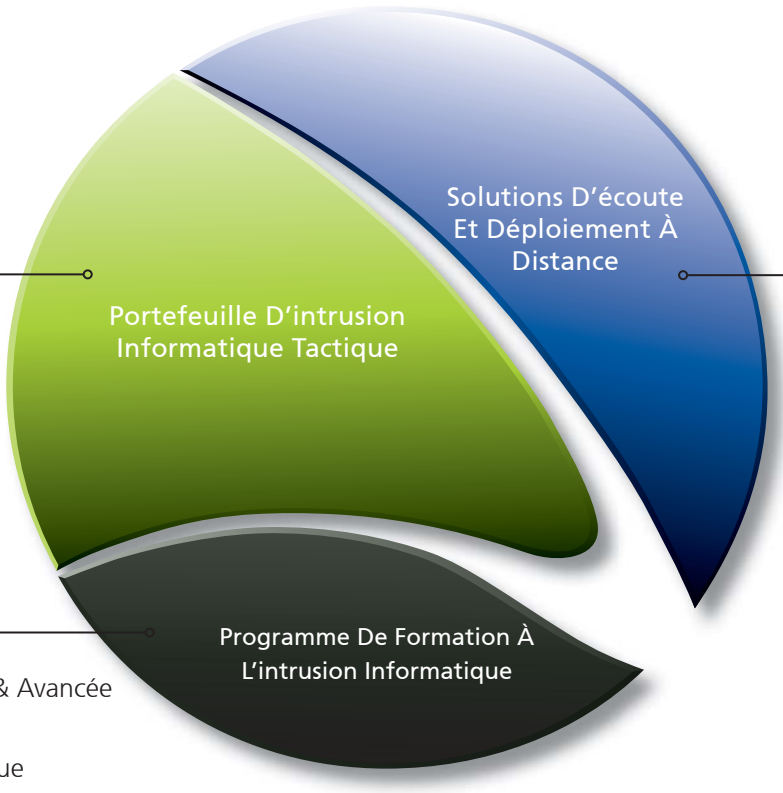
FINFISHER™ : Solutions D'intrusion Informatique et D'écoute à Distance Pour les Gouvernements

WWW.FINFISHER.COM

FINFISHER™
IT INTRUSION



- Kit FinIntrusion
- Suite FinUSB
- FinFirewire

FinSpy
- FinSpy
- FinSpy Mobile

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

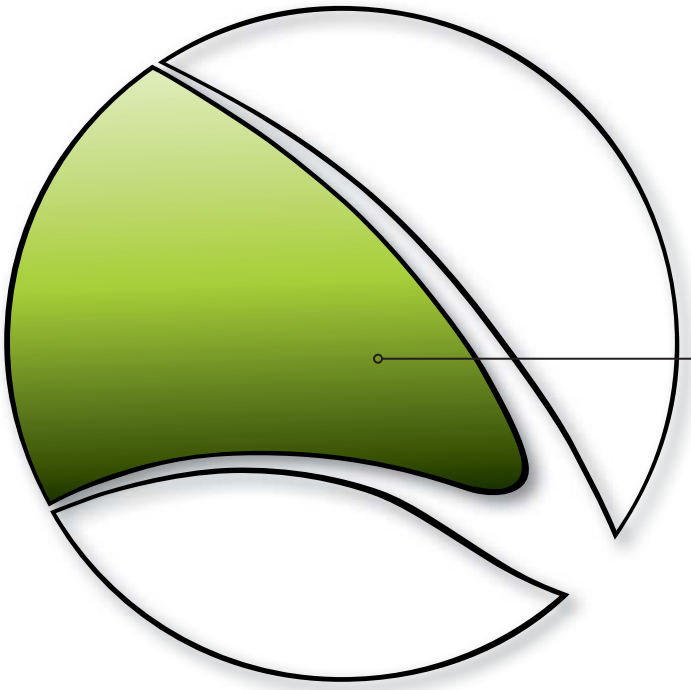
- Intrusion Basique & Avancée
- Intrusion sans fil
- Exploitation Pratique
- Pénétration d'applications web
- Formation et conseil personnalisés en intrusion informatique

PORTEFEUILLE D'INTRUSION INFORMATIQUE TACTIQUE

LE KIT **FIN**INTRUSION

LA SUITE **FIN**USB

FINFIREWIRE



Gamma participe activement au développement de solutions d'intrusion informatique pour améliorer continuellement les capacités de ses clients. Des solutions et des techniques de haut niveau faciles à utiliser viennent compléter le savoir-faire de la communauté du renseignement pour donner une réponse pertinente aux défis de l'intrusion sur un plan tactique.

FINFISHER™
IT INTRUSION

WWW.FINFISHER.COM

Le KIT **FIN**INTRUSION

Le kit FinIntrusion a été conçu et développé par les meilleurs spécialistes mondiaux de l'intrusion informatique, revendiquant plus de 10 ans d'expérience dans leur domaine, et ayant collaboré à plusieurs « Tiger Teams » (Red Teams) dans le secteur privé et gouvernemental, pour évaluer la sécurité de différents réseaux et organisations.

FinIntrusion est un Kit opérationnel **secret et à jour** pouvant être utilisé pour les **opérations d'intrusion informatique** les plus courantes, que ce soit dans les domaines défensifs ou offensifs. Les clients actuels sont les **services de guerre électronique de l'armée, les agences de renseignement, les renseignements généraux et les forces de l'ordre.**

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations stratégiques/ tactiques**
Capacités:	· **Décode le cryptage WEP/WPA** · **Surveillance des réseaux (y compris les sessions SSL)** · **Attaques par intrusion informatique**
Contenu:	· **Matériel/Logiciel**

Exemple d'utilisation 1 : Unité de surveillance technique

Le kit FinIntrusion a été utilisé pour décoder **le cryptage WPA** du réseau sans fil au domicile d'une cible, puis de surveiller les identifiants de ses comptes **webmail (Gmail, Yahoo…) et de ses réseaux sociaux (Facebook, MySpace…)**, ce qui a permis aux enquêteurs de les **surveiller à distance** depuis le QG, sans avoir à être à proximité de la cible.

Exemple d'utilisation 2 : Sécurité informatique

Plusieurs clients ont utilisé le kit FinIntrusion pour **contourner avec succès la sécurité** de réseaux et de systèmes informatiques à des fins **offensives et défensives** en utilisant divers outils et techniques.

Exemple d'utilisation 3 : Cas d'utilisation stratégiques

Le kit FinIntrusion est largement utilisé pour accéder à distance aux comptes de messagerie et aux serveurs web de la cible, et ainsi surveiller leur activité (journaux d'accès, etc.).

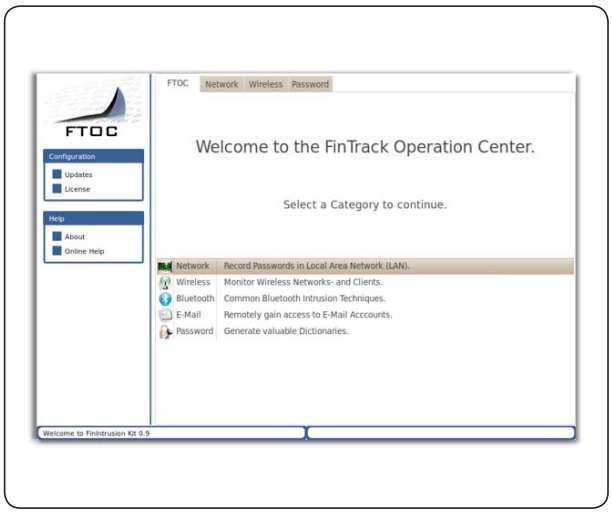
Présentation des fonctionnalités

- Découvre **les réseaux sans fil (802.11) et les appareils Bluetooth®**
- Retrouve les phrases de passe WEP (64 et 128 bits) **en 2 à 5 minutes**
- **Casse les phrases de passe WPA1 et WPA2** avec des attaques par dictionnaire
- Écoute activement le réseau local (avec ou sans fil), et **extrait les comptes et mots de passe, y compris pour les sessions cryptées TLS/SSL**
- **WiFi Catcher intégré** pouvant être combiné avec **des fonctionnalités de surveillance de mots de passe**
- **Pénètre à distance dans les comptes de messagerie** en utilisant des techniques d'intrusion réseau, système et au niveau des mots de passe
- **Évaluation et validation de la sécurité des réseaux**

Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

Le KIT **FIN**INTRUSION

Composants du produit



Le kit FinIntrusion – Unité Tactique Secrète

Componentes básicos para la intrusión de TI :

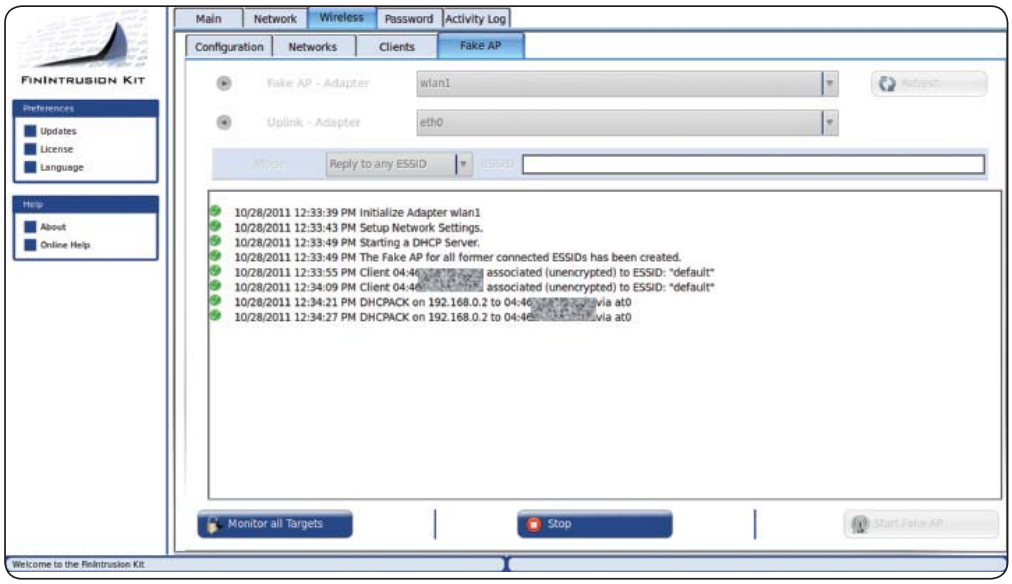
- Adaptateur WLAN haute puissance
- Adaptateur Bluetooth haute puissance
- Antennes 802.11
- Nombreux appareils courants d'intrusion informatique

Centre opérationnel FinTrack

- Interface utilisateur graphique pour l'automatisation des attaques par intrusion informatique

WiFi Catcher

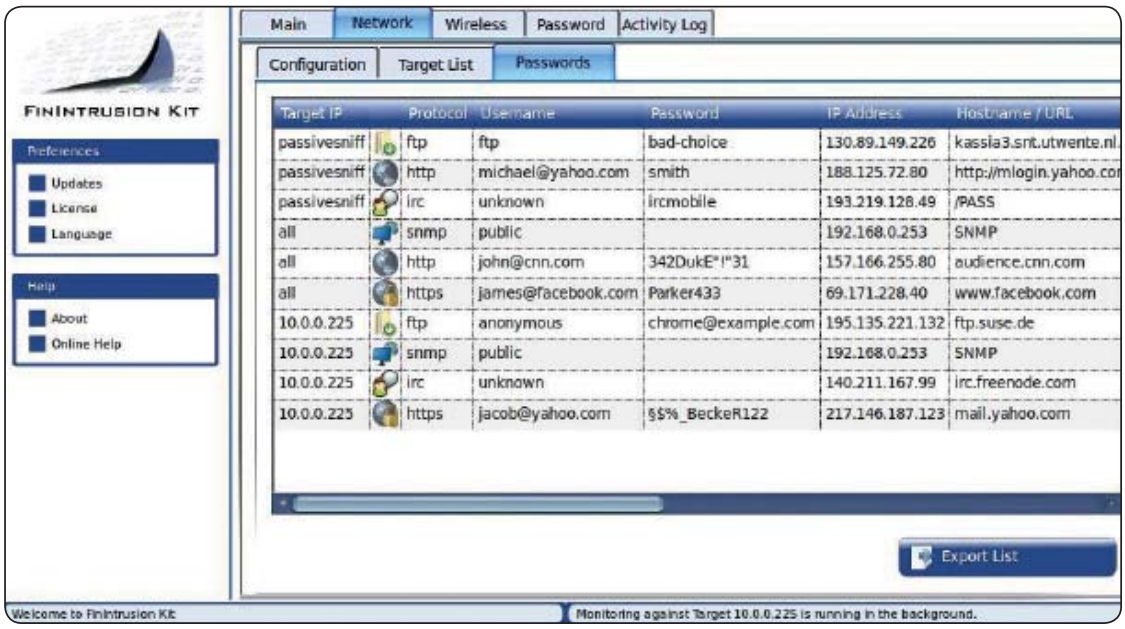
- Accroche les appareils WLAN à proximité, et enregistre le trafic et les mots de passe.



Le KIT **FIN**INTRUSION

Renifleur de mots de passe actifs LAN/WLAN

· Capture également les données cryptées SSL comme le webmail, les portails vidéo, les opérations de banque en ligne, etc.



GAMMAGROUP
GAMMA INTERNATIONAL
Royaume Uni

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

La SUITE **FIN**USB

La Suite FinUSB est un produit flexible qui permet aux forces de l'ordre et aux agences de renseignement d'extraire rapidement et en toute sécurité des informations forensiques à partir des systèmes informatiques sans avoir besoin de faire appel à des agents familiarisés avec l'informatique.

Elle a été utilisée dans le monde entier lors d'opérations réussies (secrètes ou à découvert) où ont été obtenus des renseignements précieux sur des cibles.

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations tactiques**
Capacités:	· **Collecte d'informations** · **Accès système** · **Forensique rapide**
Contenu:	· **Matériel/Logiciel**

Exemple d'utilisation 1 : Opération secrète

Une clé USB FinUSB a été donnée à une source au sein d'un Groupe Criminel Organisé (GCO). Celle-ci a extrait secrètement des authentifiants de compte web et e-mail ainsi que des documents Microsoft Office des systèmes cibles, pendant que le GCO utilisait le périphérique USB pour **échanger des fichiers standard** comme de la musique, des vidéos ou des documents Office.

Une fois le périphérique USB rapporté au QG, les données rassemblées ont pu être décryptées et analysées, puis utilisées pour écouter le groupe à distance.

Exemple d'utilisation 2 : Unité de surveillance technique

Une Unité de Surveillance Technique (UST) suivait une cible qui, changeant régulièrement de cybercafé, rendait inefficace la technique du cheval de Troie pour la surveillance. FinUSB a été utilisé pour extraire, après le départ de la cible, les **données laissées sur les terminaux publics** qu'elle avait utilisés.

Il a ainsi été possible de récupérer plusieurs documents que la cible avait ouverts dans son webmail. Les informations recueillies comprenaient, entre autres, des fichiers Office importants ainsi que l'historique de navigation trouvé par analyse des cookies.

Présentation des fonctionnalités

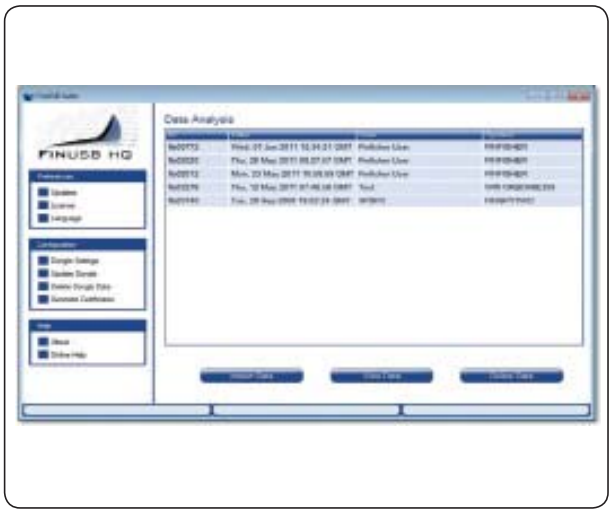
- Optimisé pour **les opérations secrètes**
- Utilisation facilitée par **exécution automatisée**
- Extraction des noms et **des mots de passe des utilisateurs** pour tous les logiciels courants, par exemple:
  - Clients de messagerie
  - Messageries instantanées
  - Navigateurs
  - Navigateurs
- **Copie silencieuse de fichiers** (disques de recherche, corbeille, dernière ouverture/modification/création)
- Extraction **d'informations réseau** (journaux de chat, historique de navigation, clés WEP/WPA(2)...)
- Compilation **d'informations système** (logiciels installés / en cours d'exécution, informations sur le disque dur...)

Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

La SUITE **FIN**USB

Composants du produit

Suite FinUSB - Unité mobile



FinUSB HQ

- IHM pour décrypter et analyser les données recueillies
- Configurez les options de fonctionnement de la clé USB

Clé USB 10 FinUSB (U3 - 16 Go)

- Extrait secrètement les données d'un système

FinUSB – Contournement du mot de passe Windows

- Contourne la connexion à Windows sans modifications permanentes du système

La SUITE **FIN**USB

Facilité d'utilisation

1. Prenez une clé USB FinUSB

2. Configurez toutes les fonctionnalités/modules requis, et mettez à jour votre clé FinUSB avec FinUSB HQ

3. Allez sur votre système cible

4. Branchez votre clé FinUSB

5. Attendez que toutes les données soient transférées

6. Revenez dans votre FinUSB HQ

7. Importez toutes les données de la clé FinUSB

8. Générez un rapport

Rapports professionnels

GAMMAGROUP
GAMMA INTERNATIONAL
Royaume Uni

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

FINFIREWIRE

Les Unités de Surveillance Technique et les experts forensiques sont souvent confrontés à des situations où ils ont besoin d'accéder à un système informatique en fonctionnement, sans l'arrêter pour éviter toute perte de données ou gagner un temps précieux lors d'une opération. Dans la plupart des cas, le système cible est protégé par un **économiseur d'écran avec mot de passe**. Il arrive aussi que l'utilisateur cible ne soit pas connecté et que **l'écran de connexion** soit actif.

FinFireWire permet à l'opérateur de contourner rapidement et discrètement **la protection de l'écran par mot de passe,** et d'accéder au système cible sans laisser de traces ni altérer des preuves forensiques importantes.

INFORMATIONS RAPIDES

Utilisation:	· **Opérations tactiques**
Capacités:	· **Contourne le mot de passe utilisateur** · **Accède secrètement au système** · **Récupère les mots de passe en RAM** · **Permet l'analyse forensique en direct**
Contenu:	· **Matériel/Logiciel**

Exemple d'utilisation 1 : Opération forensique

Une **unité forensique** s'est introduite dans l'appartement d'une cible, et a tenté d'accéder au système informatique. L'ordinateur était **allumé mais son écran était verrouillé**. Comme ils n'avaient pas le droit (pour des raisons légales) d'utiliser une solution d'écoute à distance, ses agents auraient **perdu toutes les données** s'ils éteignaient le système, parce que le **disque dur était entièrement crypté**. FinFireWire a été utilisé pour **déverrouiller le système cible à chaud**. L'agent a ainsi pu **copier tous les fichiers** de l'ordinateur, avant de mettre celui-ci hors tension et de le ramener au QG.

Exemple d'utilisation 2 : Récupération de mots de passe

En combinant le produit avec des **applications forensiques** traditionnelles comme EnCase®, les unités forensiques ont utilisé la **fonctionnalité d'image mémoire RAM** pour réaliser un instantané des informations actuellement en RAM. Elles ont également **récupéré la phrase de passe utilisée** par TrueCrypt pour crypter le disque dur.

Présentation des fonctionnalités

- **Déverrouille la connexion utilisateur** pour chaque compte utilisateur
- Déverrouille **tout économiseur d'écran protégé par mot de passe**
- **Effectue une image mémoire complète** pour l'analyse forensique
- Permet la forensique en direct du système cible **sans le redémarrer**
- Le mot de passe de l'utilisateur n'est **pas modifiéd**
- Compatible avec **Windows, Mac OSX et Linux**
- Fonctionne avec **FireWire/1394, PCMCIA et Express Card**

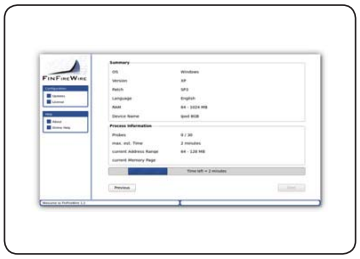
Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

FINFIREWIRE

Composants du produit

FinFireWire – Unité Tactique

· Système tactique complet



Interface utilisateur cliquer-pointer

· Interface utilisateur facile à utiliser

Cartes d'interface de connexion

· Carte d'interface PCMCIA et Express-Card pour les systèmes cibles ne disposant pas de port FireWire

Jeu de câbles universel FinWire

· 4 broches vers 4 broches
· 4 broches vers 6 broches
· 6 broches vers 6 broches

Utilisation

1. Allez sur votre système cible

2. Lancez FinFireWire

3. Branchez l'adaptateur et le câble FireWire

4. Sélectionnez une cible

5. Attendez que le système soit déverrouillé

GAMMAGROUP

GAMMA INTERNATIONAL
Royaume Uni

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

Solutions D'écoute Et De Déploiement À Distance

FINSPY

FINSPY MOBILE

FINFLY USB

FINFLY LAN

FINFLY WEB

FINFLY EXPLOIT PORTAL

FINFLY ISP

FINFLY NET

Les solutions d'écoute et d'infection à distance sont utilisées pour accéder aux systèmes cibles et donner un accès complet aux informations stockées. Elles permettent également de prendre le contrôle des fonctions des systèmes cibles, jusqu'à la collecte des données et des communications cryptées. En utilisation conjointe avec des méthodes sophistiquées d'infection, les agences gouvernementales seront capables d'infecter à distance les systèmes cibles.

FINFISHER™
IT INTRUSION

WWW.FINFISHER.COM

FINSPY

FinSpy est une solution d'écoute à distance éprouvée qui permet aux gouvernements de faire face aux défis actuels de **la surveillance des cibles mobiles et sensibilisées aux problématiques de sécurité**. Elles **changent régulièrement de lieu**, utilisent des canaux de **communication cryptés et anonymes**, et **résident dans des pays étrangers**.

Les solutions habituelles d'interception légale **doivent répondre à de nouveaux défis** qui ne peuvent être **résolus qu'à l'aide de systèmes actifs** comme FinSpy :

- Données transmises sur aucun réseau
- Communications cryptées
- Cibles situées dans des pays étrangers

FinSpy a **fait ses preuves** lors d'opérations dans le monde entier **depuis plusieurs années**. Des renseignements précieux ont été recueillis sur des personnes et des organisations cibles.

Quand FinSpy est installé sur un système informatique, il est possible **d'y accéder et de le contrôler à distance** dès qu'il est connecté à Internet ou au réseau, **quel que soit l'endroit dans le monde** où se trouve le système cible.

Descripción General De Funciones

Ejemplos de funciones en el ordenador objetivo:

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

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations stratégiques/tactiques**
Capacités:	· **Écoute d'ordinateurs à distance** · **Écoute des communications cryptées**
Contenu:	· **Matériel/Logiciel**

Exemple d'utilisation 1 : Agence de renseignement

FinSpy a été installé sur plusieurs systèmes informatiques de **cybercafés situés dans des secteurs critiques**, afin d'y surveiller toute activité suspecte et, plus particulièrement, les **communications Skype** avec des personnes à l'étranger. Grâce à la webcam, des photos des cibles ont été prises pendant qu'elles utilisaient le système.

Exemple d'utilisation 2 : Crime organisé

FinSpy a été **secrètement déployé sur les systèmes** cibles de plusieurs membres d'un Groupe Criminel Organisé. En utilisant **la traçabilité du pays et l'accès à distance aux microphones**, des renseignements précieux ont pu être recueillis à partir de **chacune des réunions tenues** par ce groupe.

QG - Exemple de fonctionnalités :

- Protection des preuves (preuves valables conformément aux **normes européennes**)
- **Gestion des utilisateurs** en fonction des authentifiants de sécurité
- Caché au public grâce à des **proxies d'anonymisation**
- Peut être **entièrement intégré** à la fonctionnalité d'écoute LEMF (Law Enforcement Monitoring Functionality)

Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

Composants du produit

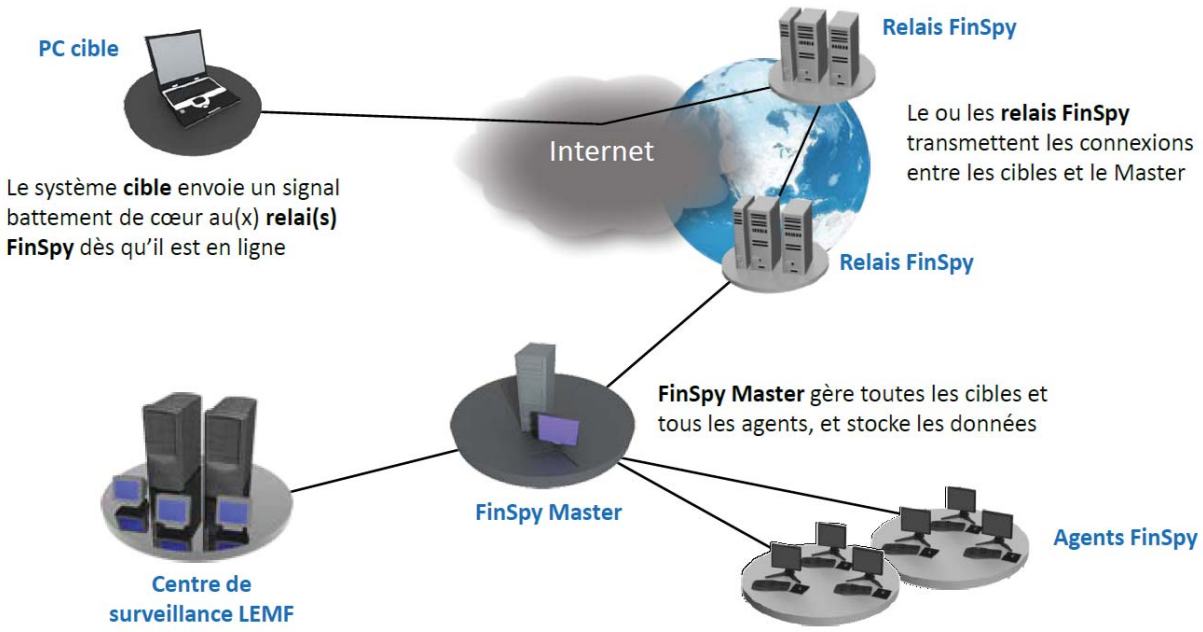
FinSpy Master et Proxy

- Contrôle total des systèmes cibles
- Protection des preuves pour les données et les journaux d'activité
- Stockage sécurisé
- Gestion des utilisateurs et des cibles à base d'habilitations de sécurité

FinSpy Agent

- Interface utilisateur graphique pour les sessions en direct
- Configuration et analyse des données des cibles

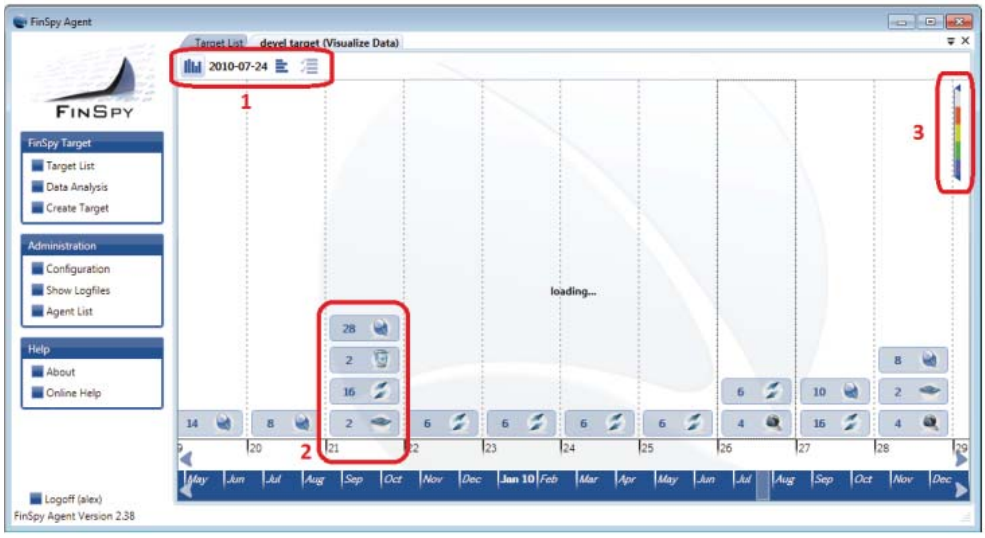
Accès aux systèmes informatiques cibles dans le monde entier



Interface utilisateur facile à utiliser

Configuration de la cible en direct et hors ligne

Renseignements complets sur le système cible



1. Affichage de données multiples
2. Analyse de données structurées
3. Niveaux d'importance pour tous les fichiers enregistrés

GAMMAGROUP

GAMMA INTERNATIONAL
Royaume Uni

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

FINSPY MOBILE

FinSpy Mobile résout les problèmes rencontrés par les gouvernements en matière de capacités d'interception sur les principales **plateformes de smartphones**.

En particulier, des organisations **sans capacités d'interception réseau ou hors antenne** peuvent avoir de meilleures capacités à accéder aux téléphones portables et les intercepter. De plus, cette solution permet **d'accéder aux communications cryptées** ainsi qu'aux **données stockées dans les appareils** et non transmises.

Les solutions habituelles d'interception tactique ou stratégique **doivent répondre à des défis** qui ne peuvent être **résolus qu'à l'aide de systèmes offensifs** comme FinSpy Mobile :

- Données conservées dans l'appareil et transmises sur aucun réseau
- Communications cryptées dans l'interface hertzienne, qui évitent l'utilisation de systèmes hors antenne actifs ou passifs tactiques
- Cryptage de bout en bout depuis l'appareil (ex. : messages PIN, mails, messageries instantanées...)

FinSpy Mobile a répondu efficacement aux attentes des agences gouvernementales qui collectent des renseignements **à distance sur des téléphones portables cibles**.

Lorsque FinSpy Mobile est installé sur un téléphone portable, la cible peut être **contrôlée et surveillée à distance**, où qu'elle se trouve dans le monde.

INFORMATIONS RAPIDES

Utilisation :	· **Opérations stratégiques/ tactiques**
Capacités :	· **Surveillance des téléphones portables à distance**
Contenu:	· **Matériel/Logiciel**

Exemple d'utilisation 1 : Agence de renseignement

FinSpy Mobile a été déployé sur les **téléphones portables BlackBerry** de plusieurs cibles pour surveiller leurs communications, notamment **les SMS/MMS, le mail et la messagerie instantanée BlackBerry**.

Exemple d'utilisation 2 : Crime organisé

FinSpy Mobile a été **secrètement déployé sur les téléphones portables** de plusieurs membres d'un Groupe Criminel Organisé. Grâce aux données de **suivi GPS** et aux **appels silencieux**, des renseignements précieux ont pu être recueillis à partir de **chacune des réunions tenues** par ce groupe.

Présentation des fonctionnalités

Téléphone cible - Exemple de fonctionnalités :

- **Communications secrètes** avec le QG
- Enregistrement des **communications standard** comme les appels vocaux, SMS/MMS et les mails
- **Surveillance en direct** par appels silencieux
- **Téléchargement de fichiers** (contacts, calendrier, images, fichiers)
- **Traçabilité du pays** de la cible (GPS et Identifiant de cellule)
- Enregistrement complet de toutes **les communications de la messagerie BlackBerry**
- Prise en charge de la plupart des systèmes d'exploitation courants : **Windows Mobile/Phone, iOS (iPhone), BlackBerry OS, Android** et **Symbian**

QG – Exemple de fonctionnalités :

- Protection des preuves (preuves valables conformément aux **normes européennes**)
- **Gestion des utilisateurs** en fonction des habilitations de sécurité
- Caché au public grâce à des **Proxies D'Anonymisation**
- Peut être **entièrement intégré** à la fonctionnalité d'écoute LEMF (Law Enforcement Monitoring Functionality)

Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

FINSPY MOBILE

Composants du produit

FinSpy Master et Proxy

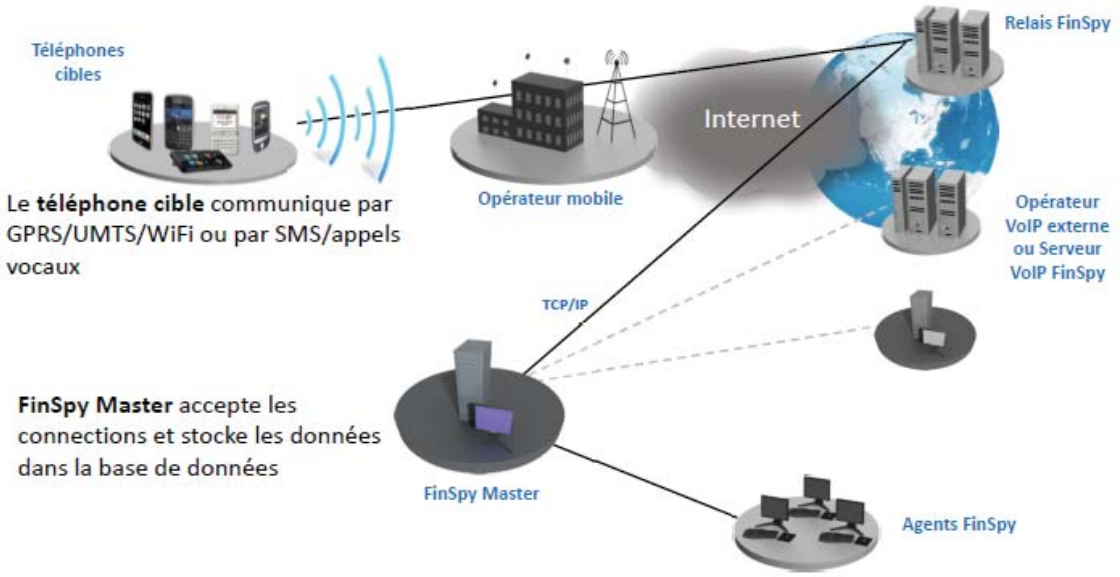
- Contrôle total des systèmes cibles
- Protection des preuves pour les données et les journaux d'activité
- Stockage sécurisé
- Gestion des utilisateurs et des cibles à base d'habilitations de sécurité

FinSpy Agent

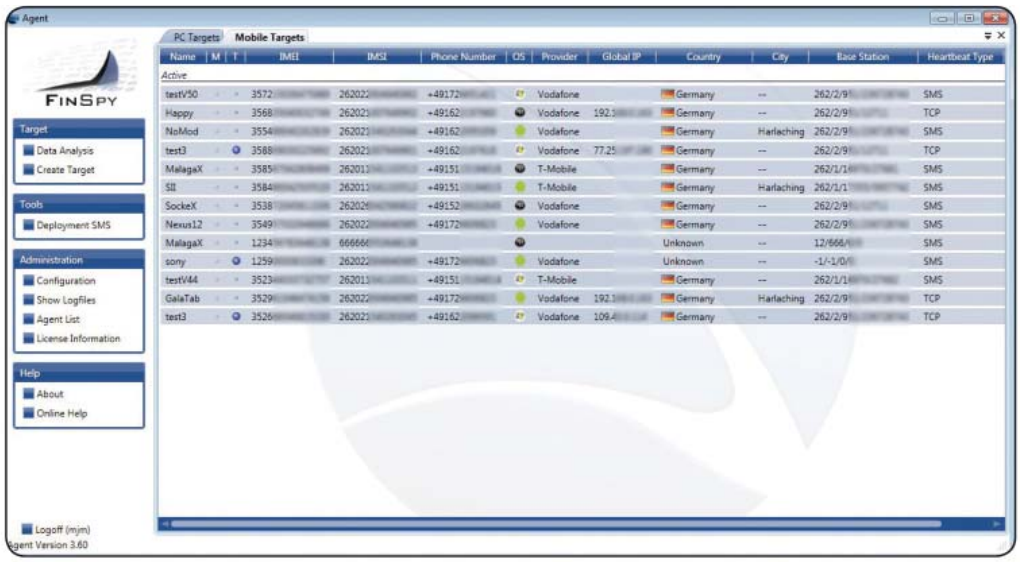
- Interface utilisateur graphique pour les sessions en direct
- Configuration et analyse des données des cibles

FINSPY MOBILE

Accès aux téléphones portables cibles dans le monde entier

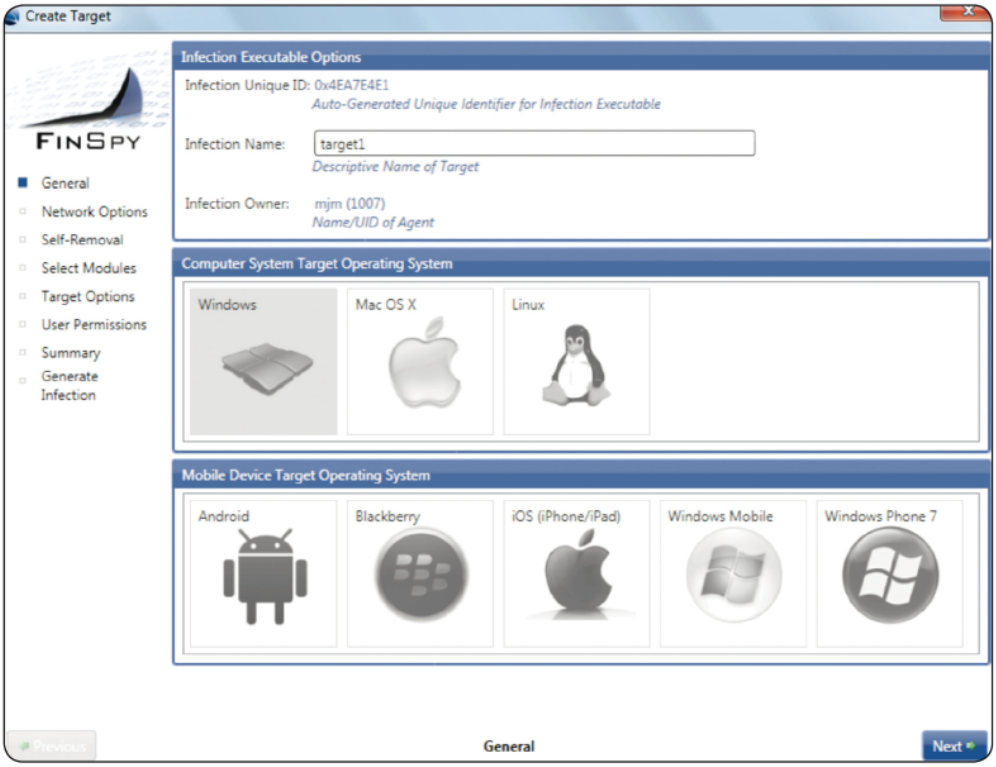


Interface utilisateur facile à utiliser



FINSPY MOBILE

Compatible avec toutes les plateformes mobiles courantes



GAMMAGROUP

GAMMA INTERNATIONAL
Royaume Uni

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

FINFLY USB

FinFly USB permet d'installer facilement et de façon fiable des solutions d'écoute à distance sur des systèmes informatiques quand l'accès physique est disponible.

Lorsque l'USB FinSpy est insérée dans l'ordinateur, celle-ci **installe automatiquement le logiciel configuré**. L'utilisateur interagit peu ou pas du tout lors de l'installation. Lorsque le logiciel est utilisé en opérations, **il ne nécessite pas que les agents soient familiarisés avec l'informatique**. FinFly USB peut être utilisé sur **plusieurs systèmes** avant d'être renvoyé au QG.

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations tactiques**
Capacités:	· **Déploie une solution d'écoute à distance sur la cible**
Contenu:	· **Matériel**

Exemple d'utilisation 1 : Unité de surveillance technique

Dans plusieurs pays, les **unités de surveillance technique** ont utilisé avec succès la clé USB FinFly pour déployer une solution d'écoute à distance sur des systèmes cibles **hors tension**, simplement en **démarrant ceux-ci via le périphérique USB FinFly**. Cette technique fonctionnait même sur des systèmes cibles avec un **cryptage activé sur la totalité du disque dur** avec des produits comme TrueCrypt.

Exemple d'utilisation 2 : Agence de renseignement

Une source au sein d'un groupe terroriste local a reçu une clé USB FinFly qui a **secrètement installé une solution d'écoute** à distance sur plusieurs ordinateurs du groupe alors qu'ils étaient en train d'utiliser le périphérique pour s'échanger des documents. Les systèmes cibles ont pu alors être **écoutés à distance depuis le QG**, et FinFly USB a ensuite été rendu par la source.

Présentation des fonctionnalités

- Déploiement possible même sur des **systèmes hors tension avec cryptage activé sur la totalité du disque dur** (ex. : TrueCrypt)
- **Installe secrètement la solution d'écoute à distance** lors de l'insertion dans le système cible
- Nécessite **peu ou pas d'interaction utilisateur**
- La fonctionnalité peut être **dissimulée en plaçant des fichiers classiques** comme de la musique, de la vidéo et des documents Officesur le périphérique
- Le matériel est un **périphérique USB standard et non suspect**

Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

FINFLY USB

Composants du produit

Périphériques USB FinFly

- Clé USB
- Déploie une solution d'écoute à distance sur des systèmes cibles
- Déploie une solution d'écoute à distance pendant le processus de démarrage

Intégration complète FinSpy

- Génération et activation automatique via l'agent FinSpy

GAMMAGROUP

GAMMA INTERNATIONAL
Royaume Uni

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

FINFLY LAN

L'un des défis majeurs pour les forces de l'ordre, ce sont les **Cibles Mobiles** pour lesquelles **L'accès Physique** Au Système Informatique **N'est Pas Possible**, et les cibles qui n'ouvrent pas de fichiers envoyés par e-mail sur leur compte.

En particulier, les cibles sensibilisées à la sécurité sont **presque impossibles à surveiller** parce qu'elles gardent leurs systèmes parfaitement à jour, et **aucun** « **exploit** » ou autre technique d'intrusion basique ne pourra fonctionner.

FinFly LAN a été conçu pour déployer secrètement une solution d'écoute à distance sur les systèmes cibles dans des réseaux locaux, avec ou sans fil (802.11). Il est capable de patcher à la volée les fichiers téléchargés par la cible, d'infecter la cible en envoyant des fausses mises à jour logicielles de logiciels courants ou encore **d'injecter la charge dans les sites Web visités.**

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations tactiques**
Capacités:	· **Déploie une solution d'écoute à distance sur le système cible dans le réseau local**
Contenu:	· **Logiciel**

Exemple d'utilisation 1 : Unité de surveillance technique

Une unité de surveillance technique suivait une cible depuis des semaines sans être en mesure d'accéder physiquement à l'ordinateur cible. Ils ont utilisé FinFly LAN pour installer la solution d'écoute à distance sur le système cible alors qu'elle utilisait un **hotspot public** dans un café.

Exemple d'utilisation 2 : Anti-corruption

FinFly LAN a été utilisé pour installer la solution d'écoute à distance sur l'ordinateur d'une cible pendant qu'elle utilisait celui-ci dans sa **chambre d'hôtel**. Les agents étaient dans une autre chambre. Ils se sont **connectés au même réseau**, et ont déclenché l'installation en manipulant les sites web que la cible était en train de visiter.

Présentation des fonctionnalités

- **Découvre tous les systèmes informatiques** connectés au réseau local
- Fonctionne dans des **réseaux avec et sans fil** (802.11)
- Peut être combiné avec le kit FinIntrusion pour un **accès secret au réseau**
- Cache la solution d'écoute à distance dans les **téléchargements des cibles**
- Injecte la solution d'écoute à distance sous la forme de **mises à jour logicielles**
- Installe la solution d'écoute à distance **via les sites web visités par la cible**

Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

FINFLY LAN

Composants du produit

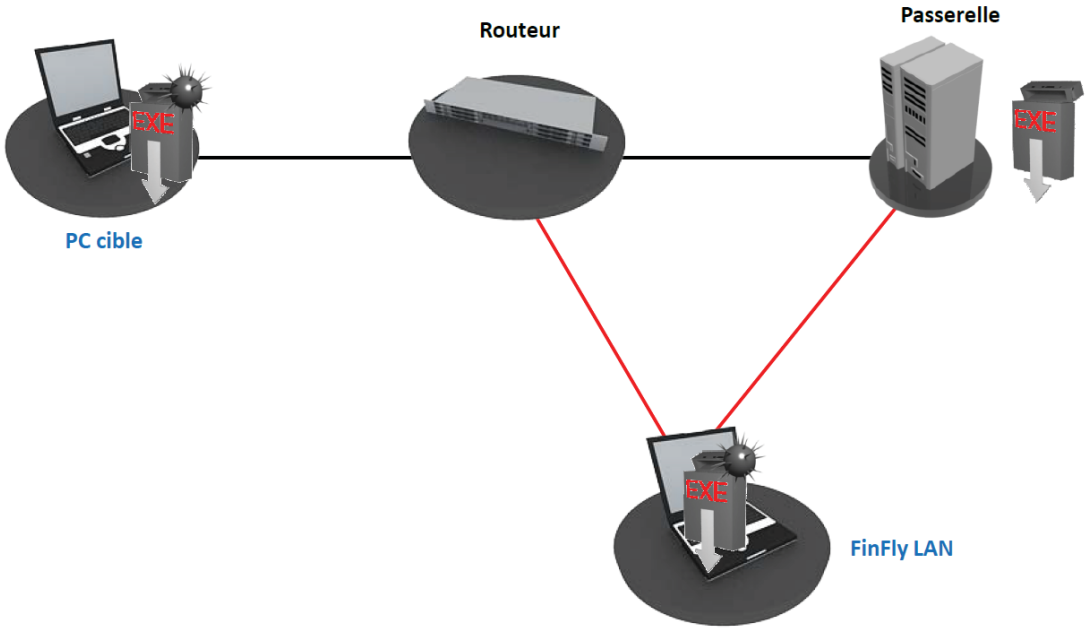
FinFly LAN

· Un logiciel sur Linux avec une interface utilisateur simple

Kit FinIntrusion - Intégration (en option)

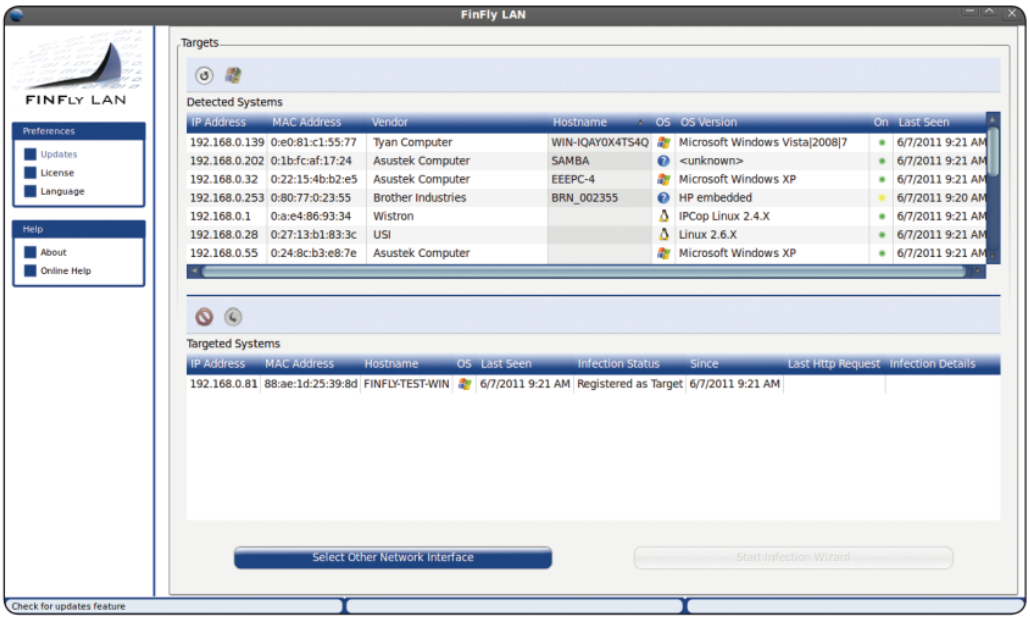
· FinFly LAN sera chargé comme module dans le kit FinIntrusion

Déploiement via les réseaux locaux



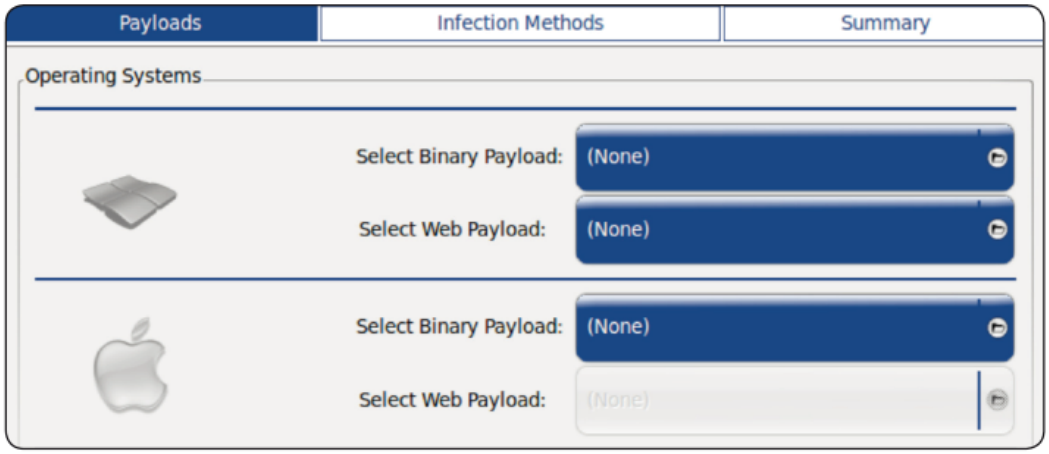
Interface utilisateur automatisée

· Simple à utiliser, sans nécessité de formation approfondie



Prise en charge de cibles multiples et de la charge utile

· Différents exécutables peuvent être ajoutés pour chaque cible



GAMMAGROUP

GAMMA INTERNATIONAL
Royaume Uni

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

FINFLY WEB

L'un des défis majeurs de l'utilisation d'une solution d'écoute à distance est de l'installer sur le système cible, en particulier lorsqu'on ne dispose que de peu d'informations (par exemple juste une **adresse mail**) et **qu'aucun accès physique** n'est possible.

FinFly Web est conçu pour permettre un déploiement **secret et à distance** sur un système cible en utilisant un large éventail **d'attaques via le web**.

FinFly Web fournit une **interface cliquer-pointer** qui permet à l'agent de **créer facilement un code de déploiement personnalisé** à partir des modules sélectionnés.

La charge sera déployée au moment où le système cible visitera le site web préparé avec le code personnalisé.

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations stratégiques**
Capacités:	· **Déploie une solution d'écoute à distance sur le système cible dans le réseau local**
Contenu:	· **Logiciel**

Exemple d'utilisation 1 : Unité de surveillance technique

Après avoir profilé une cible, l'unité a créé un **site web susceptible d'intéresser** celle-ci, et lui a envoyé le lien **par le biais d'un forum de discussion**. Dès l'ouverture du lien vers le site web de l'unité, une solution d'écoute à distance a été installée sur le système cible, et la cible a été **écoutée depuis le QG**.

Exemple d'utilisation 2 : Agence de renseignement

Un client a déployé **FinFly ISP chez le principal opérateur** de son pays. Il a été **combiné avec FinFly Web** pour **déployer la charge à distance quand la cible visitait un site web de confiance**.

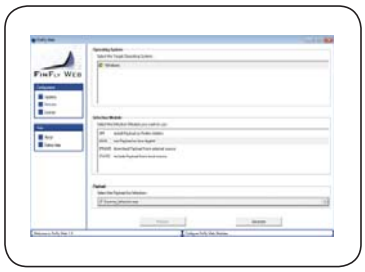
Présentation des fonctionnalités

- **Des modules Web** entièrement personnalisables
- Directement installables secrètement **dans chaque site Web**
- Intégration complète avec **FinFly LAN, FinFly NET** et **FinFly ISP** pour un déploiement y compris dans des sites web populaires (webmail, portails vidéo, etc.)
- Installe la solution d'écoute à distance, **même si la seule information connue est l'adresse mail**
- Possibilité de cibler chaque personne visitant **les sites web configurés**

Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

FINFLY WEB

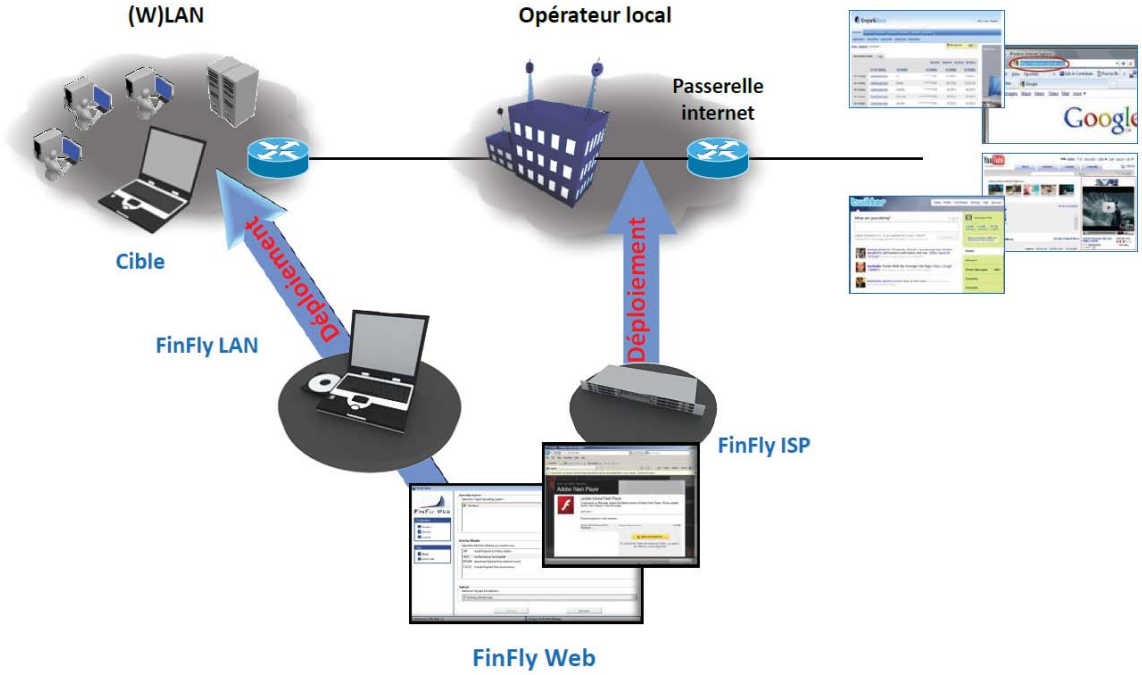
Composants du produit



FinFly Web

· Générateur de sites web personnalisés

Intégration complète avec FinFly LAN et FinFly ISP



GAMMAGROUP

GAMMA INTERNATIONAL
Royaume Uni

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

FINFLY EXPLOIT PORTAL

Les méthodes standard de déploiement pour les solutions d'écoute à distance **ne peuvent généralement pas être appliquées avec des cibles bien entraînées et extrêmement prudentes** car elles sont familières des techniques et des outils classiques de déploiement.

Dans la plupart des scénarios, **les exploits 0-Day** constitue un moyen extrêmement puissant et **fiable pour déployer les solutions d'écoute à distance** en exploitant **des vulnérabilités encore non corrigées** dans les logiciels utilisés par la cible.

FinFly Exploit Portal offre un accès à une vaste bibliothèque d'exploits 0-Day et 1-Day pour les logiciels courants comme Microsoft® Office, Internet Explorer, Adobe Acrobat Reader et bien d'autres.

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations stratégiques**
Capacités:	· **Déploie une solution d'écoute à distance sur le système cible dans le réseau local**
Contenu:	· **Logiciel**

Exemple d'utilisation 1 : Unité criminelle high-tech

Une unité criminelle High-Tech menait une **enquête sur un cybercrime** et devait déployer une solution d'écoute à distance sur un système cible. Ils ont préparé un fichier PDF utilisant un exploit 0-Day sur Adobe Acrobat Reader et l'ont envoyé par mail à la cible. La solution d'écoute à distance a été automatiquement déployée au moment où la cible a ouvert le fichier.

Exemple d'utilisation 2 : Agence de renseignement

Une cible a été identifiée **au sein d'un forum de discussion** mais aucun contact direct ou par mail n'était possible. L'agence a créé un serveur web contenant un **exploit 0-day sur Internet Explorer**. La charge a été déployée sur le système cible **au moment où la cible a ouvert l'URL** qui lui avait été envoyée via un message privé sur le forum de discussion.

Présentation des fonctionnalités

- Accès complet au **portail web et au générateur d'exploit**
- **Exploits 0-Day de niveau gouvernement** qui fonctionnent sur de multiples systèmes et niveaux de patches **sans modification supplémentaire**
- Au moins **4 exploits majeurs** (logiciels courants de navigation, mail et visualisation de fichiers) disponibles en permanence
- **Garantie 30 jours** pour chaque exploit au sein du portail
- Des **exploits 1-Day** régulièrement mis à jour pour différents logiciels

Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

FINFLY EXPLOIT PORTAL

Composants du produit

FinFly Exploit Portal

- Bibliothèque d'exploits d'interfaces web

Exemple du portail FinFly Exploit

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
Royaume Uni

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

FINFLY ISP

Dans de nombreuses opérations en conditions réelles, il n'est pas possible d'accéder physiquement aux systèmes cibles dans un pays particulier. **L'installation secrète** d'une solution d'écoute à distance est nécessaire pour être en mesure de **surveiller la cible depuis le QG**.

FinFly ISP est une solution (mobile) stratégique, **à l'échelle du pays, mais également tactique (mobile),** pouvant être **intégrée dans le réseau d'accès et/ou d'infrastructure d'un opérateur** pour installer la solution d'écoute à distance sur les systèmes cibles sélectionnés.

Les boîtiers FinFly ISP sont basés sur **une technologie serveur de classe transporteur** qui offre une fiabilité **et une évolutivité maximales** pour répondre à quasiment tous les défis liés aux topologies réseau. Un large éventail d'interfaces réseau - toutes **sécurisées par des fonctions de contournement -** sont disponibles pour la connectivité requise au réseau actif.

Plusieurs méthodes passives et actives d'identification de la cible - de la **surveillance en ligne** par dérivation passive des **communications interactives** entre FinFly ISP et les serveurs AAA - garantissent que les cibles sont identifiées et que leur trafic approprié sera fourni au processus de déploiement.

FinFly ISP est capable de **patcher à la volée** les fichiers qui sont téléchargés par la cible**, ou d'envoyer des fausses mises à jour logicielles** de logiciels courants. La nouvelle version intègre la puissante application de déploiement à distance **FinFly WEB** de Gamma, qui injecte une charge dans tout site web visité par la cible.

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations stratégiques**
Capacités:	· **Déploie une solution d'écoute à distance sur le système cible via le réseau de l'opérateur**
Contenu:	· **Matériel/Logiciel**

Exemple d'utilisation : Agence de renseignement

FinFly ISP a été déployé dans les réseaux des principaux opérateurs du pays, et a été activement utilisé pour déployer une solution d'écoute à distance sur les systèmes cibles. Comme les cibles ont des comptes DSL avec des adresses IP dynamiques, elles sont identifiées à partir de leur compte Radius.

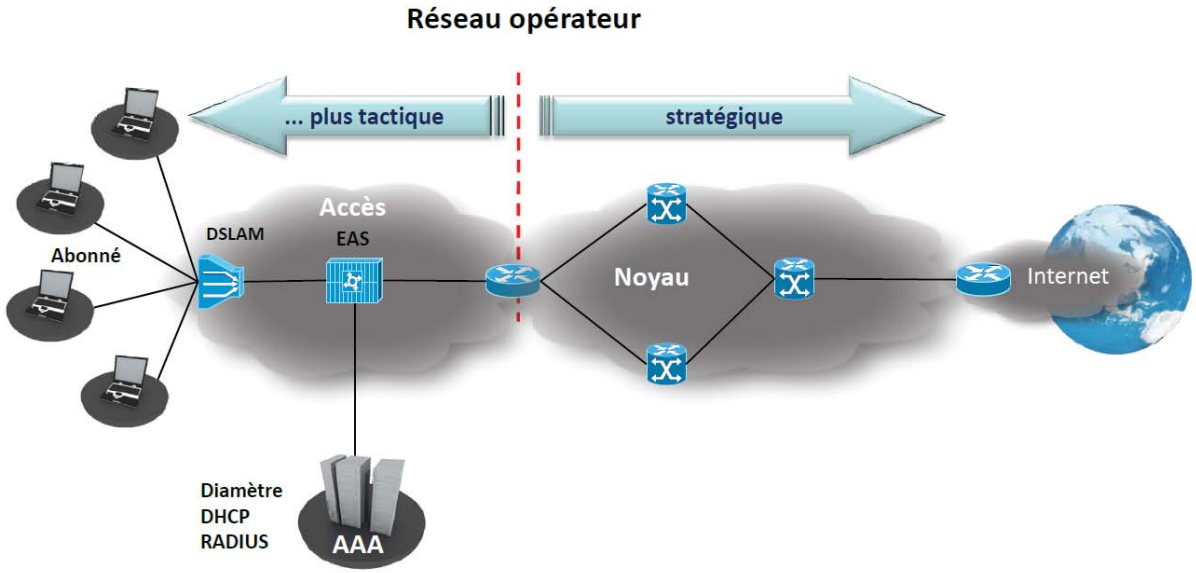
Présentation des fonctionnalités

- Peut être installé au sein du **réseau d'un opérateur**
- Gère **tous les protocoles courants**
- Sélectionne les cibles par **adresse IP, compte Radius, DHCP et MSISDN**
- Cache la solution d'écoute à distance dans les **téléchargements des cibles**
- Injecte une solution d'écoute à distance sous la forme de **mises à jour logicielles**
- Installe la solution d'écoute à distance via les **sites web visités par la cible**

Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

Différentes possibilités d'emplacement

· FinFly ISP peut être utilisé comme solution tactique ou stratégique au sein des réseaux de l'opérateur



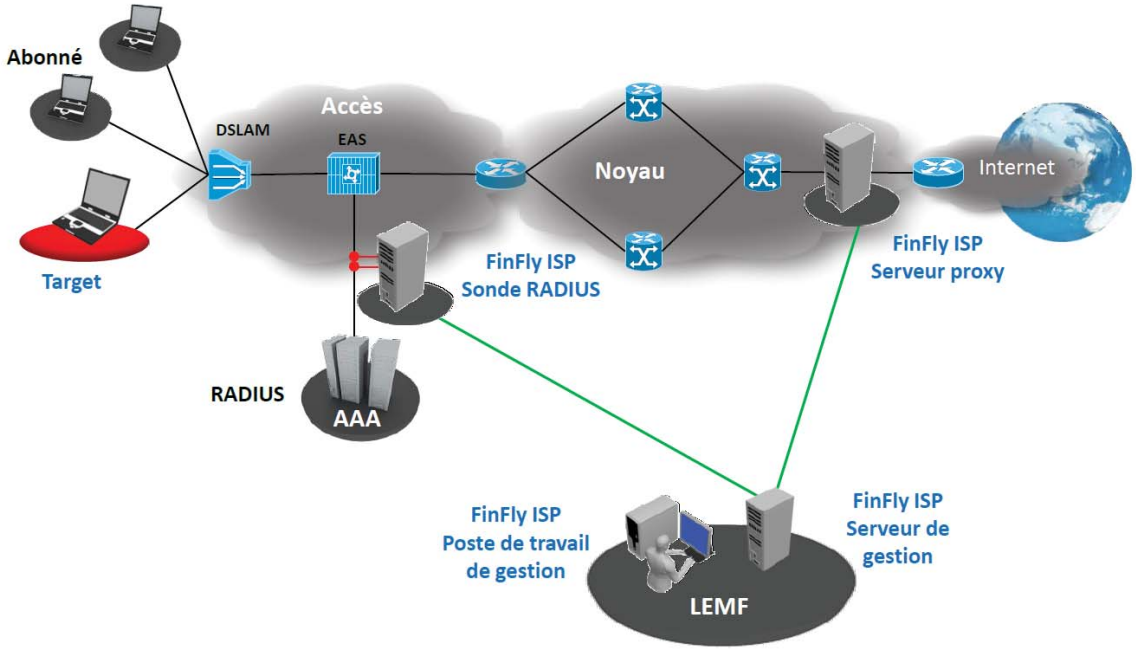
Une solution tactique est mobile. Le matériel est dédié aux tâches de déploiement au sein du réseau d'accès près des points d'accès des cibles. Elle peut être déployée rapidement pour répondre aux exigences tactiques focalisées sur une cible précise ou un nombre réduit de cibles dans une zone particulière.

Une solution stratégique serait une installation permanente de FinFly ISP à l'échelle d'un pays ou d'un opérateur, pour sélectionner des cible et déployer les charges depuis le QG distant sans avoir besoin que les forces de l'ordre se trouvent sur place.

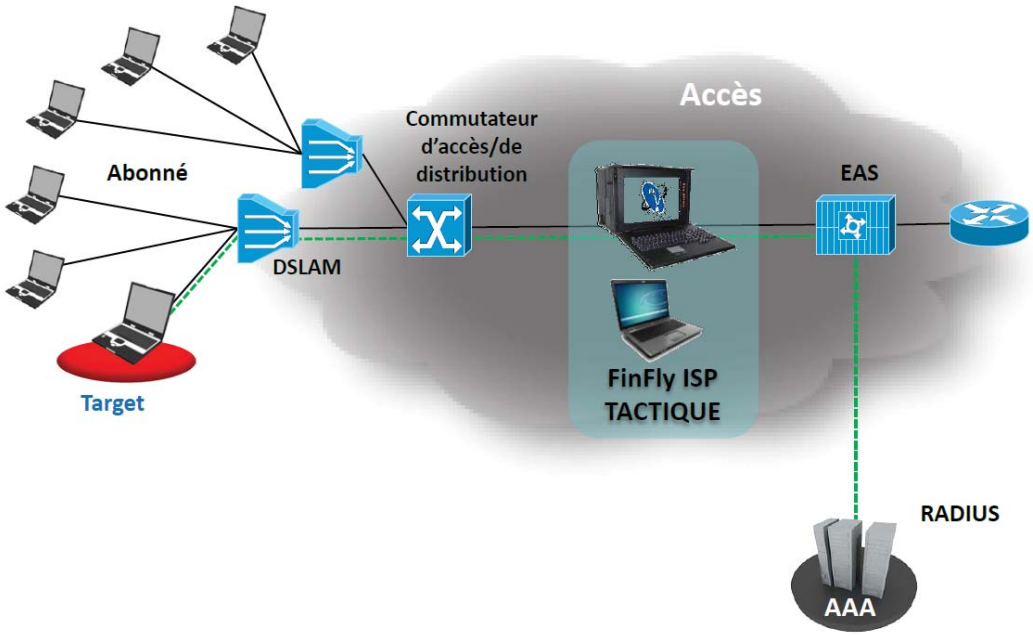
Il est bien sûr possible de combiner des solutions tactiques et stratégiques pour atteindre un maximum de souplesse au niveau des opérations de déploiement.

Configuration réseau

Déploiement stratégique



Déploiement tactique



FINFLY ISP

Composants du produit

FinFly ISP Stratégique

Un déploiement stratégique de FinFly ISP consiste au moins en ce qui suit :

- Système de gestion au niveau LEMF
- Serveur(s) de vérification d'identification des cibles au niveau du système AAA du réseau
- Serveur(s) proxy de déploiement au niveau, par exemple, de la ou des passerelles internet

Serveurs FinFly ISP
HP ProLiant Série DL G7
Poste de travail Entreprise

Poste de travail FinFly ISP
HP Série Z

Débit:	> 20 Gbits/s
Nb. max de cartes réseau:	2 – 8 Cartes réseaux
Interfaces:	1GE cuivre / fibre 10GE cuivre / fibre SONET/SDH OC-3 / -192 STM-1 / -64 ATM AAL5
Processeurs:	1x – 8x Intel XEON
Noyau:	2 à 8 cœurs par processeur
RAM:	12 Go – 1 To
Capacité disque dur:	3 x 146 Go – 4,8 To SAS
Fonctionnalités:	HP iLO 3 Alimentation redondante Ventilateurs redondants Fonction Bypass Switch (le cas échéant)
Système d'exploitation:	GNU Linux (Debian 5.0) durci

FinFly ISP Tactique

Un système FinFly ISP tactique consiste en ce qui suit :

- Serveur proxy d'identification et de déploiement sur les cibles (Portable)
- Système de gestion (Notebook)

Portable FinFly ISP
Atlas A9 17" Portable

Gest. FinFly ISP
Lenovo Thinkpad
Série T

Débit:	6 Gbits/s
Nb. max de cartes réseau:	3 cartes réseaux (Interfaces)
Interfaces:	1x 1000BASE-T (cuivre ; 2 ports) 1x 1000BASE-SX (fibre multi-mode ; 2 ports) 1x 1000BASE-LX (fibre mono-mode ; 2 ports) Autres sur demande
Processeurs:	1x Intel Core i7 Intel Xeon sur demande
Cœurs:	4 cœurs par processeur
RAM:	12 Go minimum
Capacité disque dur:	2 x 1 To SATA
Lecteur optique:	DVD+/-RW SATA
Moniteur:	1 x 17" TFT, clavier, pavé tactile
Fonctionnalités:	Fonction Bypass Switch pour les cartes réseau
Système d'exploitation:	GNU Linux (Debian 5.0) durci Windows 7 Prof. (nb. gestion)

GAMMAGROUP

GAMMA INTERNATIONAL
Royaume Uni

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

FINFLY NET

Dans de nombreuses opérations en conditions réelles, il n'est pas possible d'accéder physiquement aux systèmes cibles dans un pays particulier.

Pour résoudre ce problème, **il est nécessaire d'installer** secrètement une solution d'écoute à distance **permettant de surveiller la cible depuis le QG**.

FinFly NET est une solution **tactique** (portable) à déployer très rapidement dans un **environnement LAN « amical »** (ex. : hôtel, hotspot, entreprise - avec le soutien du propriétaire du réseau), pour installer à distance la solution d'écoute à distance sur les systèmes cibles sélectionnés.
FinFly NET est basé sur un **portable PC ultra-performant** combiné avec un **notebook de gestion** pour offrir un maximum de mobilité et de souplesse dans les réseaux cibles. Un large éventail de cartes réseau **(toutes sécurisées par des fonctions de contournement)** sont disponibles pour la connectivité requise au réseau actif.

L'utilisateur final peut choisir plusieurs **méthodes passives sophistiquées pour l'identification des cibles et du trafic**. Celles-ci vont de la surveillance DHCP/RADIUS (adresses MAC, noms d'utilisateurs), la surveillance des flux ou la prise d'empreinte (fingerprinting). Chaque méthode peut être utilisée de façon autonome ou en combinaison, pour augmenter au maximum les chances d'identifier les cibles qui nous intéressent. Bien sûr, des adresses IP fixes peuvent également être utilisées.

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations tactiques**
Capacités:	· **Déploie une solution d'écoute à distance sur le système cible dans un environnement LAN « amical »**
Contenu:	· **Matériel/Logiciel**

Il est capable de **patcher à la volée les fichiers téléchargés** par la cible, **d'infecter la cible en envoyant des fausses mises à jour logicielles** de logiciels courants ou encore **d'injecter la charge dans les sites Web visités**.

Exemple d'utilisation sur un LAN : Agence de renseignement

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

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

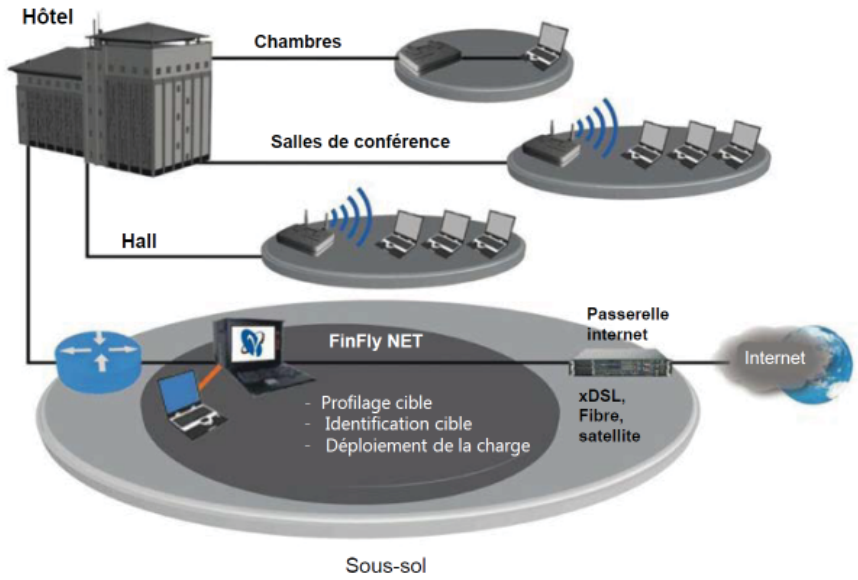
Présentation des fonctionnalités

- Peut être installé au sein d'un **environnement LAN** (hôtel, hotspot, entreprise…)
- Ethernet 1000Base-T, 1000Base-SX, 1000Base-LX
- Identifie les cibles au moyen de différentes **méthodes de profilage/identification**
- Cache une solution d'écoute à distance dans les **téléchargements des cibles**
- Injecte une solution d'écoute à distance sous la forme de **mises à jour logicielles**
- Installe une solution d'écoute à distance via les **sites web visités par la cible**

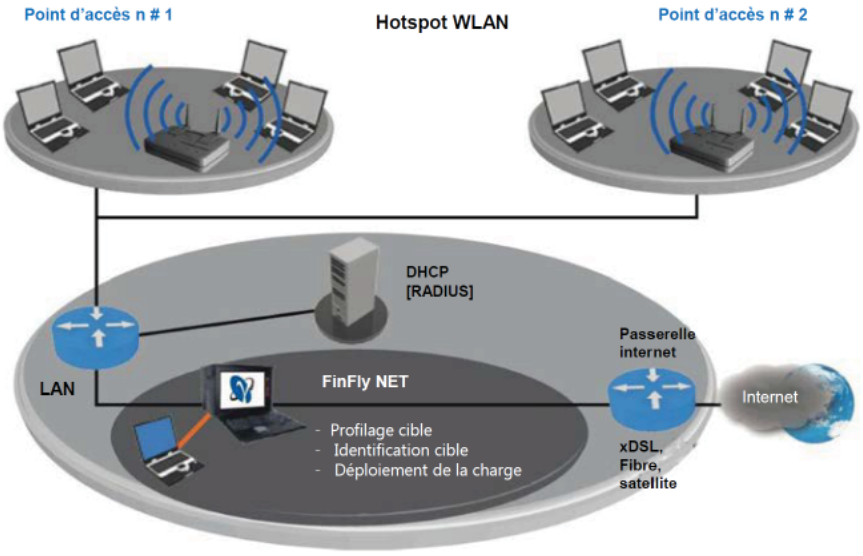
Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit.

DIFFÉRENTES POSSIBILITÉS DE DÉPLOIEMENT

Déploiement sur le LAN d'un hôtel



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



FinFly NET sera déployé à l'endroit le plus approprié à l'intérieur de l'établissement. Une fois connecté le portable en ligne au(x) liaison(s) fournie(s), l'utilisateur peut commencer à analyser le trafic en sélectionnant différentes méthodes pour identifier les cibles intéressantes et leur trafic IP. Les méthodes à utilisées for l'identification des cibles dépendent fortement de la configuration réseau, des fonctionnalités et des services offerts et utilisés.

IDENTIFICATION ET PROFILAGE DES CIBLES

Module de reniflage HTTP
Langues, historique, types et versions des navigateurs et du système d'exploitation

Module de reniflage des mails
POP3, SMTP

Module de reniflage des login
FTP, HTTP, IMAP, IRC, NNTP, POP, SMTP

Module de reniflage TCP/UDP
IP source/destination, ports source/destination

Module de reniflage DHCP/RADIUS
MAC, nom de l'hôte, début/fin de session IP

MÉTHODES DE DÉPLOIEMENT SUR LES CIBLES

Binaire/Téléchargemement
Patchs de fichiers « .exe » et/ou « .scr »

Injection via des mises à jour
Fausses mises à jour pour différentes applications

Déploiement sur site web
Utilisation de FinFly Web pour un déploiement pendant la navigation

FINFLY NET

Composants du produit

FinFly NET consiste en ce qui suit:

- Serveur proxy d'identification, de profilage et de déploiement sur les cibles (Portable)
- Système de gestion (Notebook)

FinFly NET Portable
Atlas A9 17" Portable

Gest. FinFly NET
Lenovo Thinkpad
Série T

Débit:	6 Gbits/s
Nb. max de cartes réseau:	3 cartes réseaux (Interfaces)
Interfaces:	1x 1000BASE-T (cuivre ; 2 ports) 1x 1000BASE-SX (fibre multi-mode ; 2 ports) 1x 1000BASE-LX (fibre mono-mode ; 2 ports) Autres sur demande
Processeurs:	1x Intel Core i7 Intel Xeon sur demande
Cœurs:	4 cœurs par processeur
RAM:	12 Go minimum
Capacité disque dur:	2 x 1 To SATA
Lecteur optique:	DVD+/-RW SATA
Moniteur:	1 x 17' TFT, clavier, pavé tactile
Fonctionnalités:	Fonction Bypass Switch pour les cartes réseau
Système d'exploitation:	GNU Linux (Debian 5.0) durci Windows 7 Prof. (nb. gestion)

Remarque importante:
À côté de FinFly NET, Gamma offre les mêmes capacités de renseignement intégrées dans la solution FinFly ISP, alors que les capacités d'identification des cibles sont mises en œuvre dans une solution opérateur fixe ou portable. Cette solution se caractérise par une technologie serveur ultra-performante qui sera personnalisée et intégrée dans l'environnement opérateur pertinent et les exigences associées.

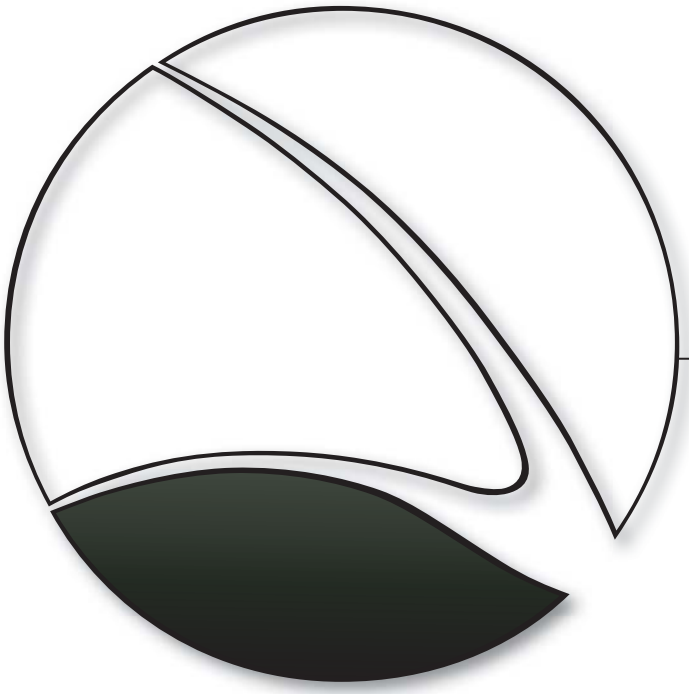
GAMMAGROUP

GAMMA INTERNATIONAL
Royaume Uni

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

Programme De Formation À L'intrusion Informatique

FINTRAINING



Le programme de formation à l'intrusion informatique comprend des cours qui portent sur les produits proposés ainsi que sur les méthodes et les techniques pratiques d'intrusion informatique. Ce programme transfère aux utilisateurs des années de connaissance et d'expérience, maximisant ainsi leurs compétences dans ce domaine.

FINFISHER™
IT INTRUSION

WWW.FINFISHER.COM

Programme De Formation À L'intrusion Informatique

FINTRAINING

La sensibilisation à la sécurité est **indispensable pour tout gouvernement** soucieux de maintenir la sécurité informatique et de **prévenir efficacement les menaces** contre une infrastructure informatique, susceptibles d'entraîner une perte au niveau confidentialité, intégrité et disponibilité des données.

En revanche, des sujets tels que la **cyberguerre**, l'interception active et la collecte de renseignements par **intrusion informatique** ont pris de l'importance au quotidien. Ils nécessitent que les gouvernements **mettent en place des équipes d'intrusion informatique** pour **répondre à ces nouveaux défis**.

Les formations FinTraining sont dispensées par les **meilleurs experts en intrusion sur la planète**. Elles déroulent de **véritables scénarios concrets** qui mettent l'accent sur les opérations en **conditions réelles** comme celles auxquelles peut se retrouver confronté l'utilisateur final dans ses **défis quotidiens**.

Gamma combine les cours de formation individuels à un **programme de formation professionnelle et de conseil** qui permet de mettre en place ou améliorer les capacités d'une équipe d'intrusion informatique. Les formations sont **entièrement personnalisées** en fonction des défis et exigences opérationnelles de l'utilisateur.

INFORMATIONS RAPIDES	
Utilisation:	· **Transfert de connaissances**
Capacités:	· **Savoir-faire en matière d'intrusion informatique** · **Compétences en cyberguerre**
Contenu:	· **Formation**

Exemples de sujets abordés pendant la formation

- **Profilage** de cibles (sites web et individus)
- Traçage **des mails anonymes**
- **Accès distant** aux comptes webmail
- **Évaluation de la sécurité** des serveurs et des services web
- Exploitation pratique des **logiciels**
- **Intrusion informatique sans fil** (WLAN/802.11 et Bluetooth)
- Attaques contre les **infrastructures critiques**
- Reniflage **de données et d'authentifiants utilisateur** dans les réseaux
- **Surveillance des hot-spots**, des cybercafés et des réseaux dans les hôtels
- **Interception et enregistrement des appels** (VoIP et DECT)
- **Craquage des** hashs des mots de passe

Programme de conseil

- Programme complet **de formation et de conseil** en intrusion informatique
- Constitution, structuration et **formation de l'équipe d'intrusion informatique**
- **Évaluation** complète des membres de l'équipe

Cours personnalisés dans des établissements de formation haut de gamme dans le monde entier

GAMMAGROUP

GAMMA INTERNATIONAL
Royaume Uni

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

FINSUPPORT

FinSupport

L'assistance FinSupport fournit les mises à niveau et les mises à jour de la ligne de produits FinFisher™ conjointement à un contrat d'assistance annuel.

La page web et l'équipe d'assistance FinFisher™ fournissent les services suivant à nos clients :

- Accès en ligne à:
  - Manuel utilisateur le plus récent
  - Spécifications produit les plus récentes
  - Dernières diapositives de formation sur les produits
  - Frontal de rapport de bugs
  - Rapport du tout dernier test antivirus
  - Frontal de demande de nouvelles fonctionnalités

- Mises à jour logicielles régulières:
  - Correctifs de bugs
  - Nouvelles fonctionnalités
  - Nouvelles versions majeures

- Assistance technique via Messenger:
  - Corrections de bugs
  - Assistance opérationnelle partielle

Assistance FinLifelineSupport

L'assistance FinLifelineSupport offre une assistance back-office professionnelle pour les questions techniques et la résolution des problèmes. Elle fournit également une assistance back-office à distance pour des corrections de bugs dans les logiciels FinFisher™ et le remplacement de matériel sous garantie.
De plus, avec l'assistance FinLifelineSupport, le client reçoit automatiquement les nouvelles fonctionnalités avec la livraison standard des corrections de bugs.

INFORMATIONS RAPIDES	
Utilisation:	· **Solution globale et Support opérationnel**
Capacités:	· **Correction des bugs, mise à jour à jour des fonctionnalités**
Contenu:	· **Matériel/Logiciel**

Mises à niveau logicielles

L'assistance technique FinLifelineSupport comprend des mises à niveau logicielles, et garantit des mises à niveau automatiques du système existant avec des correctifs logiciels fournis via le système de mise à jour.

Ces mises à niveau comprennent de nouvelles fonctionnalités et de nouvelles améliorations conformes à la feuille de route du client (hors matériel).

WWW.FINFISHER.COM

GAMMA INTERNATIONAL
Royaume Uni

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