



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



**FINFISHER™**

IT INTRUSION

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

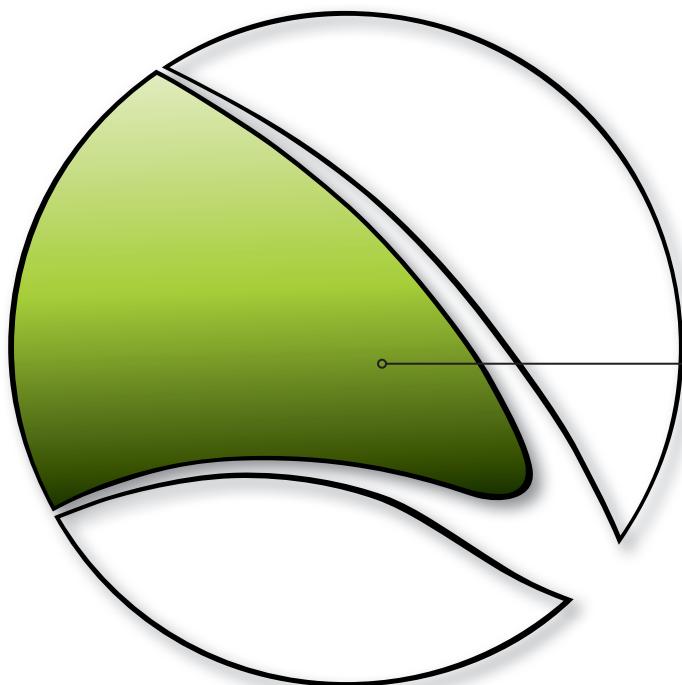


# Portfólio De Intrusão Táctica De TI

**FINKIT DE INTRUSÃO**

**FINUSB SUITE**

**FINFIREWIRE**



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

## 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**.

### 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, depois, para controlar **Webmail (Gmail, Yahoo, ...)** e **credenciais de redes sociais (Facebook, MySpace, ...)**. Isto permitiu que os investigadores **controlassem remotamente** estas contas a partir da sede, sem necessidade de estarem perto do alvo.

INFORMAÇÕES RÁPIDAS	
Utilização:	<ul style="list-style-type: none"><li>· Operações estratégicas</li><li>· Operações táticas</li></ul>
Capacidades:	<ul style="list-style-type: none"><li>· Quebras na encriptação WEP/WPA</li><li>· Controlo de rede (incluindo sessões SSL)</li><li>· Ataques de intrusão de TI</li></ul>
Conteúdo:	<ul style="list-style-type: none"><li>· Hardware/Software</li></ul>

### Exemplo 2 de utilização: Segurança de TI

Vários clientes utilizaram o kit FinIntrusion para **comprovar com sucesso a segurança** das redes e sistemas informáticos para efeitos 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 e servidores de web do alvo (por exemplo, Blogs, Fóruns de discussão) e o controlo das suas actividades, incluindo registos de acesso e muito mais.

### Resumo das funcionalidades

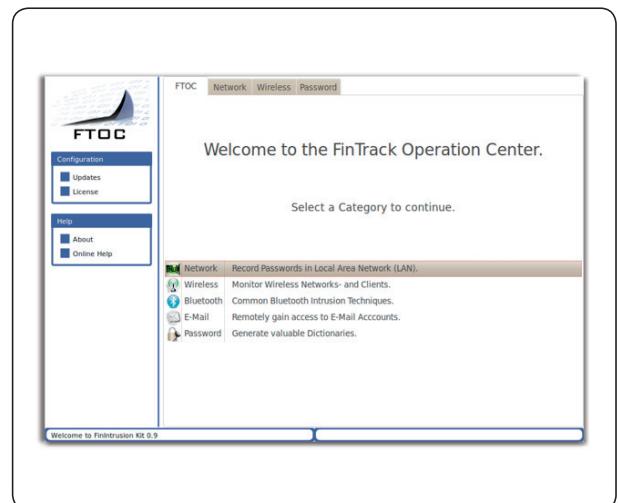
- Detecta **LAN sem fios (802.11)** e **dispositivos Bluetooth®**
- Recupera palavras-passe WEP (64 e 128 bits) **no prazo de 2 a 5 minutos**
- **Quebra palavras-passe WPA1 e WPA2**, utilizando ataques do dicionário
- Controla activamente LAN (com e sem fios) e **extraí Nomes de utilizador e Palavras-passe mesmo de sessões encriptadas TLS/SSL**
- Emula **Pontos de acesso sem fios simulados** (802.11)
- 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 uma lista completa das funcionalidades, consulte as especificações do produto



## FINKIT DE INTRUSÃO

### Componentes Do Produto



### Kit FinIntrusion – Unidade táctica dissimulada

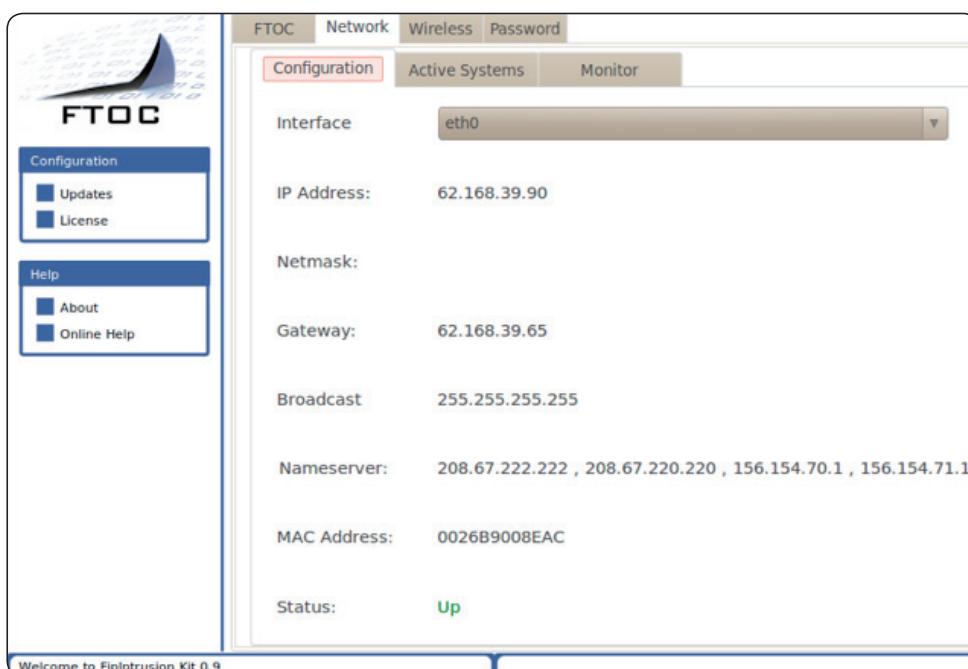
Componentes básicos de intrusão de TI:

- 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

### Controlo de LAN/WLAN automatizado



### Intrusão De LAN (802.11) Sem Fios

Captura mesmo os dados encriptados SSL como Web-mail, Portais de vídeo, Banca online e muito mais

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...**



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

Foi utilizado com êxito em operações por todo o mundo, onde importantes serviços secretos foram encontrados em alvos, em operações dissimuladas e abertas.

DE UN VISTAZO	
Utilização:	· Operações tácticas
Capacidades:	· Obtenção de informações · Acesso do sistema · 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 comuns**, 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 de cookies e muito mais.

### Resumo das funcionalidades

- Optimizado para **Operações dissimuladas**
- Utilização fácil através da **execução automatizada**
- **Encriptação segura** com RSA e AES
- 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...)

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

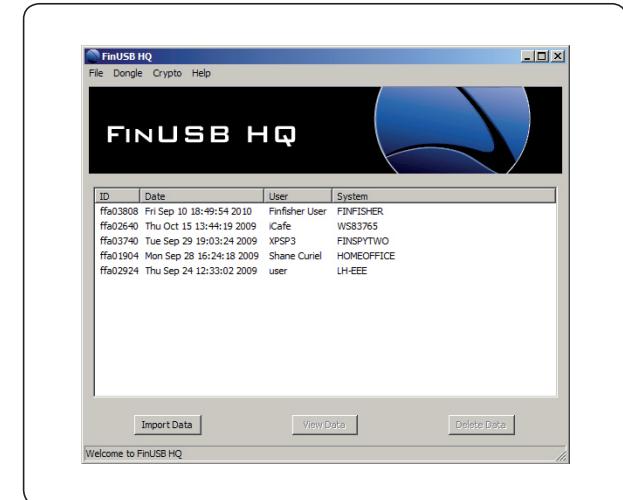


## FINUSB SUITE

### 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 Dongle FinUSB (U3 - 16GB)

- Extrai dissimuladamente os dados do sistema
- Encripta dados enquanto estão a ser processados



FinUSB - Ignorar palavra-passe do Windows

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

### Usabilidade 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. Crie um relatório



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. Crie um relatório

### Relatórios Profissionais



As unidades de vigilância técnica e os especialistas forenses enfrentam, frequentemente, uma situação em 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 aceda ao sistema alvo sem deixar rastro e sem danificar as provas forenses essenciais.

### 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, 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 **copiasse todos os ficheiros** antes de desligar o computador e o levar para a sede.

### Resumo das funcionalidades

- 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 os **sistemas Windows, Mac e Linux**
- Funciona com **FireWire/1394, PCMCIA e Express Card**

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

INFORMAÇÕES RÁPIDAS	
Utilização:	· Operações tácticas
Capacidades:	· Ignora palavra-passe do utilizador · Acede dissimuladamente ao sistema · Recupera palavras-passe a partir da RAM · Permite dados forenses directos
Contenido:	· Hardware/Software

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

Combinando 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.

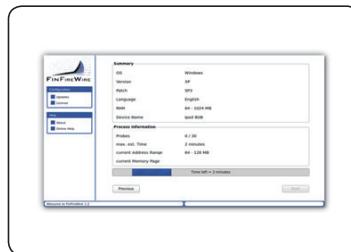


### Componentes Do Produto



**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 ExpressCard 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



As informações aqui contidas são confidenciais e estão sujeitas a alterações sem aviso prévio. A Gamma Group International não será responsável por omissões ou erros editoriais ou técnicos aqui contidos



GAMMA INTERNATIONAL  
United Kingdom

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

[info@gammagroup.com](mailto:info@gammagroup.com)

# Controlo Remoto E Soluções De Infecção

**FINSPY**

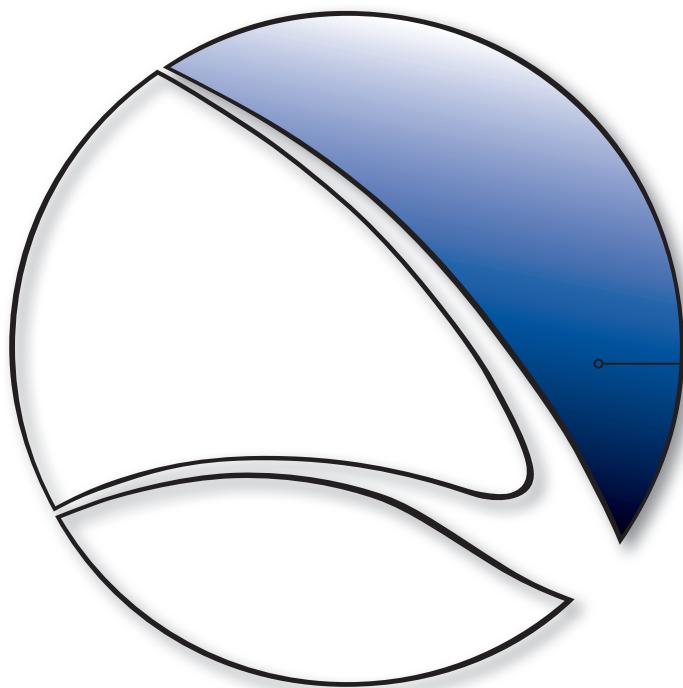
**FINSPY MOBILE**

**FINFLY USB**

**FINFLY LAN**

**FINFLY WEB**

**FINFLY ISP**



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.



**FINFISHER™**  
IT INTRUSION

O FinSpy é uma solução de controlo remoto comprovada em campo, que permite aos governos enfrentarem os desafios actuais de monitorização de **Alvos Móveis e em Alerta de Segurança** que mudam regularmente de local, empregam canais de **comunicações encriptados e anónimos** e/ou **residem em países estrangeiros**.

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

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

O FinSpy tem provado ser bem sucedido em operações por todo o mundo **durante vários anos**, tendo sido obtidas importantes informações secretas 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 ponto do mundo** onde o sistema alvo se encontrar.

DE UN VISTAZO	
Uso:	<ul style="list-style-type: none"><li>· Operaciones estratégicas/tácticas</li></ul>
Capacidades:	<ul style="list-style-type: none"><li>· Monitorizar equipos remotos</li><li>· Monitorizar comunicaciones cifradas</li></ul>
Contenido:	<ul style="list-style-type: none"><li>· Hardware/Software</li></ul>

### 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 actividades suspeitas, especialmente as **comunicações de Skype** para estrangeiros. 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.

### Resumo das funcionalidades

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**

Ejemplos de funciones en la sede central:

- Protecção de provas (Prova válida de acordo com os **Padrões europeus**)
- **Gestão do utilizador** de acordo com as autorizações de segurança
- Comunicações e encriptação dos dados de segurança utilizando **RSA 2048 e AES 256**
- Oculto do público através de **Proxies anónimos**
- Pode ser **totalmente integrado** com a funcionalidade de controlo das forças policiais

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



### Componentes Do Produto



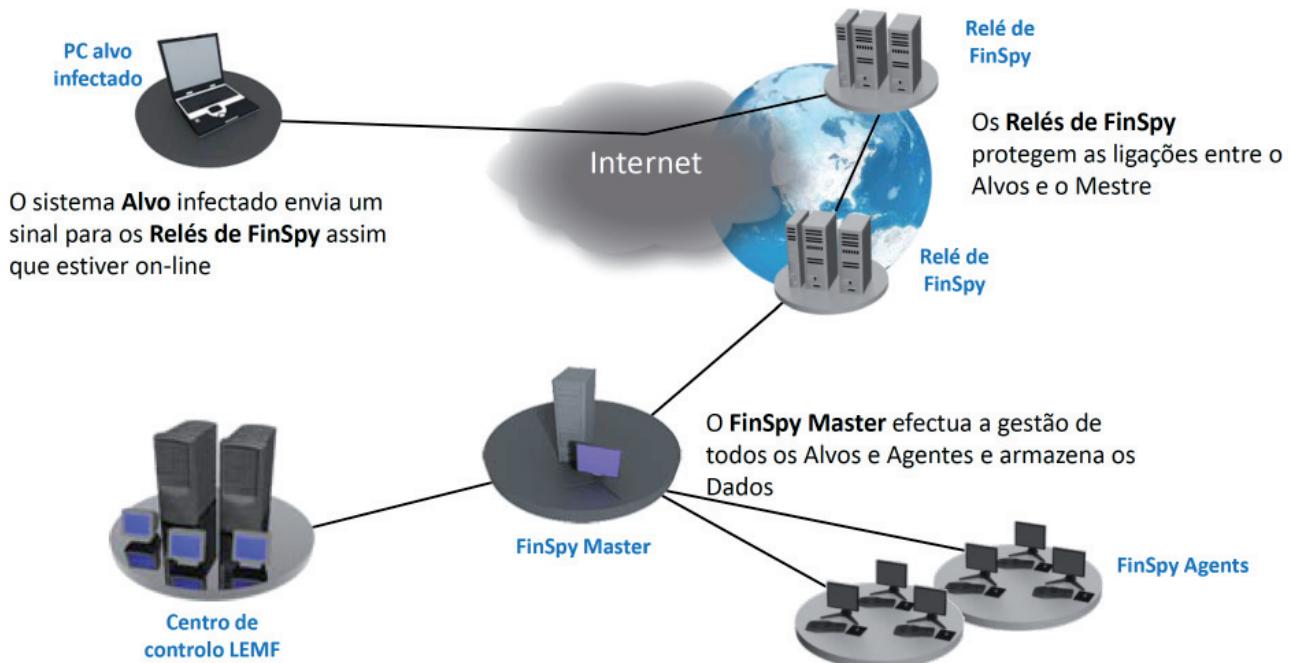
#### FinSpy Master e Proxy

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

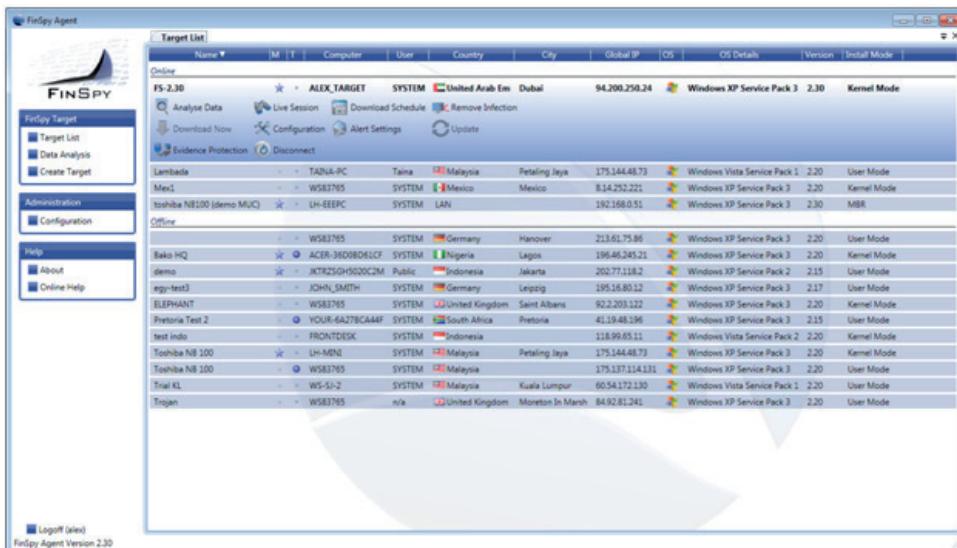
#### FinSpy Agent

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

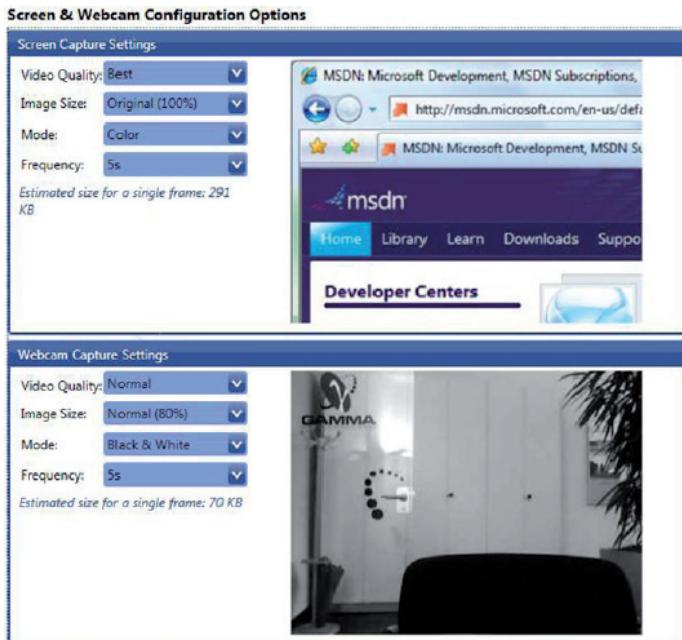
### Acesso Aos Sistemas Informáticos Alvo Em Todo O Mundo



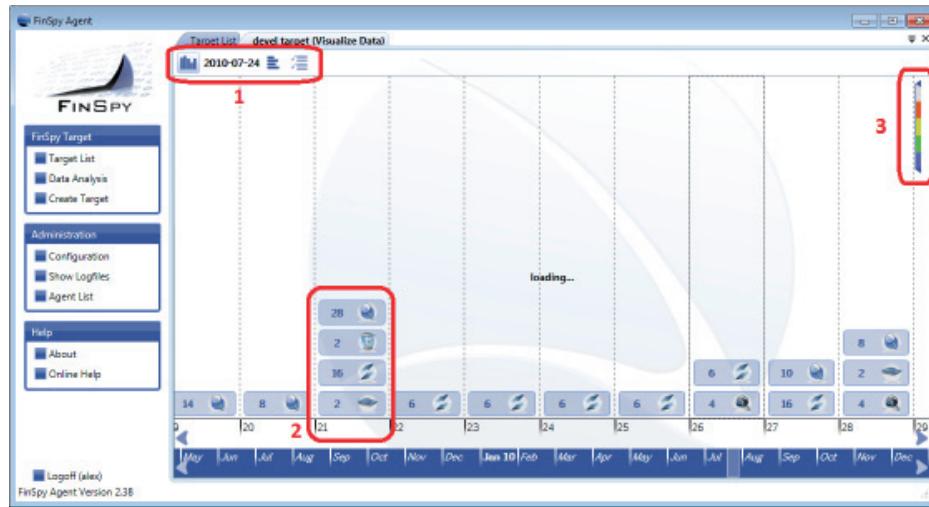
### Interface De Utilizador Fácil De Utilizar



### Configuração Directa



### Acesso Directo Ao Sistema



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



As informações aqui contidas são confidenciais e estão sujeitas a alterações sem aviso prévio. A Gamma Group International não será responsável por omissões ou erros editoriais ou técnicos aqui contidos.

GAMMA INTERNATIONAL  
United Kingdom

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

## LICENCIAS FINSPY

### **Linhas gerais**

A solução FinSpy contém 3 tipos de licenças de produto:

#### **A. Licença de actualização**

A Licença de actualização controla se o **FinSpy** consegue encontrar novas actualizações a partir do servidor Actualização Cobham. Está combinado com o módulo **Suporte pós venda** do **FinFisher™**.

Depois da expiração, o sistema **FinSpy** continuará **totalmente funcional**, mas não encontrará versões mais recentes nem correções de problemas a partir do servidor Actualização de FinSpy.

#### **B. Licença de agente**

A Licença de agente controla o número de **Agentes de FinSpy** que podem iniciar sessão simultaneamente no **FinSpy Master**.

Exemplo:

- São adquiridas **5 Licenças de agente**.
- As licenças de **Agente FinSpy** podem ser instaladas num número ilimitado de sistemas. No entanto,
- Só 5 sistemas de **Agente FinSpy** podem iniciar sessão no **FinSpy Master** e trabalhar com os **dados ao mesmo tempo**

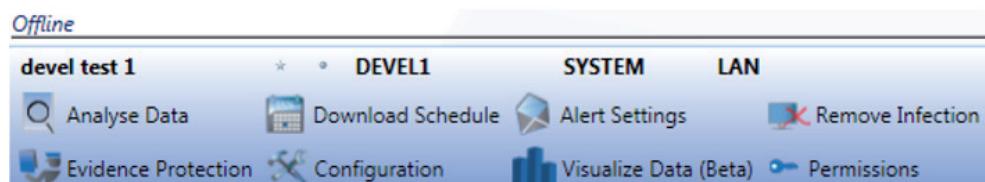
#### **C. Licença alvo**

A Licença alvo controla o número de **Alvos FinSpy** que podem ser simultaneamente **ativos**.

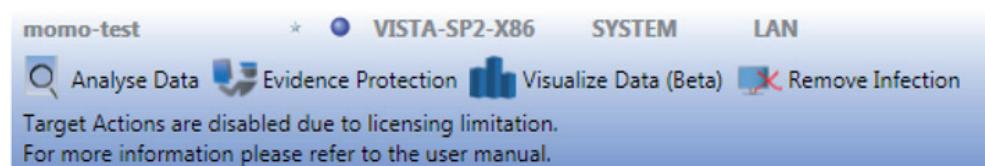
Active refere-se às instalações **Alvo FinSpy activadas**, independentemente do Sistema alvo estar online ou offline.

Quando o **Alvo FinSpy** é utilizado num Sistema alvo e não estão disponíveis quaisquer Licenças Alvo, o **Alvo FinSpy** fica temporariamente desactivado e não será possível qualquer gravação e acesso directo. Assim que a nova licença estiver disponível (por exemplo, actualizando a licença existente ou desinfectando um dos **Alvos FinSpy** activos), será atribuído ao alvo uma licença livre, sendo activada e começando a gravar e a fornecer acesso directo.

### **Captura de ecrã de alvo activo com licença**



### **Captura de ecrã de alvo inactivo sem licença**



# Controlo Remoto E Soluções De Infecção

## FINSPY MOBILE

O FinSpy Mobile preenche uma lacuna nas capacidades de intercepção dos Governos para as **plataformas de telemóveis inteligentes** mais comuns.

Especificamente, as organizações **sem capacidade de intercepção de rede ou de recepção directa** podem aceder aos telemóveis e interceptar dispositivos com capacidades avançadas. Além disso, a solução oferece **acesso a comunicações encriptadas**, bem como a **dados armazenados no dispositivo** que não são transmitidos.

As soluções tradicionais táticas 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 táticos
- Encriptação terminal-para-terminal a partir do dispositivo, como Mensageiros, 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 de forma remota**, independentemente da parte do mundo onde o alvo se localizar.

### Resumo das funcionalidades

Computador 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 nacional** 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 e Android**

DE UN VISTAZO	
Uso:	<ul style="list-style-type: none"><li>· Operaciones estratégicas</li><li>· Operaciones tácticas</li></ul>
Capacidades:	<ul style="list-style-type: none"><li>· Monitorización remota de teléfonos móviles</li></ul>
Contenido:	<ul style="list-style-type: none"><li>· Hardware/Software</li></ul>

### 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.

Sede – Funcionalidades de exemplo:

- Protecção de provas (Prova válida de acordo com os **Padrões europeus**)
- **Gestão do utilizador** de acordo com as autorizações de segurança
- Comunicações e encriptação dos dados de segurança utilizando **RSA 2048 e AES 256**
- Oculto do público através de **Proxies anónimos**
- Pode ser **totalmente integrado** com a funcionalidade de controlo das forças policiais

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

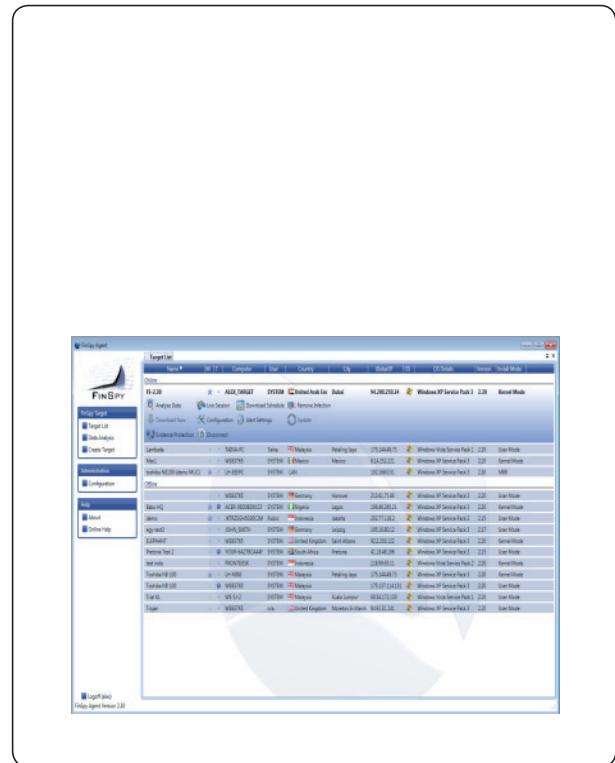


**FINFISHER™**  
IT INTRUSION

# Controlo Remoto E Soluções De Infecção

## FINSPY MOBILE

### Componentes Do Produto



#### FinSpy Master e Proxy

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

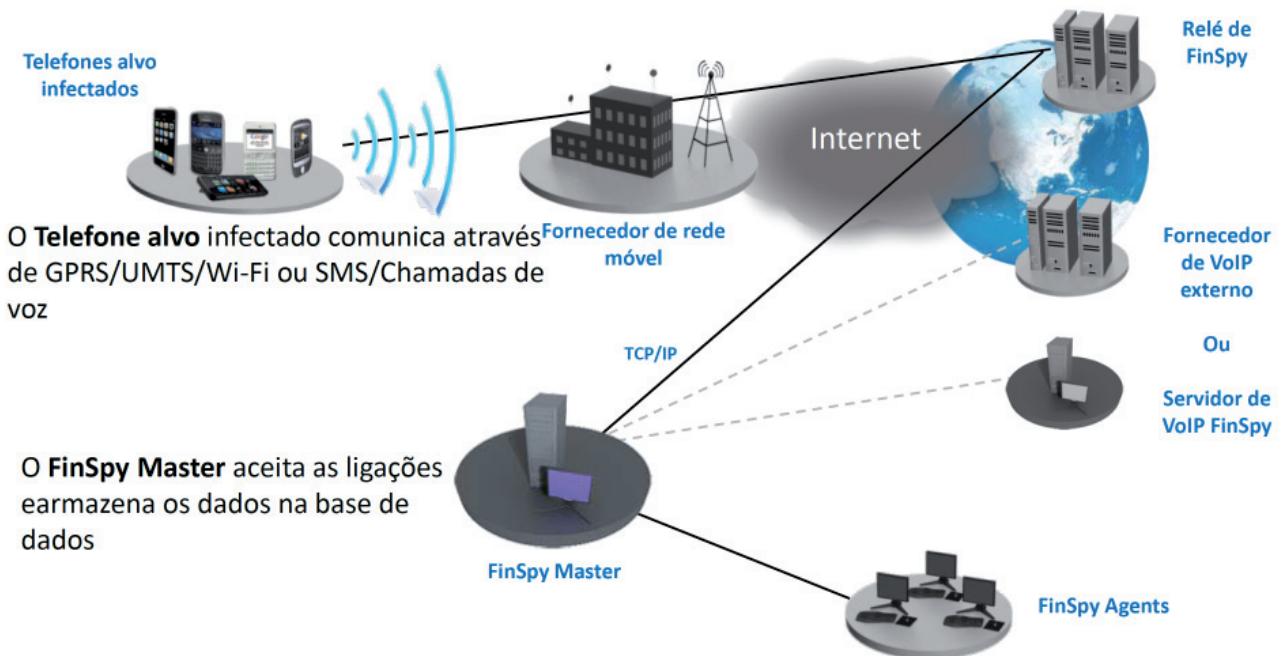
#### FinSpy Agent

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

# Controlo Remoto E Soluções De Infecção

## FINSPY MOBILE

### Acesso aos telemóveis alvo em todo o mundo



### Interface de utilizador 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 displays an event log titled "Event Report" with the following columns:

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



# Controlo Remoto E Soluções De Infecção

FINFLY USB

O FinFly USB proporciona uma forma 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, **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.

DE UN VISTAZO	
Uso:	· Operaciones tácticas
Capacidades:	· Implementa una solución de monitorización remota en el objetivo
Contenido:	· 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 desenvolver uma solução de monitorização remota nos sistemas alvo que foram **desligados**, através da simples **inicialização do sistema a partir do dispositivo FinFly USB**.

## 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 estavam a utilizar o dispositivo para trocarem documentos entre si. Os sistemas alvo foram, então, **monitorizados remotamente a partir da sede** e o FinFly USB foi devolvido posteriormente pela Fonte.

## Resumo das funcionalidades

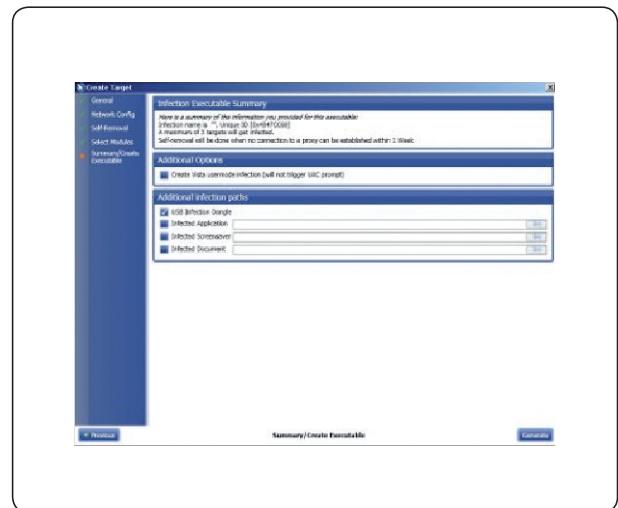
- Instala dissimuladamente a solução de monitorização remota ao ser inserido no sistema alvo
- É necessária **pouca ou nenhuma interacção do utilizador**
- A funcionalidade pode ser **dissimulada, colocando ficheiros normais** como música, vídeos e documentos do Office no dispositivo
- Infecção do sistema alvo desligado aquando da **inicialização a partir de USB**
- O hardware é um dispositivo **USB comum e não suspeito**

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



**FINFISHER™**  
IT INTRUSION

### Componentes Do Produto



#### FinFly USB

- Dongle SanDisk 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

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 infectados** que tenham sido enviados por e-mail para as suas contas.

Em particular, os alvos alertados para a segurança são **quase impossíveis de infectar**, porque mantêm os sistemas **actualizados**, e **nenhuma instalação** ou técnicas básicas de intrusão terão sucesso.

O FinFly LAN foi desenvolvido para dissimular uma solução de monitorização remota nos sistemas alvo em LAN (com e sem fios/802.11). É capaz de **infectar ficheiros descarregados** pelo alvo em tempo real, infectar o alvo **enviando actualizações falsas** do software mais popular ou infectar o alvo, **injectando a carga nos sites visitados**.

### 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. Foi utilizado o FinFly LAN para instalar a solução de controlo remoto no computador alvo, quando este utilizava um **ponto de acesso público** num café.

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

### Exemplo 2 de utilização: Anticorrupção

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

### Resumo das funcionalidades

- **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 a Solução de Controlo Remoto como **actualizações de software**
- Instala, remotamente, a solução de controlo remoto através dos sites visitados pelo alvo

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



### Componentes Do Produto



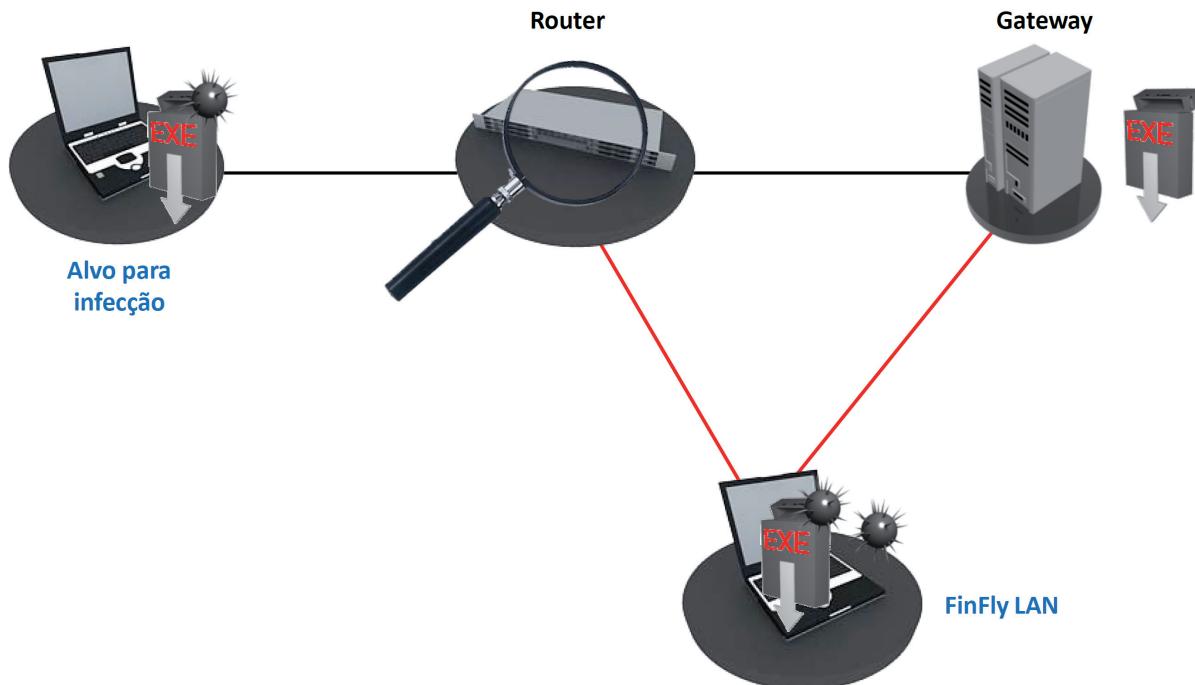
#### FinFly LAN

- Software baseado em Linux com interface fácil de utilizar

#### FinIntrusion Kit - Integração (opcional)

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

### Infecção Através De LANs



### Interface de utilizador 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

### Suporte de carga e vários alvos

- Podem ser adicionados diferentes executáveis para cada alvo

**Infection Techniques**

Binary Infection(.exe,.scr)

Operation mode: Do not Infect

www.microsoft.com

▶

◀

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



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 aplicar uma infecção **remota e de cobertura** a 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 infecção personalizado** simples, de acordo com os módulos seleccionados.

Os sistemas alvo que visitam um site preparado com o código de infecção implementado serão **infectados dissimuladamente** com o software configurado.

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

Depois de traçar o perfil de um alvo, a unidade criou um **sítio de interesse** para o mesmo e enviou-lhe a **ligação através de uma quadro de discussão**. Depois de abrir a ligação para o site da unidade, uma solução de controlo remoto foi instalada no sistema alvo e o alvo pode ser **monitorizado a partir da sede**.

### DE UN VISTAZO

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

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

O cliente instalou o **FinFly ISP no ISP principal** do seu país. Este foi **combinado com o FinFly Web** para, de forma remota, **infectar os alvos que visitaram os sites de ofensa governamental**, injectando dissimuladamente o código FinFly Web nos sites marcados.

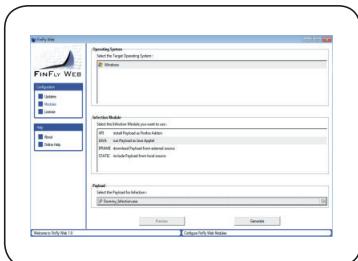
### Resumo das funcionalidades

- Módulos da Web totalmente personalizáveis
- Podem ser **instalados dissimuladamente em cada site**
- Integração total com **FinFly LAN** e **FinFly ISP** para instalação mesmo dentro de sites populares, como Webmail, Portais de Vídeo 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 **sites configurados**

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



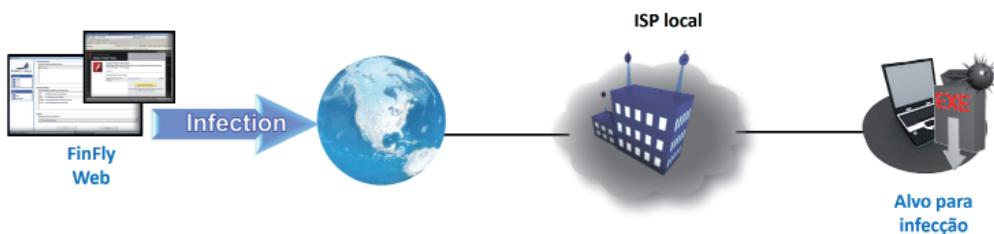
### Componentes Do Produto



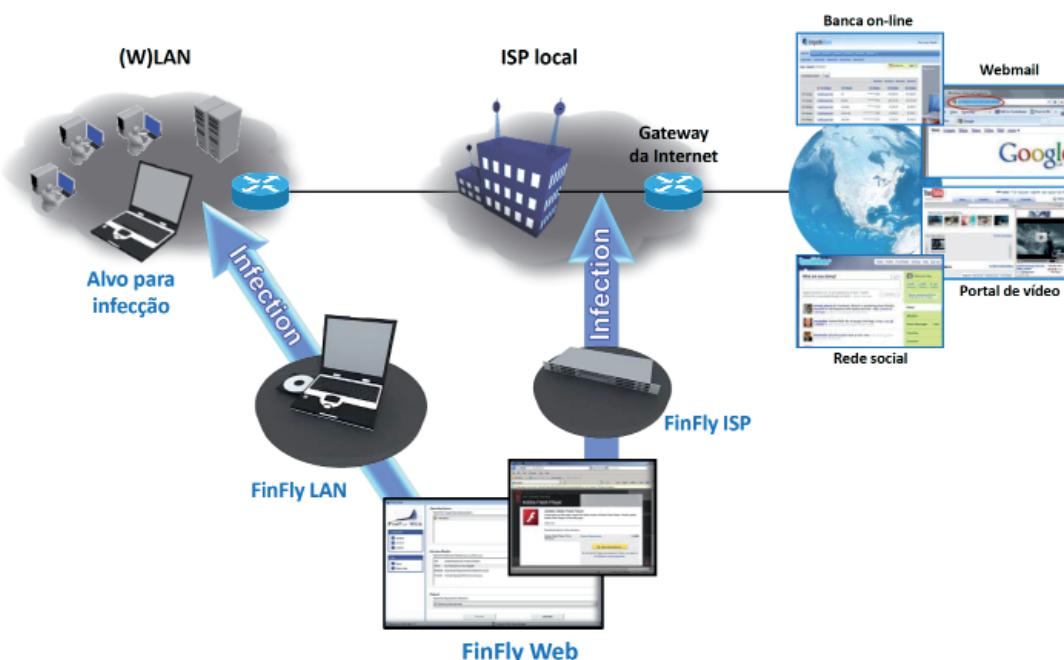
#### FinFly Web

- Software de apontar e clicar para criar sites de infecções personalizadas

### Infecção directa de FinFly Web



### Integração total com o FinFly LAN e FinFly ISP



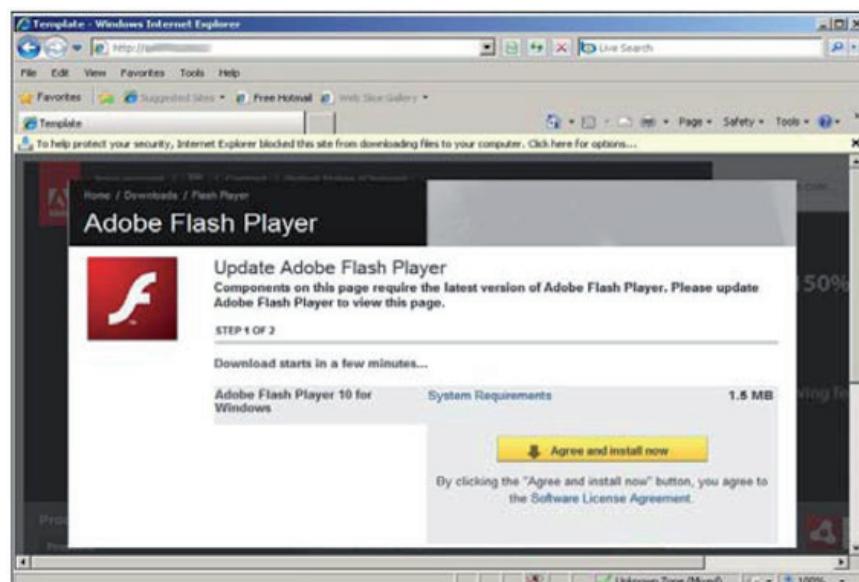
### Ejemplo: Java Applet (Internet Explorer, Firefox, Opera, Safari)

O site pedirá ao alvo para aceitar um plug-in de Java que possa ser assinado com qualquer nome de empresa (por exemplo “Microsoft Corporation”)



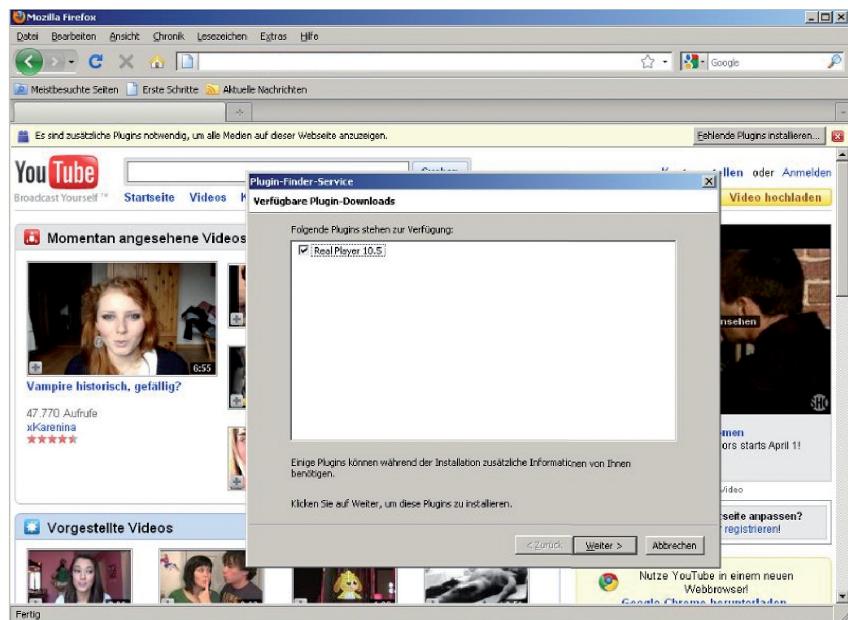
### Exemplo: Componente em falta (IE, Firefox, Opera, Safari)

O site fará parecer que um plug-in ou um codec está em falta no sistema alvo, e pedirá para descarregar e instalar o software em falta



### Exemplo: XPI em falta (apenas Firefox, todas as plataformas)

Este módulo solicitará ao alvo que instale os plug-ins adicionais para ser possível visualizar o site.



# Controlo Remoto E Soluções De Infecção

**FINFLY ISP**

Em muitas operações 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 operadora**, 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 online** 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 infecção.

O FinFly ISP consegue **infectar ficheiros** que tenham sido descarregados pelo alvo **directamente** ou infecta o alvo **enviando actualizações de software malicioso** do software popular. A nova versão integra, agora, a poderosa aplicação de infecção remota Cobham **FinFly Web** para infectar alvos directamente, ao **visitar qualquer site**.

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

## Exemplo de utilização: Agência de serviços secretos

O FinFly ISP foi instalado nas redes do ISP principal do país, e utilizado activamente para instalar remotamente uma solução de controlo remoto nos sistemas alvo. Como os alvos possuem contas ADSL de IP dinâmico, são identificados com o Nome de Início de Sessão de Raio.

## Resumo das funcionalidades

- Pode ser instalado dentro de uma **rede de um ISP**
- Suporta **todos os protocolos comuns**
- Alvos seleccionados pelo **endereço de IP ou nome de início de sessão de raio**
- 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 sites **visitados pelo alvo**

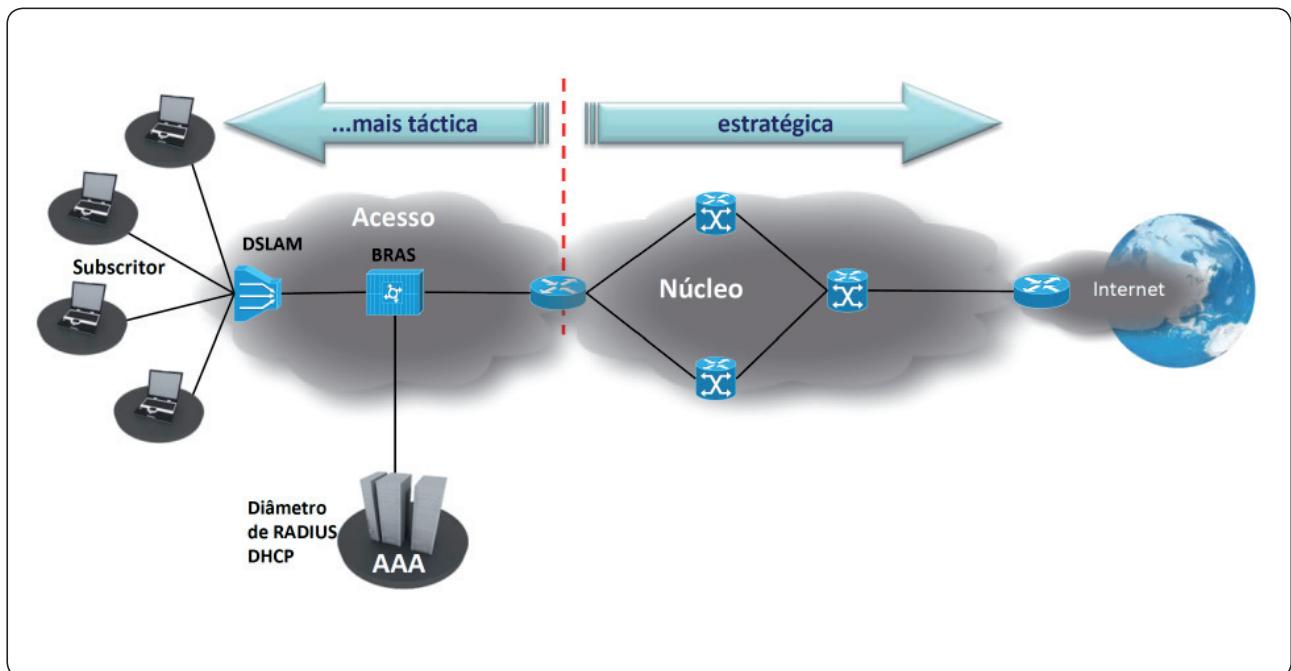
Para uma lista completa de funcionalidades, consulte as especificações do produto



**FINFISHER™**  
IT INTRUSION

### Possibilidades De Localização Diferente

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



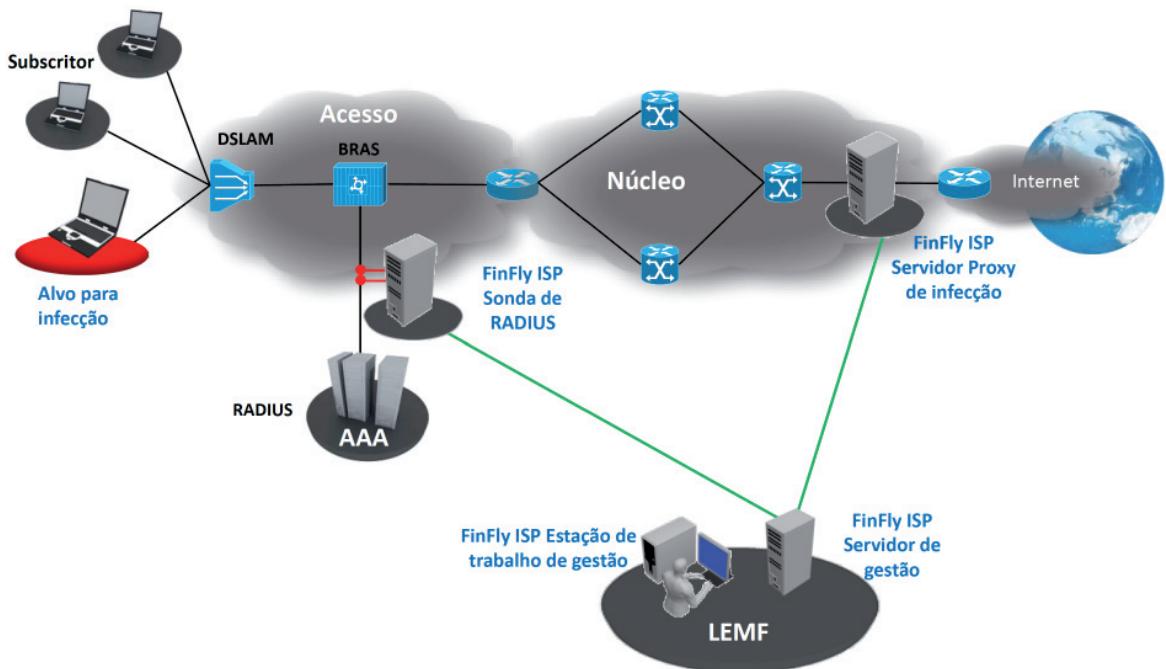
Uma solução táctica é móvel e o hardware é dedicado às tarefas de infecção dentro da rede de acesso próximo dos pontos de acesso do alvo. Esta pode ser instalada numa base de curto prazo, de acordo com os requisitos tácticos centralizados num alvo específico ou num número pequeno de alvos numa área.

Uma solução estratégica consiste numa instalação permanente, de ISP e em todo o país do FinFly ISP, para seleccionar e infectar qualquer alvo a partir da sede remota, sem ser necessário o LEA estar no local.

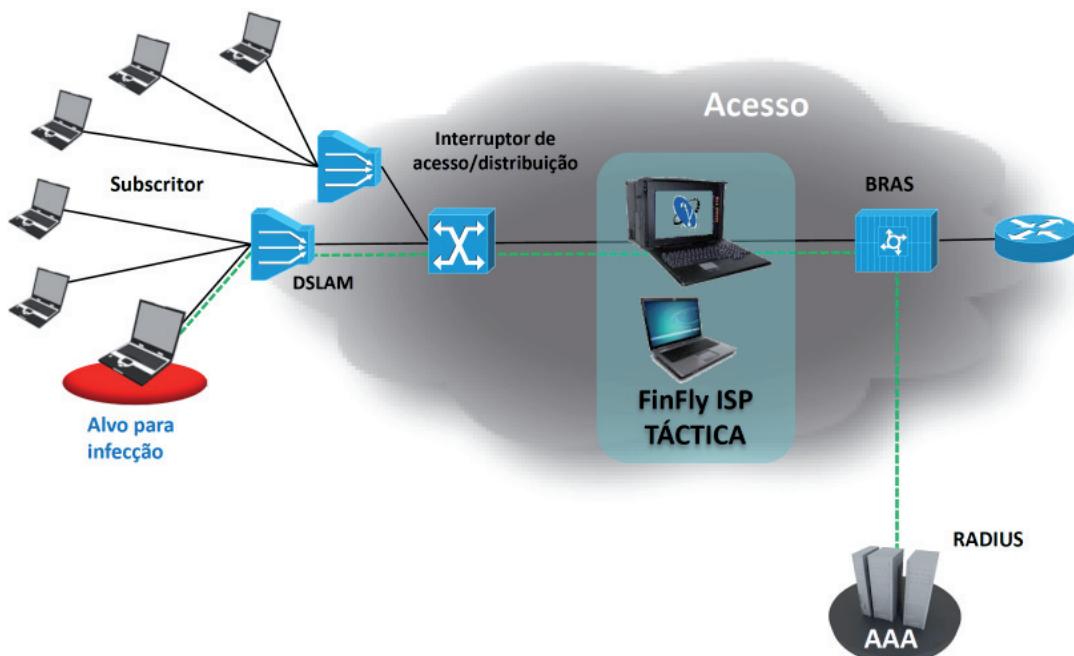
Claro que é possível combinar soluções tácticas e estratégicas para atingir um máximo de flexibilidade para as operações de infecção.

### Configuração da rede

#### Disposição estratégica



#### Disposição táctica



### Componentes Do Produto

#### FinFly ISP Strategic

Uma colocação estratégica de FinFly ISP que consiste, pelo menos, no seguinte:

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

Servidores FinFly ISP Estação de trabalho	FinFly ISP HP Série Z
HP ProLiant Série DL G7 Estação de trabalho empresarial	
	

<b>Rendimento</b>	> 20 Gbps
<b>Nº máx. de NIC:</b>	2-8 NIC
<b>Interfaces:</b>	1 GE Cobre / Fibra 10 GE Cobre / Fibra SONET/SDH OC-3 / -192 STM-1 / -64 ATM AAL5
<b>Procesadores:</b>	Intel XEON 1x – 8x
<b>Núcleo</b>	2 – 8 núcleos / procesador
<b>RAM:</b>	12 GB – 1 TB
<b>Capacidade disco duro:</b>	SAS 146GB – 4.8TB de 3x
<b>Funcionalidades</b>	HP iLO 3 Potência redundante Ventiladores redundantes Função de interruptor de bypass (se aplicável)
<b>Sistema operativo</b>	Linux GNU (Debian 5.0) reforçado

#### FinFly ISP Táctica

Un sistema FinFly ISP táctico consta de lo siguiente:

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

FinFly ISP Táctica Gestão portátil	FinFly ISP Táctica
Atlas A9 17" Portable	Lenovo Thinkpad Série T
	

Os dados técnicos/especificações estão sujeitos a alterações sem aviso prévio.

<b>Rendimento</b>	5 Gbps
<b>Nº máx. de NIC:</b>	3 NIC
<b>Interfaces:</b>	1GE Cobre / Fibra SONET/SDH OC-3 / -12 STM-1 / -4 ATM AAL5
<b>Procesadores:</b>	2 Intel Core i7
<b>Núcleo</b>	6 núcleos / procesador
<b>RAM:</b>	12 GB
<b>Capacidad disco duro:</b>	2 SATA de 1 TB
<b>Unidad óptica</b>	DVD+/-RW SATA
<b>Monitor</b>	1 x 17" TFT
<b>Funcionalidades</b>	Função de interruptor de bypass para NICs
<b>Sistema operativo</b>	Linux GNU (Debian 5.0) reforçado

### FinSupport

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

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

- Acesso online a:
  - Manual do Utilizador mais recente
  - Especificações do produto mais recentes
  - Slides de formação do produto mais recentes
  - Atendimento para relato de problemas
  - Atendimento para solicitação de funcionalidades
- Actualizações regulares do software:
  - Correcção de problemas
  - Novas funcionalidades
  - Novas versões principais
- Suporte técnico através de Skype:
  - Correcção 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 FinFisher™ e substituições do hardware ao abrigo da garantia. Além disso, com o FinLifelineSupport, o cliente recebe automaticamente novas funcionalidades com a edição padrão de correcção de problemas.

### Correcção de problemas

O FinSupport é uma organização de suporte orientado por produto, em que um gestor de suporte pós-venda altamente experiente recebe perguntas relacionadas por e-mail ou telefone. O gestor de suporte pós-venda está sediado na Alemanha e o seu horário de funcionamento é das 09:00 às 17:00, CET (Central European Time - Hora da Europa Central).

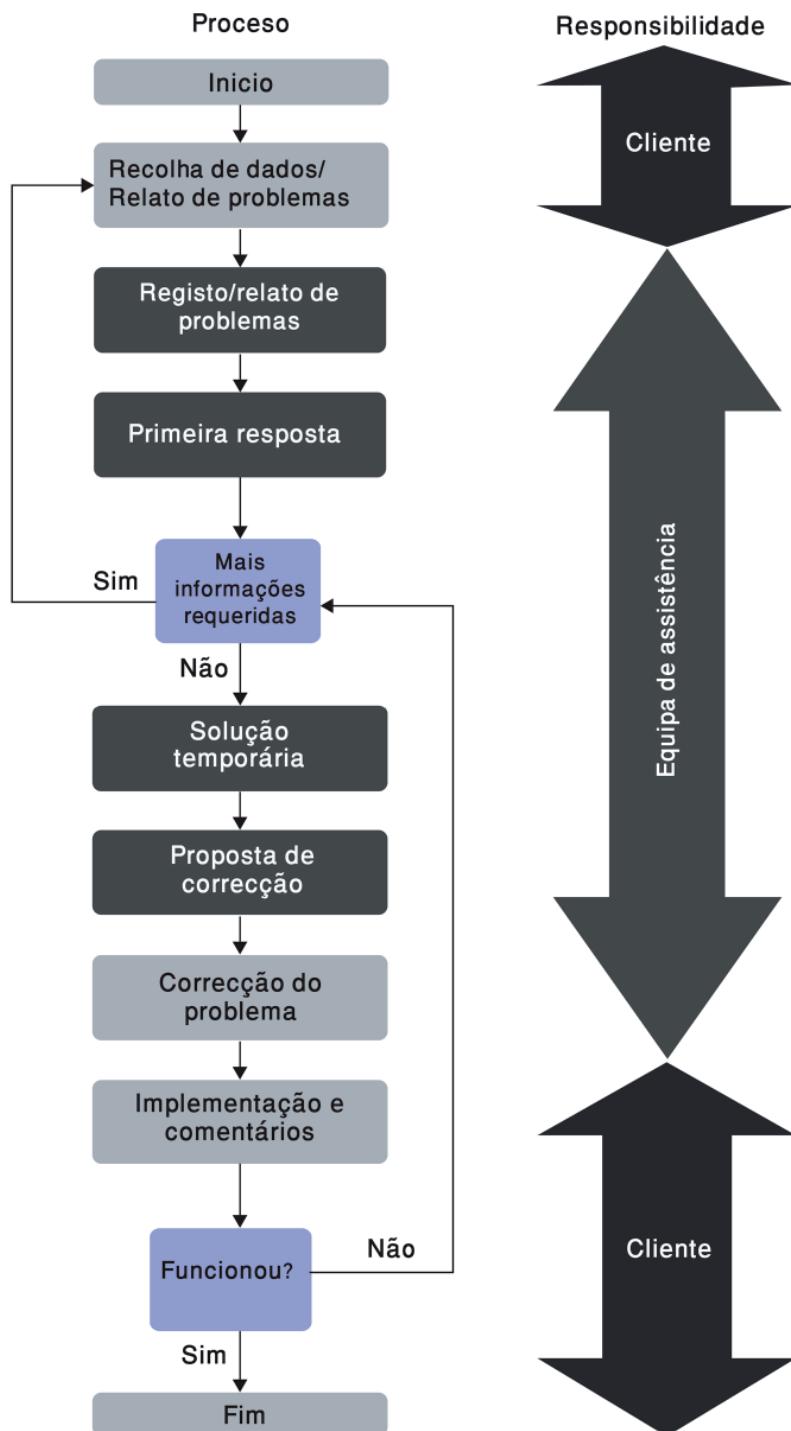
Com o FinLifelineSupport, a assistência está disponível das 09:00 às 17:00, CET. Se um pedido de assistência for registado fora das horas normais de expediente, será endereçado imediatamente para o dia útil seguinte.

Quando o cliente relata um incidente, registamos um IR (Incident Report - Relatório de incidente) e documentamos a prioridade do incidente. Dentro de um período especificado, seguir-se-ão acções de correcção com base na prioridade atribuída. A equipa do FinFisher™ tem, então, a responsabilidade de coordenar a investigação e a resolução do IR, bem como a comunicação do estado e as novas informações ao originador do IR.

Para questões de alta prioridade, garantimos que o sistema continua a funcionar sem problemas, fornecendo rapidamente soluções e correcções testadas de problemas. Quando a equipa do FinFisher™ fornece uma solução, é remetido simultaneamente o PR (Problem Report - Relatório do problemas) para o departamento R&D (Research and Development - Pesquisa e Desenvolvimento) para garantir uma solução rápida. Estas medidas de suporte profissionais garantem que o software satisfaz as mais elevadas expectativas.



O fluxograma seguinte fornece uma ilustração do procedimento operacional típico e das áreas de responsabilidade (**Nota:** Neste fluxograma, o “cliente” representa o originador do IR):



# Controlo Remoto E Soluções De Infecção

**FIN SUPPORT**

A tabela seguinte fornece o procedimento normal de tratamento de incidentes do cliente:

Cliente	Processamento e tarefas do IR (Incident Report)
	O FinFisher™ possui contactos dedicados por e-mail e linha directa de telefone/fax para relatar incidentes.
No caso de um defeito (suspeição) de hardware/software, recebe o IR (Incident Report) de acordo com os métodos de comunicação definidos.  O IR deve incluir: - ID do contrato - Nome do cliente - Sistema/tecnologia afectado - Descrição do defeito - Prioridade (consulte a definição abaixo) - Sintomas do erro disponíveis	
O cliente coopera, fornecendo mais sintomas do erro mediante solicitação	No prazo de um dia de trabalho, o cliente recebe um número de ticket para confirmar a recepção e controlar o IR e, também, os resultados da análise inicial
	O FinLifelineSupport suporta a recolha de sintomas de erro, mediante solicitação
	O FinLifelineSupport ajuda com soluções temporárias
	O FinLifelineSupport fornece propostas de correcção para o IR, com medidas de correcção planeadas e tempo de resposta, após a análise do incidente
	O FinLifelineSupport proporciona questões de modificação do hardware ou software, se o incidente relatado necessitar de correcção
O cliente implementa a modificação fornecida do hardware/software. O cliente confirma a correcção com êxito.	O FinLifelineSupport ajuda na implementação da modificação do hardware <sup>(i)</sup> /software

- (i) O hardware adquirido separadamente não está sob garantia.



### Definições de consulta e prioridade de falhas

O FinLifelineSupport processa as consultas recebidas e os relatórios de problemas de acordo com a sua urgência. Dois factores classificam a urgência de um incidente, e ambos estão incluídos em cada IR:

- “Prioridade” baseada apenas no âmbito técnico do erro
- A “Gravidade do cliente” é um factor mais objectivo e baseia-se no impacto resultante do cliente

A tabela de “Prioridade” seguinte fornece uma visão geral do âmbito técnico correspondente:

Prioridade	Definição	Exemplo
1	Questão crítica: Aspecto crucial do sistema que não está a funcionar	O Proxy está em baixo e não pode ser estabelecida qualquer comunicação com o FinSpy alvo.
2	Questão principal sem solução	Uma actualização do antivírus detecta um RMS já instalado que requer uma actualização imediata para permanecer operacional no sistema infectado.
3	Questão principal com solução	A funcionalidade FinSpy alvo não funciona correctamente, mas pode ser corrigida com uma solução.
4	Questão menor com pouco impacto no sistema	Ícone incorrecto mostrado para um ficheiro descarregado

### Tempos de resposta

Em 90% de todos os incidentes, manteremos os nossos tempos de resposta conforme ilustrado na tabela abaixo.

“Dias de trabalho” = Conforme definido no calendário alemão, ficando, assim, excluídos os feriados existentes na Alemanha.

Existem três fases nos nossos tempos de resposta:

- Resposta inicial
- Feedback da acção de correção
- Resolução do problema (ou desagravamento da prioridade)

O tempo para a “Resposta inicial” é a partir do momento em que registamos um incidente até à resposta de confirmação actual enviada para o cliente que recebe o aviso de recepção do incidente.

A “Resposta inicial” também pode solicitar informações mais detalhadas ou, em casos menos complexos, pode resolver imediatamente o problema.

# Controlo Remoto E Soluções De Infecção

**FIN SUPPORT**

Tempos de resposta	Resposta inicial	Feedback da acção de correcção	Resolução do PROBLEMA/Desagravamento da PRIORIDADE
Prioridade 1 - questão crítica	Mesmo dia útil	1 dia útil	2 dias úteis Nota: Dependendo do problema e da pesquisa requerida, pode ser necessário mais tempo para resolver o problema.
Prioridade 2 - Questão principal sem solução	Mesmo dia útil	2 dias úteis	5 dias úteis Nota: Dependendo do problema e da pesquisa requerida, pode ser necessário mais tempo para resolver o problema.
Prioridade 3 - Questão principal com solução	Mesmo dia útil	3 dias úteis	14 dias úteis Nota: Dependendo do problema e da pesquisa requerida, pode ser necessário mais tempo para resolver o problema.
Prioridade 4 - questão menor	Mesmo dia útil	7 dias úteis	Actualização seguinte do 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).



# Programa De Formação De Intrusão De TI

**FINTRAINING**



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

# Programa De Formação De Intrusão De TI

FINTRAINING

A consciencialização da segurança é **essencial para qualquer Governo**, de modo a manter a segurança da TI e a **evitar ameaças** com sucesso contra a infra-estrutura de TI, o que pode resultar numa perda de confidencialidade, integridade e disponibilidade de dados.

Por outro lado, tópicos como **Ciber-guerra**, Intercepção Activa e Recolha de Informações de Serviços Secretos através da **intrusão de TI** tornam-se cada vez mais importantes, e requerem que os governos **criem equipas de intrusão TI** para **enfrentarem estes novos desafios**.

Os cursos FinTraining são ministrados por **especialistas de intrusão de TI de nível mundial**, e apoiam-se em **cenários totalmente práticos**, centralizados em **operações da vida real**, conforme requerido pelo utilizador final para resolver os seus **desafios diários**.

A **Cobham** combina os cursos de formação individual num **programa de formação profissional e consultoria** 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. Para garantir a total aplicação dos conhecimentos transferidos, **o suporte operacional do país** é fornecido durante o programa.

## Alguns Temas do Curso

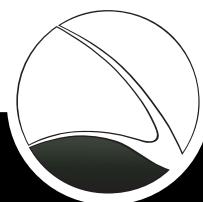
- Definición de perfiles de sitios web y personas objetivo
- Seguimiento de correos electrónicos anónimos
- Acceso remoto a cuentas de correo Web
- Evaluación de seguridad de servidores y servicios web
- Explotación práctica de software
- Intrusión de TI inalámbrica (WLAN/802.11 y Bluetooth)
- Ataques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

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

## Programa de consulta

- Programa de **Formação e consultoria** de intrusão total de TI
- Criação estruturada e **Formação da equipa de intrusão de TI**
- **Avaliação total dos membros da equipa**
- Sessões práticas de formação centralizadas em **Operações da Vida Real**
- Consultoria operacional no país

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



**FINFISHER™**  
IT INTRUSION



GAMMA INTERNATIONAL  
United Kingdom

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

[info@gammagroup.com](mailto:info@gammagroup.com)

**WWW.GAMMAGROUP.COM**