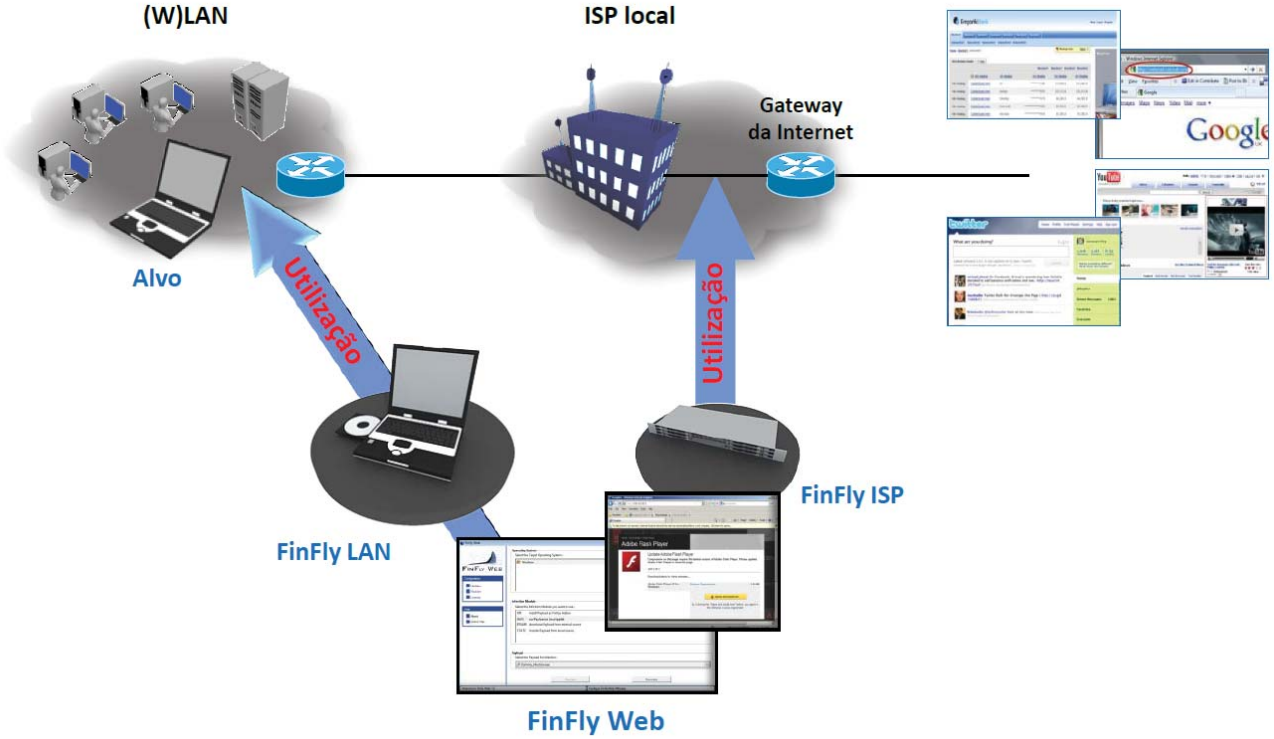
## Componentes do produto



**FinFly Web**

· Gerador de sítio da Web personalizado

## Integração total com o FinFly LAN e FinFly ISP








GAMMA GROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# FINFLY EXPLOIT PORTAL

Os métodos de utilização padrão para soluções de controlo remoto podem, **muitas vezes**, ser aplicados quando do processamento de **alvos bem treinados e extremamente cuidadosos**, pois são familiares com ferramentas e técnicas comuns de utilização.

Na maioria dos cenários, a **opção Explorações de 0 dias** fornece uma forma extremamente poderosa e **fiável para utilizar as Soluções de controlo remoto** explorando **vulnerabilidades não corrigidas** no software que o Alvo está a utilizar.

O portal FinFly Exploit oferece acesso a **uma grande biblioteca** de Explorações de 0 dias e 1 dia para o software popular, como Microsoft® Office, Internet Explorer, Adobe Acrobat Reader e muito mais.

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operaciones estratégicas** |
| **Capacidades:** | · **Implementa una solución de monitorización remota en el sistema objetivo a través de los archivos y el servidor** |
| **Conteúdo:** | · **Portal Web** |

**Exemplo 1 de utilização: Unidade de crime de alta tecnologia**

Uma Unidade de crime de alta tecnologia estava a **investigar um ciber-crime** e necessário para continuar uma Solução de controlo remoto num sistema alvo. Eles utilizaram uma Exploração de 0 dias Adobe Acrobat Reader e enviaram um ficheiro PDF preparada através de e-mail para o alvo. A Solução de controlo remoto foi utilizada automaticamente depois do alvo ter aberto o ficheiro.

**Exemplo 2 de utilização: Agência de serviços secretos**

Um alvo foi identificado **num Quadro de discussão** mas não foi possível qualquer contacto directo ou por e-mail. A Agência criou um Servidor da Web contendo uma **Exploração de 0 dias do Internet Explorer** que utilizou a carga explosiva no sistema alvo **depois do alvo ter aberto o URL**, que foi enviado para ele através de uma mensagem privada no Quadro de discussão.

**Visão geral da funcionalidade**

- Acesso total ao Portal da **Web e Gerador de exploração**
- **Explorações de 0 dias de grau de governo** que funciona em vários sistemas e níveis de correcção sem mais modificações
- Pelo menos, **4 explorações principais** (software comum de navegador/correio/visualização de ficheiros) disponíveis de forma permanente
- **Garantia de 30 dias** para todas as explorações dentro do portal
- **Explorações de 1 dia** actualizadas de forma permanente para vário software

**Para obter uma lista completa de funcionalidades, consulte as especificações do produto.**

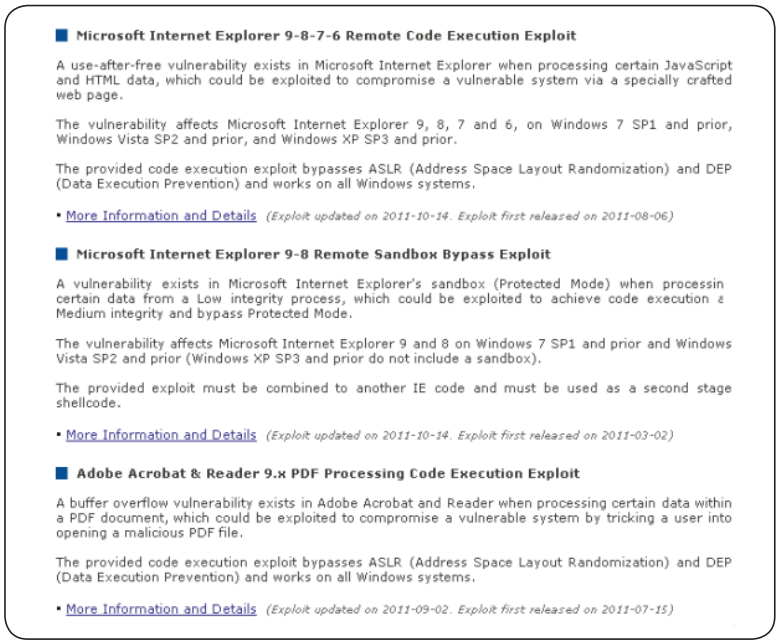
# FINFLY EXPLOIT PORTAL

## Componentes do produto


**FinFly Exploit Portal**

· Web Interface Exploit Library

## Exemplo do portal de exploração 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 processin certain data from a Low integrity process, which could be exploited to achieve code execution a 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)*





GAMMAGROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# FINFLY ISP

Em muitas operação da vida real, o acesso físico a sistemas alvo no país não pode ser obtido e uma **instalação remota** dissimulada de uma solução de controlo remoto é requerida para **monitorizar o alvo a partir da sede**.

O FinFly ISP é uma solução estratégica, **aplicável a todo o país e táctica** (móvel) que pode ser **integrada num acesso de ISP e/ou rede principal**, para instalar remotamente a solução de controlo remoto em sistemas alvo seleccionados.

As aplicações do FinFly ISP baseiam-se na **tecnologia do servidor de grau da transportadora**, proporcionando o máximo de **fiabilidade e escalabilidade** para satisfazer todos os desafios relacionados com topologias de rede. Está disponível uma vasta gama de interfaces de rede – todas **protegidas com funções de bypass** – para a ligação de rede activa requerida.

Vários métodos passivos e activos da identificação do alvo – a partir do **controlo on-line** através do toque passivo para **comunicações interactivas**, entre o FinFly ISP e os servidores AAA – asseguram que os alvos são identificados e o respectivo tráfego é fornecido para o processo de utilização.

O FinFly ISP consegue **corrigir ficheiros** que tenham sido descarregados pelo alvo **directamente, ou enviar actualizações de software malicioso** para software popular. A nova edição integra a aplicação de utilização remota poderosa **FinFly Web** de Gamma que injecta uma carga explosiva em qualquer sitio da Web visitado pelo alvo.

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operações estratégicas** |
| **Capacidades:** | · **Coloca uma solução de monitorização remota no sistema alvo através de sítios da rede do ISP** |
| **Conteúdo:** | · **Hardware/Software** |

**Exemplo de utilização: Agência de serviços secretos**

O FinFly ISP foi instalado nas redes do ISP principal do país, e foi utilizado activamente para instalar remotamente uma solução de controlo remota nos sistemas alvo. Como os alvos possuem contas ADSL de IP dinâmico, eles são identificados com o nome de início de sessão de raio.

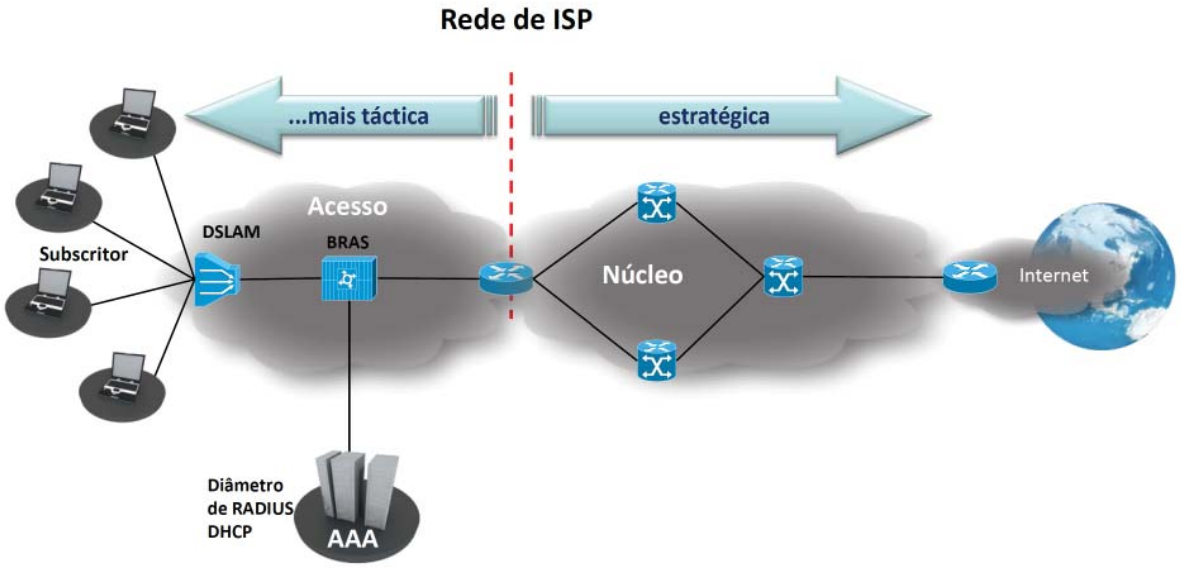
**Visão geral da funcionalidade**

- Pode ser instalado dentro de uma **rede de um ISP**
- Suporta **todos os protocolos comuns**
- Alvos seleccionados por **endereço IP, Nome de início de sessão Radius DHCP e MSISDN**
- Oculta a solução de controlo remoto em **Descarregamentos de alvos**
- Injecta uma solução de controlo remoto como **actualizações de software**
- Instala, remotamente, a solução de controlo remoto através dos **sítios da Web visitados pelo alvo**

**Para obter uma lista completa de funcionalidades, consulte as especificações do produto.**

## Possibilidades de localização diferente

· O FinFly ISP pode ser utilizado como uma solução táctica ou estratégica em redes de ISP



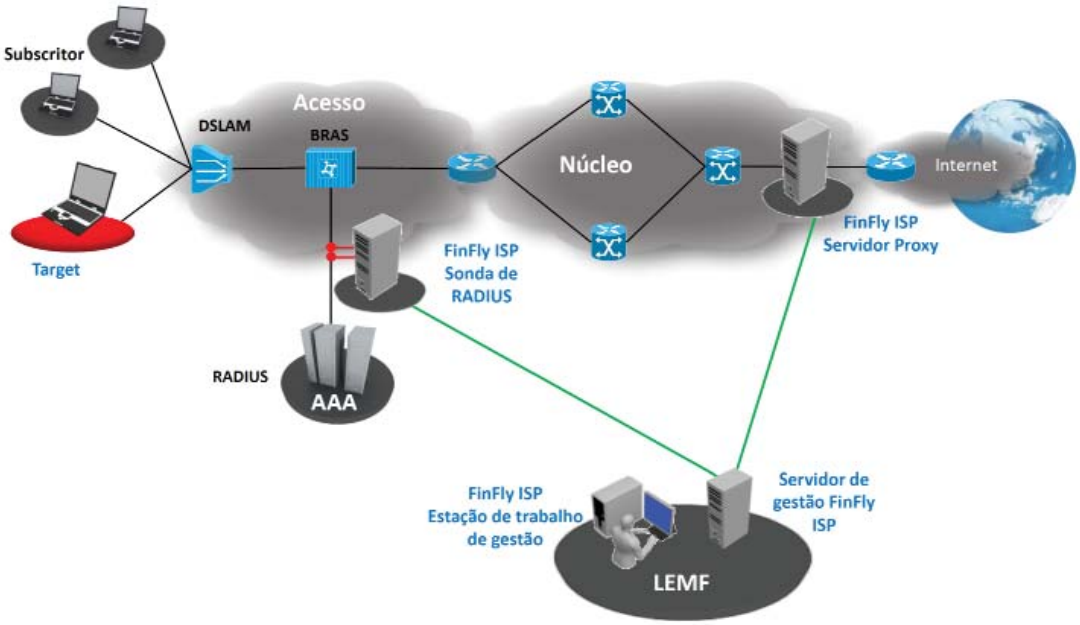

Uma solução táctica é móvel e o hardware é dedicado às tarefas de utilização dentro da rede de acesso próximo dos pontos de acesso do alvo. Ela pode ser instalada numa base de curto prazo, de acordo com os requisitos tácticos centralizados num alvo específico ou num número pequeno de alvos numa área.

Uma solução estratégica consiste numa instalação permanente, de ISP e em todo o país do FinFly ISP, para seleccionar os alvos e cargas explosivas de utilização a partir de sedes remotas, sem ser necessário o LEA estar numa localização.

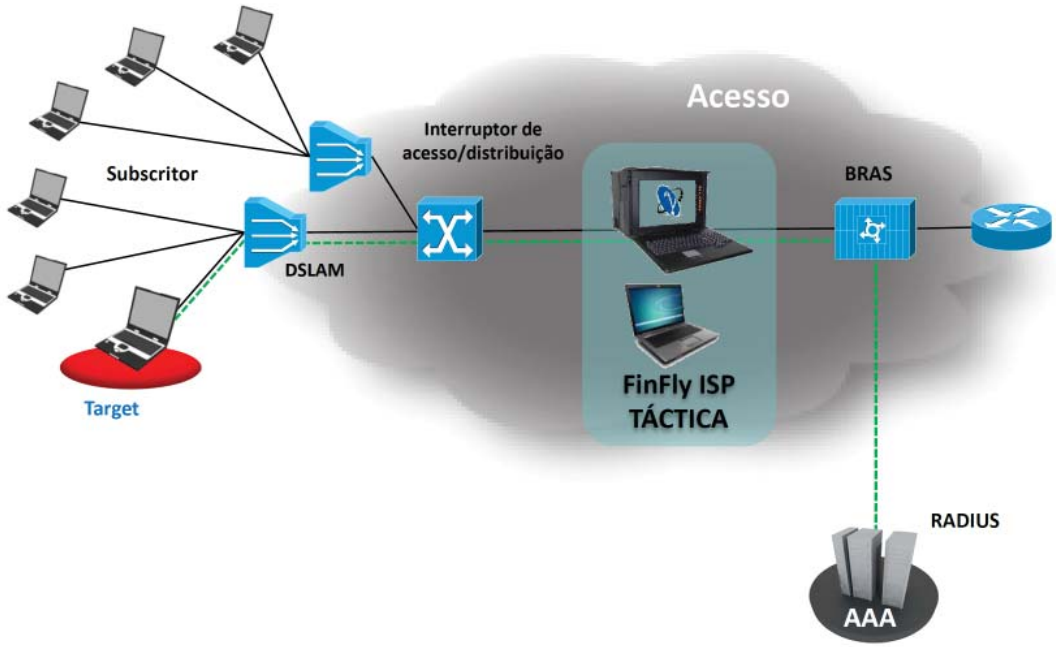
Claro que é possível combinar soluções tácticas e estratégicas para atingir um máximo de flexibilidade para as operações de infecção.

## Configuração da rede

### Disposição estratégica




### Disposição táctica



# FINFLY ISP

## Componentes do produto

### Estratégica de ISP de FinFly

Uma colocação estratégica de FinFly ISP consiste, ao menos, do seguinte:

- Sistema de gestão em LEMF
- Servidores de sonda de identificação alvo no sistema AAA da rede
- Servidores de Proxy de infecção em, por exemplo, Gateways de Internet

**Servidores FinFly ISP**
HP ProLiant DL-Series G7
Estação de trabalho empresarial

**Estação de trabalho ISP FinFly**
HP Z-Series

| | |
|---|---|
| Rendimento | > 20 Gbps |
| N° máx. de NIC: | 2-8 NIC |
| Interfaces: | 1 GE Cobre / Fibra<br>10 GE Cobre / Fibra<br>SONET/SDH OC-3 / -192<br>STM-1 / -64<br>ATM AAL5 |
| Processadores: | Intel XEON 1x – 8x |
| Núcleo | 2 – 8 Núcleos/Processador |
| RAM: | 12 GB – 1 TB |
| Capacidade de HDD: | SAS 146GB – 4.8TB de 3x |
| Funcionalidades | HP iLO 3<br>Potência redundante<br>Ventiladores redundantes<br>Função de interruptor de bypass (se aplicável) |
| Sistema operativo | Linux GNU (Debian 5.0) endurecido |

### Táctica de FinFly ISP

Um sistema táctico de FinFly ISP consiste do seguinte:

- Identificação do alvo e servidor portátil de proxy de infecção
- Portátil do sistema de gestão

**FinFly ISP portátil**
Atlas A9 17" Portable

**FinFly ISP Estação de trabalho**
Lenovo Thinkpad T-Series

| | |
|---|---|
| Rendimento | 6 Gbps |
| N° máx. de NIC: | 3 NIC |
| Interfaces: | 1x 1000BASE-T (cobre; 2 puertos)<br>1x 1000BASE-SX (fibra MM; 2 puertos)<br>1x 1000BASE-LX (fibra SM; 2 puertos)<br>Outros a pedido |
| Procesadores: | 1 Intel Core i7<br>Intel Xeon a pedido |
| Núcleo | 4 núcleos/processador |
| RAM: | Mínimo de 12 GB |
| Capacidade de HDD: | 2 x SATA de 1TB |
| Unidad óptica | DVD+/-RW SATA |
| Monitor | 1 x 17" TFT, teclado, painel táctil |
| Funcionalidades | Função de interruptor de bypass para NICs |
| Sistema operativo | Linux GNU (Debian 5.0) endurecido<br>Windows 7 Prof. (Gestão Nb.) |





GAMMAGROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# FINFLY NET

Em muitas operação da vida real, o acesso físico a sistemas alvo no país não pode ser obtido.

Para resolver esta situação, é necessária uma **instalação remota dissimulada** de uma Solução de controlo remoto **para ser possível controlar o alvo a partir da sede**.

**FinFly NET** é uma solução **táctica** (portátil) a ser utilizada num **ambiente de LAN "simples"** (como hotéis, pontos de acesso directos, empresas - com apoio do proprietário da rede) de forma rápida, para instalação remota da Solução de controlo remoto em sistemas alvo seleccionados.
A solução FinFly NET é baseada num **PC portátil de alto desempenho** com um **portátil de gestão** para fornecer o máximo de mobilidade e flexibilidade nas redes alvo. Está disponível uma vasta gama de placas de interface de rede – todas **protegidas com funções de bypass** – para a ligação de rede activa requerida.

O utilizador final pode seleccionar vários **métodos passivos sofisticados de Identificação de alvo e tráfego**. Estes variam de Controlo de DHCP/RADIUS (Endereço de MAC, Nomes de utilizador), Controlo de fluxo e Impressões digitais. Cada método pode ser utilizado de forma autónomo ou combinado, para fornecer o máximo de sucesso na identificação de alvos de interesse. Os endereços de IP fixos também podem ser utilizados.
Consegue **alterar ficheiros que tenham sido descarregados** pelo alvo directamente, **envia actualizações de software malicioso** do software popular ou **injecta carga explosiva nos sítios da Internet visitados**.

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Operações tácticas** |
| **Capacidades:** | · **Utiliza a Solução de controlo remoto no sistema alvo num ambiente de LAN "fácil de utilizar"** |
| **Conteúdo:** | · **Hardware/Software** |

**Exemplo de utilização de LAN: Agência de serviços secretos**

FinFly NET é utilizado, por exemplo, numa LAN de hotel de DSLModem antes do tráfego de IP ser transmitido para uma rede do fornecedor de serviços de Internet.

Os alvos de interesse são **identificados do tráfego de IP por vários métodos passivos de perfilamento** e identificação, e a Solução de controlo remoto será utilizada nos sistema alvo identificados positivamente.

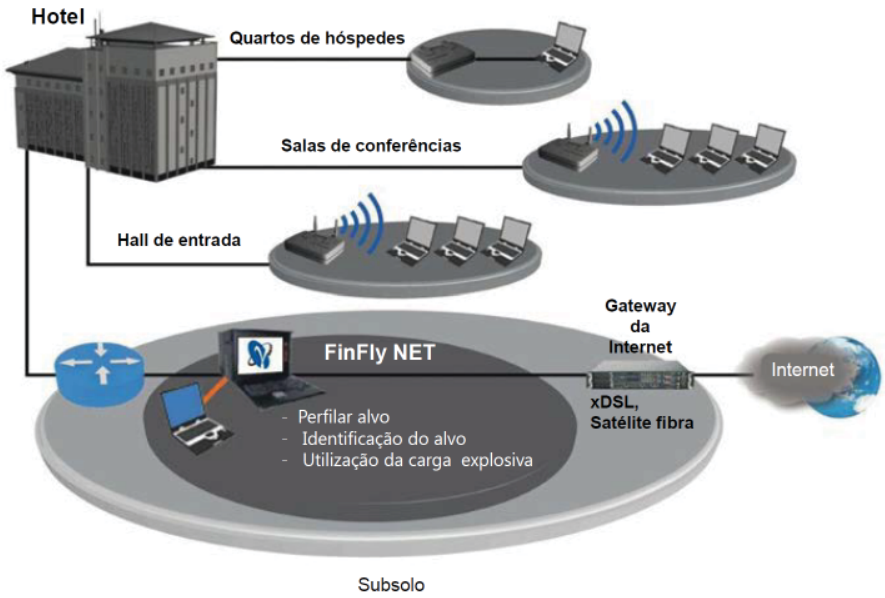
**Visão geral da funcionalidade**

- Pode ser instalada dentro de um **ambiente de LAN** (hotel, ponto de acesso directo, empresa…)
- Ethernet 1000Base-T, 1000Base-SX, 1000Base-LX
- Identifica os alvos utilizando métodos diferentes e passivos **de perfilamento/identificação**
- Oculta a solução de controlo remoto em **Descarregamentos de alvos**
- Injecta uma solução de controlo remoto como **actualizações de software**
- Instala a solução de controlo remoto através dos sítios da **Web visitados pelo alvo**

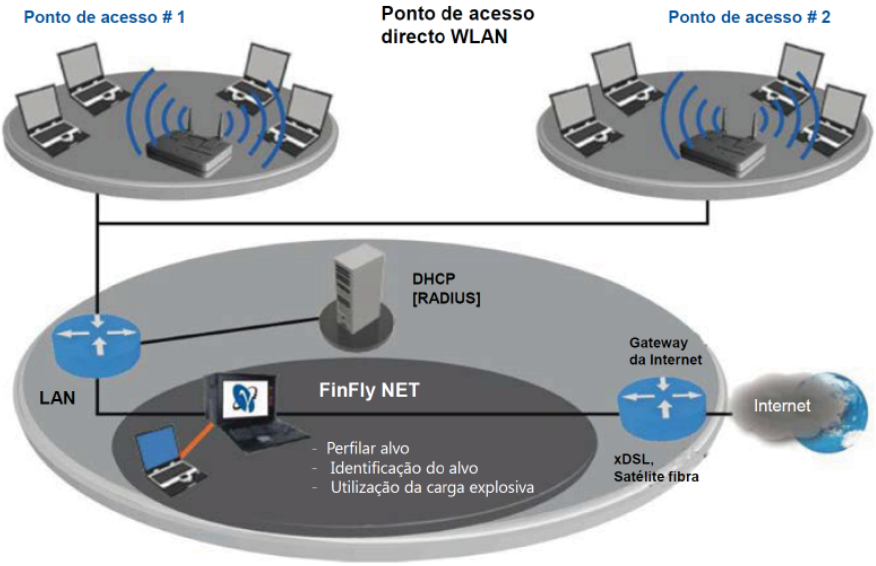
**Para obter uma lista completa de funcionalidades, consulte as especificações do produto.**

## DIFERENTES POSSIBILIDADES DE UTILIZAÇÃO

### Utilização na LAN de um hotel




### Utilização na LAN de um ponto de acesso directo WLAN




A FinFly NET será utilizada no local apropriado dentro das instalações. Depois de ligar a entrada de linha portátil às ligações fornecidas, o utilizador pode iniciar a análise do tráfego seleccionando diferentes métodos para identificar os alvos de interesse e respectivo tráfego de IP. Os métodos a serem utilizados para identificação do alvo dependem fortemente da configuração da rede, bem como das funcionalidades e serviços fornecidos e utilizados.

## PERFILAMENTO E IDENTIFICAÇÃO DO ALVO

**Módulo de identificação de HTTP**
Tipos e versões, histórico e idiomas do navegador e sistema operativo

**Módulo de identificação de e-mail**
POP3, SMTP

**Módulo de identificação de início de sessão**
FTP, HTTP, IMAP, IRC, NNTP, POP, SMTP

**Módulo de identificação de TCP/UDP**
IP de origem/destino, Portas de origem/destino

**Módulo de identificação de DHCP/RADIUS**
Início/fim de MAC, Nome de anfitrião, sessão de IP

## MÉTODOS DE UTILIZAÇÃO DO ALVO

**Binário/descarregamento**
Correcção de ficheiros ".exe" e/ou ".scr"

**Actualizar injecção**
Falsificar actualizações para aplicações diferentes

**Utilização do sítio da Web**
Utilizar FinFly Web para aplicação durante actividades de navegação

# **FIN**FLY NET

## Componentes do produto

A FinFly NET consiste no seguinte:

- Perfilamento e identificação do alvo e Utilização do servidor de Proxy
- (Portátil)
- Sistema de gestão (Portátil)

**FinFly NET portátil**
Atlas A9 17" Portable

**Gestão de FinFly NET**
Lenovo Thinkpad T-Series

| | |
|---|---|
| Rendimento | 6 Gbps |
| N° máx. de NIC: | 3 NIC |
| Interfaces: | 1x 1000BASE-T (Cobre; 2 portas)<br>1x 1000BASE-SX (MM-Fibra; 2 portas)<br>1x 1000BASE-LX (SM-Fibra; 2 portas)<br>Outros a pedido |
| Procesadores: | 1 x Intel Core i7<br>Intel Xeon a pedido |
| Núcleos | 4 núcleos/processador |
| RAM: | Mínimo de 12 GB |
| Capacidad de disco duro: | 2 x SATA de 1TB |
| Unidad óptica | DVD+/-RW SATA |
| Monitor | 1 x 17" TFT, teclado, painel táctil |
| Funcionalidades | Função de interruptor de bypass para NICs |
| Sistema operativo | Linux GNU (Debian 5.0) endurecido<br>Windows 7 Prof. (Gestão Nb.) |

**Nota importante:**
Gamma fornece junto a FinFly NET as mesmas capacidades de inteligência integradas na solução FinFly ISP, em que as capacidades de identificação do alvo são implementadas numa solução de ISP fixa ou portátil. Esta solução é caracterizada por tecnologia de servidor de alta desempenho que será personalizada e integrada no ambiente relevante de ISP e requisitos relacionados.

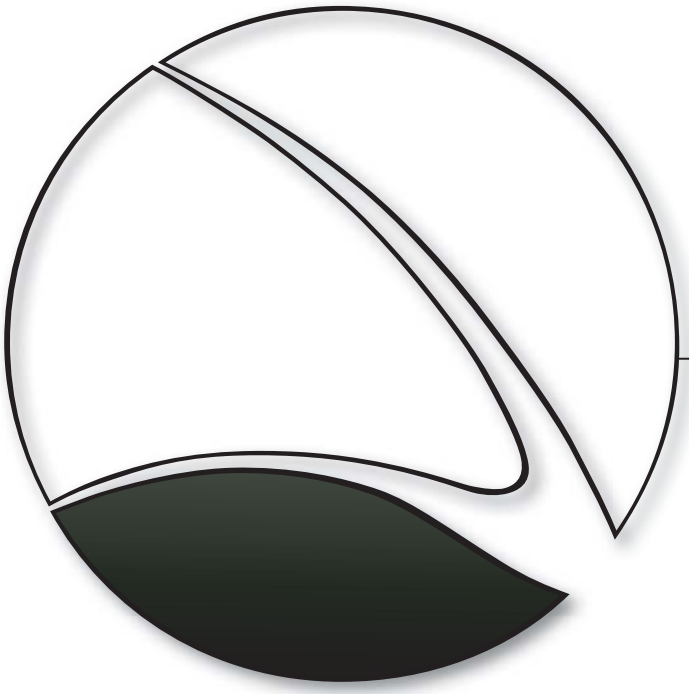




GAMMAGROUP
GAMMA INTERNATIONAL
United Kingdom
Tel : +44 - 1264 - 332 411
Fax : +44 - 1264 - 332 422

# Programa De Formação De Intrusão De TI

## **FIN**TRAINING



O programa de formação de intrusão de TI inclui cursos dos produtos fornecidos, bem como métodos e técnicas práticas de intrusão de TI. Este programa transfere anos de conhecimentos e de experiência para os utilizadores finais, maximizando as suas capacidades neste campo.

FINFISHER™
IT INTRUSION

WWW.FINFISHER.COM

# Programa De Formação De Intrusão De TI

## FINTRAINING

A consciência da segurança é **essencial para qualquer governo** de modo a manter a segurança da TI e a **evitar as ameaças** com sucesso contra a infraestrutura de TI, o que pode resultar numa perda de confidencialidade, integridade de dados e disponibilidade.

Por outro lado, tópicos como **Ciber-guerra**, Intercepção activa e obtenção dos serviços secretos através da **intrusão de TI** têm-se tornado importantes diariamente, e requerem que os governos **criem equipas de intrusão TI** para **enfrentarem estes novos desafios.**

Os cursos FinTraining são dados por **especialistas de intrusão de TI de classe mundial**, e assentam em cenários totalmente práticos que se centralizam em **operações da vida real**, conforme requerido pelo utilizador final para resolver os seus **desafios diários**.

A **Gamma** combina os cursos de formação individual num **programa de formação profissional e consultadoria** que assenta ou melhora as capacidades de uma equipa de intrusão de TI. Os cursos de formação são **completamente personalizados** de acordo com os requisitos e desafios operacionais do utilizador final.

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Transferência de conhecimentos** |
| **Capacidades:** | · **Conhecimentos de intrusão de TI**<br>· **Capacidades de ciber-guerra** |
| **Conteúdo:** | · **Formação** |

### Assuntos do curso de amostragem

- **Traçamento do perfil** de sítios da Web e pessoas alvo
- Rastreio **anónimo de e-mails**
- **Acesso remoto** a contas de Webmail
- **Avaliação de segurança** de servidores e serviços de Web
- Exploração **prática de software**
- **Intrusão de TI sem fios** (WLAN/802.11 e Bluetooth)
- Ataques em **infraestruturas críticas**
- Farejamento de **dados e credenciais do utilizador** em redes
- **Controlo de pontos de acesso**, ciber-cafés e redes de hotéis
- **Intercepção e registo de chamadas** (VoIP e DECT)
- **Danificação de palavras-passe**

### Programa de consulta

- Programa de **Formação e consultadoria** de intrusão total de TI
- Criação estruturada e **Formação da equipa de intrusão de TI**

Encontrará la lista completa de funciones en las Especificaciones del producto

**Cursos personalizados em instalações de formação de nível elevado em todo o mundo**





GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

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

# FINSUPPORT

## FinSupport

O FinSupport possui actualizações da linha de produtos FinFisherTM em combinação com um contrato de assistência anual.

A página de Web da assistência do FinFisherTM e a Equipa de suporte proporcionam os seguintes serviços aos nossos clientes:

- Acesso on-line a:
  - Manual do Utilizador mais recente
  - Especificações do produto mais recentes
  - Slides de formação do produto mais recentes
  - Atendimento para relato de problemas
  - Mais recente relatório de teste de anti-vírus
  - Atendimento para solicitação de funcionalidades

- Actualizações regulares ao software:
  - Correcções de problemas
  - Novas funcionalidades
  - Novas versões principais

- Suporte técnico através de Skype:
  - Correcções de problemas
  - Suporte operacional parcial

### FinLifelineSupport

O FinLifelineSupport proporciona um suporte de back-office profissional para a resolução de problemas e consultas técnicas. Também proporciona suporte de back-office remoto, para correcções de problemas do software FinFisherTM e substituições do hardware ao abrigo da garantia. Além disso, com o FinLifelineSupport, o cliente recebe automaticamente novas funcionalidades com a edição padrão de correcções de problemas.

| INFORMAÇÕES RÁPIDAS | |
|---|---|
| **Utilização:** | · **Solução global e apoio operacional** |
| **Capacidades:** | · **Correcção de problemas, actualização de funcionalidades e capacidades** |
| **Conteúdo:** | · **Hardware/Software** |

### Actualizações do software

O FinLifelineSupport inclui actualizações regulares do software e garante actualizações automáticas ao software existente com correcções fornecidas através sistema de actualização.

Estas actualizações incluem novas funcionalidades, novos aperfeiçoamentos e novas funções de acordo com o mapa do cliente (excluindo o hardware).

WWW.FINFISHER.COM



GAMMA INTERNATIONAL
United Kingdom

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