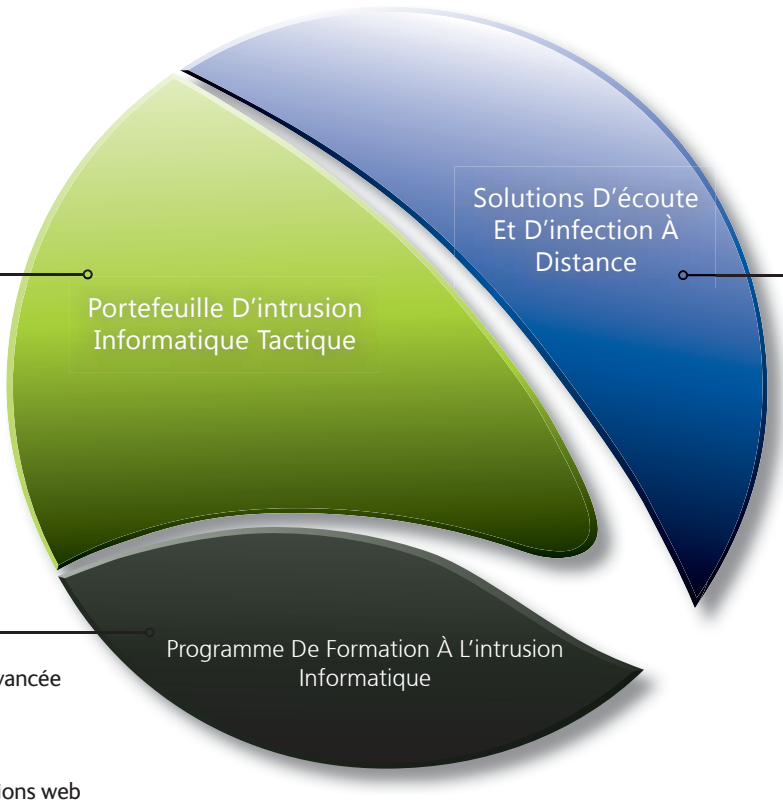
FINFISHER™: Solutions D'intrusion Informatique et D'écoute à Distance Pour les Gouvernements

WWW.GAMMAGROUP.COM

FINFISHER™
IT INTRUSION



- Kit FinIntrusion
- Suite FinUSB
- FinFirewire

FinSpy
- FinSpy
- FinSpy Mobile

FinFly
- FinFly USB
- FinFly LAN
- FinFly Web
- FinFly ISP

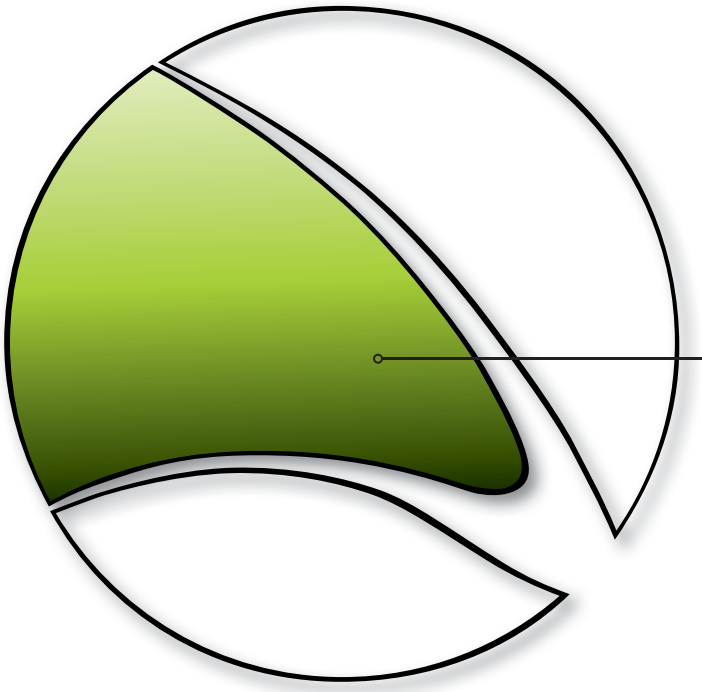
- Intrusion Basique & Avancée
- Intrusion sans fil
- Exploitation Pratique
- Pénétration d'applications web
- Formation et conseil personnalisés en intrusion informatique

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.

Portefeuille D'Intrusion Informatique Tactique

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** · **Opérations tactiques**
Capacités :	· **Casse 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 casser 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 **compromettre avec succès la sécurité** de réseaux et de systèmes informatiques à des fins o**ffensives et défensives** en utilisant divers outils et techniques.

Exemple d'utilisation 3 : Cas d'utilisation stratégiques

Le kit FinIntrusion est largement utilisé pour obtenir l'accès à distance aux comptes de messagerie et aux serveurs web de la cible (ex. : blogs, forums de discussions...), et ainsi écouter leurs activités (journaux d'accès, etc.).

Présentation des fonctionnalités

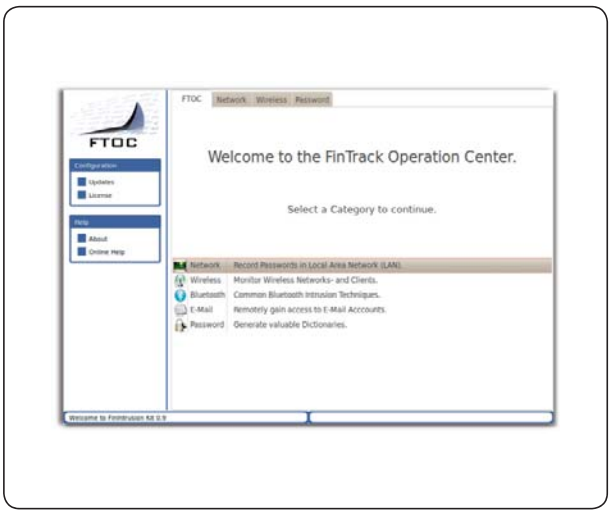
- Découvre **les réseaux sans fil (802.11) et les appareils Bluetooth®**
- Retrouve les phrases de passe WEP (64 et 128 bits) **en 2 à 5 minutes**
- **Casse les phrases de passe WPA1 et WPA2** avec des attaques par dictionnaire
- Écoute activement le réseau local (avec ou sans fil), et **extrait les comptes et mots de passe**, **y compris pour les sessions cryptées TLS/SSL**
- Émule **un faux point d'accès sans fil** (802.11)
- **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

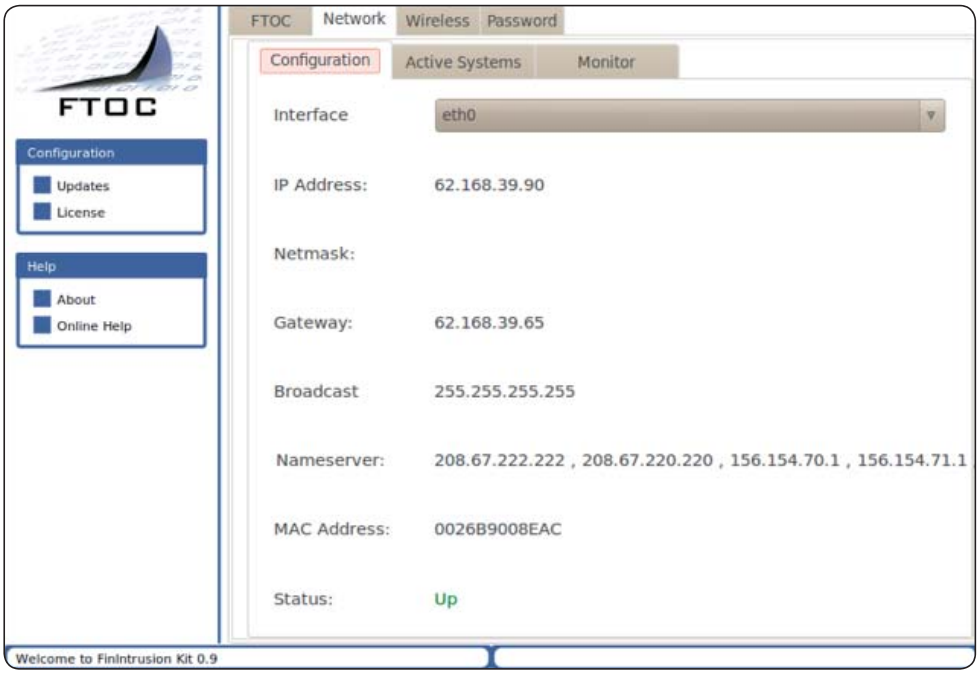
Composants du produit

Le kit FinIntrusion – Unité Tactique Secrète
Composants de base pour l'intrusion informatique :
- Adaptateur WLAN haute puissance
- Adaptateur Bluetooth haute puissance
- Antennes 802.11
- Nombreux appareils courants d'intrusion informatique



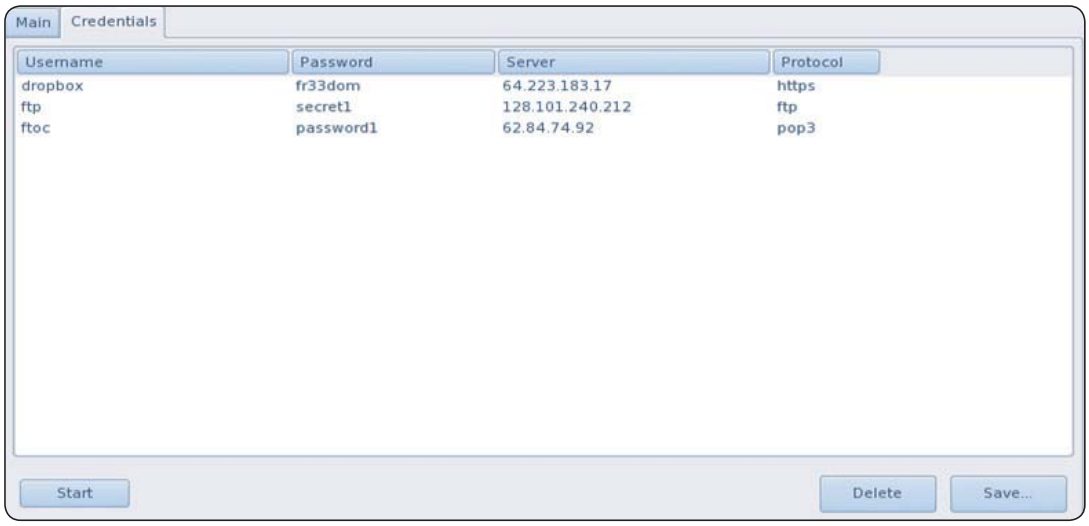
Centre opérationnel FinTrack
- Interface utilisateur graphique pour l'automatisation des a taques par intrusion informatique

Surveillance LAN/WLAN automatique



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.



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 et 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**
- **Cryptage sécurisé** avec RSA et AES
- Extraction **des noms et des mots de passe des utilisateurs** pour tous les logiciels courants, par exemple :
  - Clients de messagerie
  - Messageries instantanées
  - Navigateurs
  - Outils d'administration à distance
- **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
- Crypte les données à la volée

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

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 modifié**
- Fonctionne sur les systèmes **Windows**, **Mac et Linux**
- Fonctionne avec **FireWire/1394**, **PCMCIA et Express Card**

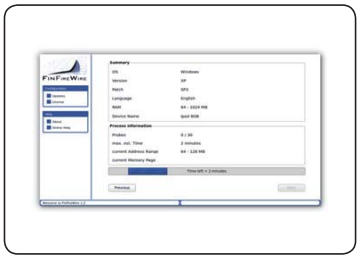
Pour une liste complète des fonctionnalités, veuillez consulter les Spécifications Produit

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
United Kingdom

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

info@gammagroup.com

Solutions D'Écoute Et D'Infection À Distance

FINSPY

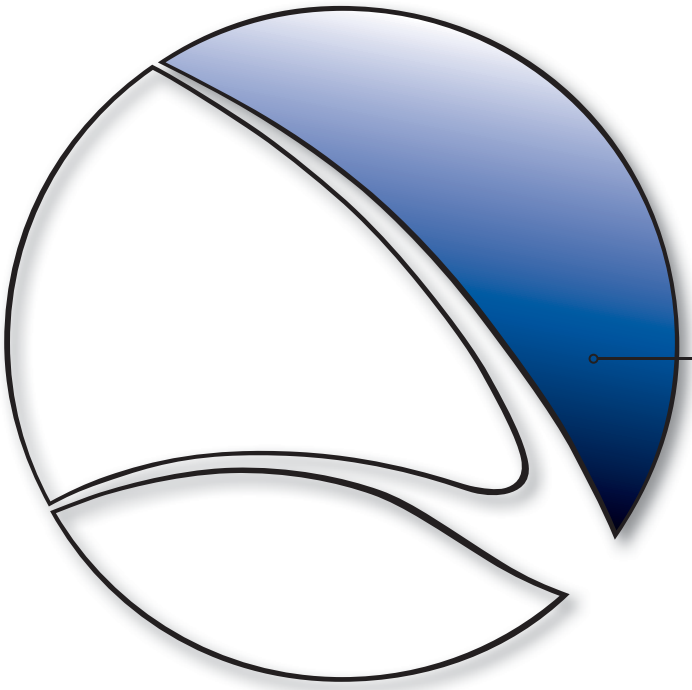
FINSPY MOBILE

FINFLY USB

FINFLY LAN

FINFLY WEB

FINFLY ISP



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.

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**. Celles-ci **changent régulièrement de lieu**, utilisent des canaux de **communication cryptés et anonymes**, et/ou **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 depuis de nombreuses années** lors d'opérations dans le monde entier. Des renseignements précieux ont été obtenus sur des individus 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.

Présentation des fonctionnalités

Ordinateur cible - Exemple de fonctionnalités :

- Contournement de 40 systèmes antivirus régulièrement testés
- **Communication secrète** avec le QG
- **Surveillance complète de Skype** (appels, chats, transferts de fichiers, vidéo, liste de contacts)
- Enregistrement des **communications standard** comme l'e-mail, les chats et la voix sur IP
- **Surveillance en direct** via la webcam et le micro
- **Traçabilité du pays** de la cible
- **Extraction silencieuse des fichiers** du disque dur
- **Enregistreur de frappe (Keylogger) au niveau processus** pour une analyse plus rapide
- **Analyse forensique à distance** du système cible
- **Filtres avancés** pour enregistrer uniquement les informations importantes
- Prise en charge de la plupart des systèmes d'exploitation courants : **Windows**, **Mac OSX et Linux**

INFORMATIONS RAPIDES	
Utilisation :	· **Opérations stratégiques/tactiques**
Capacités :	· **Écoute d'ordinateurs à distance** · **Écoute des communications cryptées**
Contenu:	· **Matériel et 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 habilitations de sécurité
- Cryptage de la communication des données avec **RSA 2048 et AES 256**
- 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

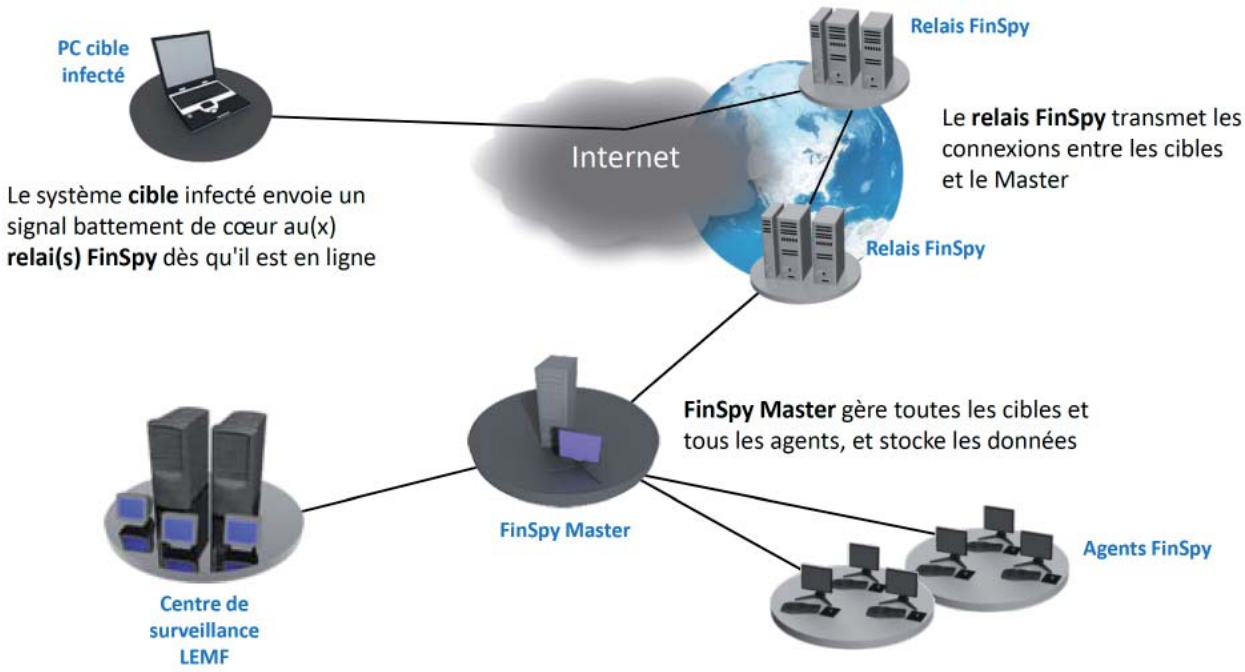
FinSpy Master et Proxy

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

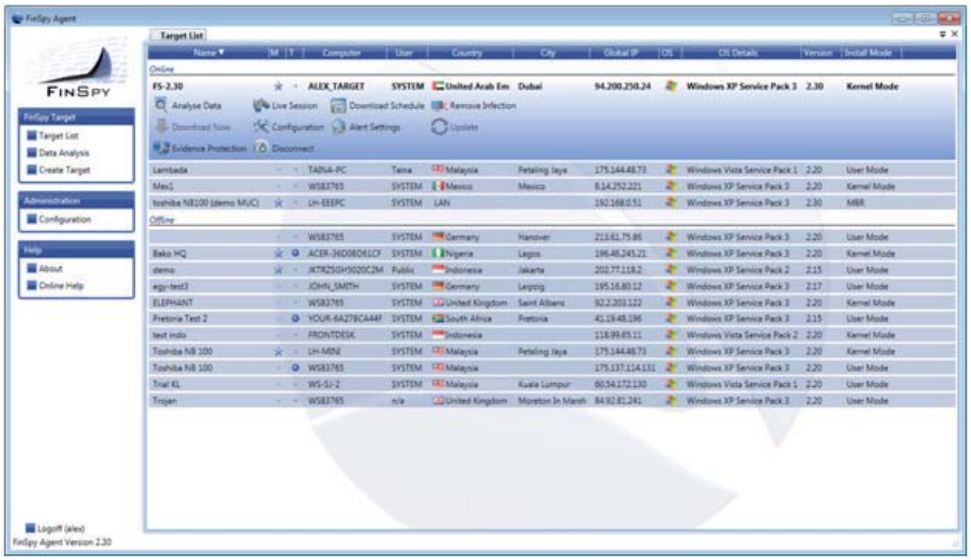
FinSpy Agent

- IHM pour les sessions en direct et l'analyse de la configuration et des données des cibles

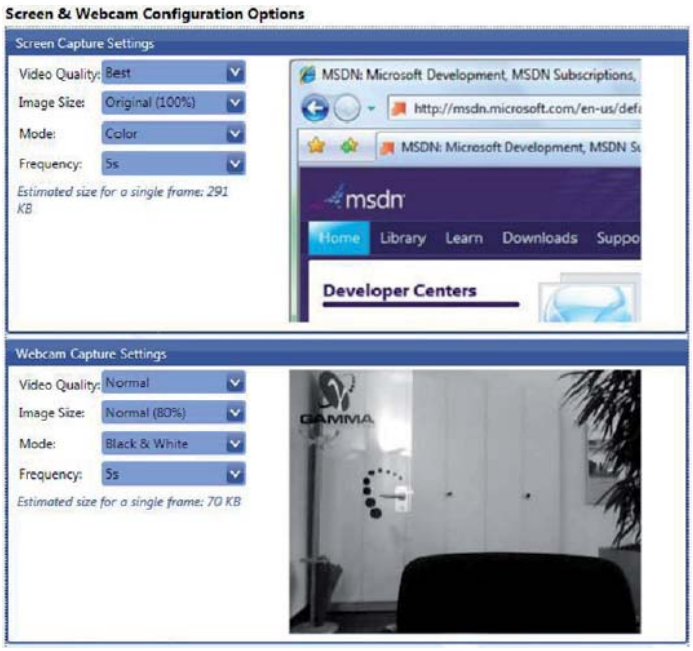
Acces Aux Systemes Informatiques Cibles Dans Le Monde Entier



Interface Utilisateur Facile A 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

LICENSES **FIN**SPY

À savoir

La solution FinSpy comporte 3 types de licences de produits :

A. Licence de mise à jour

La licence de mise à jour détermine si **FinSpy** est en mesure de récupérer les nouvelles mises à jour sur le serveur de mises à jour de Gamma. Celle-ci est associée au module de service après vente FinFisherTM.
Après expiration, le système FinSpy sera toujours entièrement fonctionnel, mais il ne sera plus en mesure de récupérer les versions les plus récentes et les corrections de bogues sur le serveur de mises à jour FinSpy.

B. Licence Agent

La licence Agent contrôle le nombre d'agents **FinSpy Agent** qui peuvent se connecter simultanément à **FinSpy Master**.

Exemple :

- **5 licences Agent** ont été acquises.
- Les licences **FinSpy Agent** peuvent être installées sur un nombre illimité de systèmes, cependant
- Seulement 5 systèmes **FinSpy Agent** peuvent simultanément se connecter à **FinSpy Master** et travailler avec **les données**

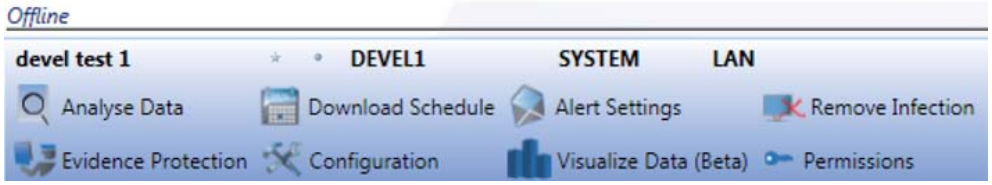
C. Licence cible

La licence cible contrôle le nombre de **cibles FinSpy** pouvant être **actives** simultanément.

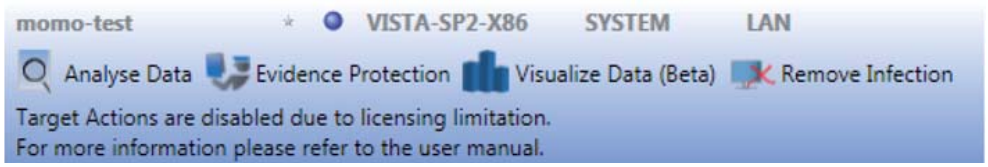
Par « active », on entend une **cible FinSpy activée**, que le système cible soit en ligne ou hors ligne.

Si la **cible FindSpy** est déployée sur un système cible mais qu'aucune licence cible n'est disponible, la **cible FinSpy** est désactivée temporairement et aucun enregistrement ou accès direct n'est possible. Dès qu'une nouvelle licence est disponible (par exemple en mettant à jour la licence existante ou en supprimant l'infection de l'une des **cibles FinSpy** actives), la cible se verra attribuer la licence libre. Étant activée, elle pourra commencer l'enregistrement et fournir un accès en direct.

Capture d'écran cible active avec licence



Capture d'écran cible inactive sans licence



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 de 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.

Présentation des fonctionnalités

Ordinateur 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**, **iOS (iPhone)**, **BlackBerry et Android**

INFORMATIONS RAPIDES	
Utilisation :	· **Opérations stratégiques** · **Opérations 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.**

QG - Exemple de fonctionnalités :

- Protection des preuves (preuves valables conformément aux **normes européennes**)
- **Gestion des utilisateurs** en fonction des habilitations de sécurité
- Cryptage de la communication des données avec **RSA 2048 et AES 256**
- 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

Product Components

FinSpy Master et Proxy

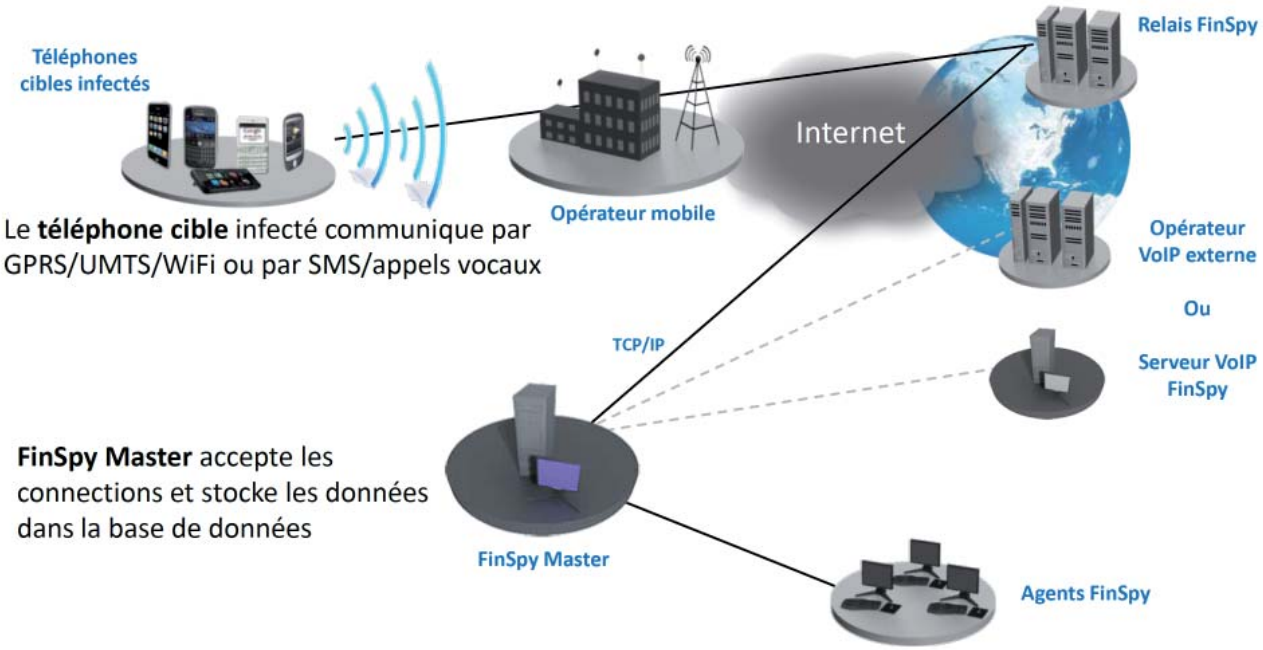
- Contrôle total des téléphones cibles
- Protection des preuves pour les données et les journaux d'activité
- Stockage sécurisé
- Gestion des utilisateurs et des cibles à base d'habilitations de sécurité

FinSpy Agent

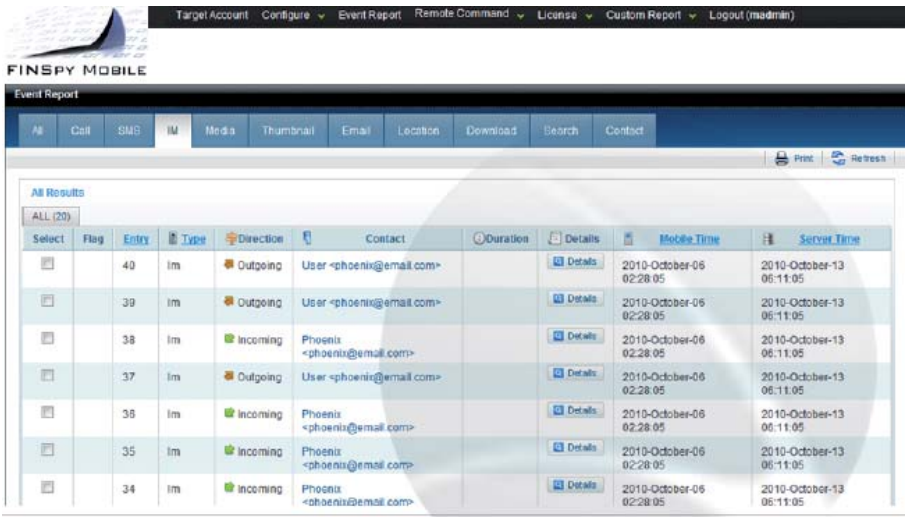
- IHM pour les sessions en direct et l'analyse de la configuration et des données des cibles

FINSPY MOBILE

Acces Aux Systemes Informatiques Cibles Dans Le Monde Entier



Interface Utilisateur Facile A Utiliser



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 n'est pas possible.

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.**

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 ensuite être **écoutés à distance depuis le QG**, et FinFly USB a ensuite été rendu par la source.

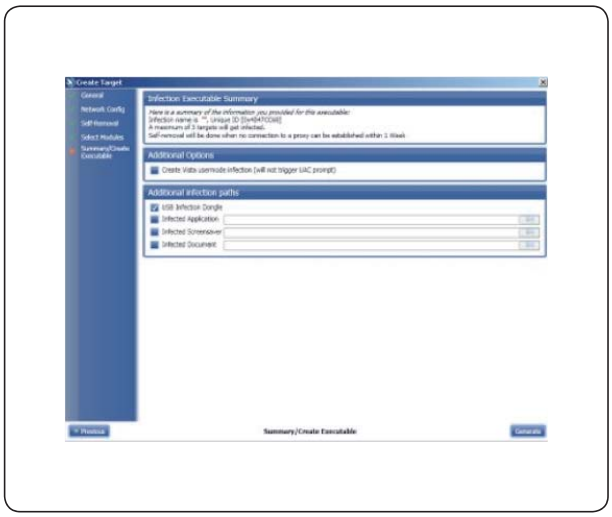
Présentation Des Fonctionnalités

- **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 Office sur le périphérique
- Infection d'un **système cible hors tension** en le **démarrant à partir de la clé USB**
- 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 SanDisk
- Déploie une solution d'écoute à distance lors de l'insertion sur des systèmes cibles
- Déploie une solution d'écoute à distance pendant le processus de démarrage

Intégration Complète FinSpy

- Génération et activation automatique via FinSpy Agent

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

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 infectés** envoyés par e-mail sur leur compte.

En particulier, les cibles sensibilisées à la sécurité sont **presque impossibles à infecter** 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 **d'infecter à la volée les fichiers qui sont téléchargés** par la cible, d'infecter la cible en **envoyant des fausses mises à jour logicielles** de logiciels courants ou encore d'infecter la cible en **injectant 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 parvenir à accéder physiquement à l'ordinateur. 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

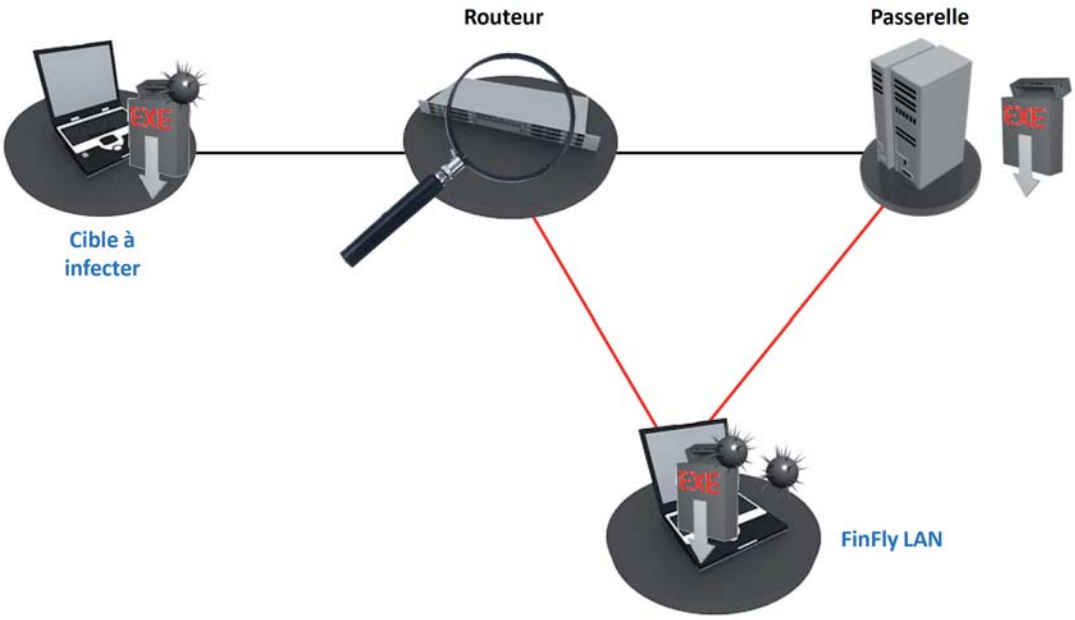
FinFly LAN

· Un logiciel sur Linux avec une interface utilisateur simple

Kit FinIntrusion - Intégration (en option)

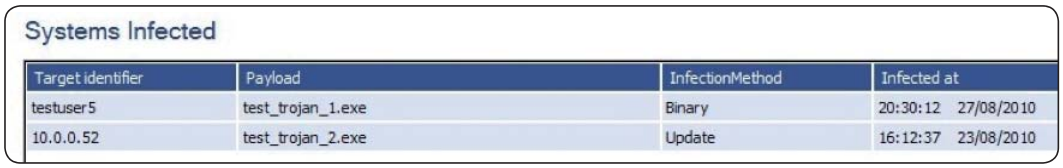
· FinFly LAN peut être chargé comme module dans le kit FinIntrusion

Infection Via Les Reseaux Locaux



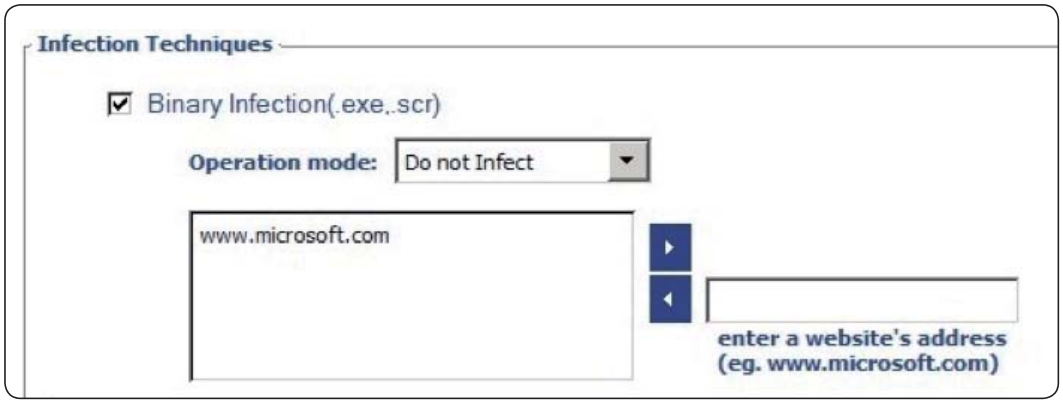
Interface utilisateur automatisée

· 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



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'information (par exemple juste une **adresse mail**) et **qu'aucun accès physique** n'est possible.

FinFly Web est conçu pour permettre une infection **à distance et secrète** d'un système cible en utilisant un large éventail **d'attaques par le web**.

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

Les systèmes cibles qui visitent un site web préparé avec le code d'infection mis en œuvre seront **secrètement infectés** avec le logiciel configuré.

INFORMATIONS RAPIDES	
Utilisation:	· **Opérations stratégiques**
Capacités:	· **Déploie une solution d'écoute à distance sur le système cible via des sites web**
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 pu 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 **infecter à distance les cibles qui visitaient des sites hostiles au gouvernement**, en injectant secrètement le code FinFly Web dans les sites en question

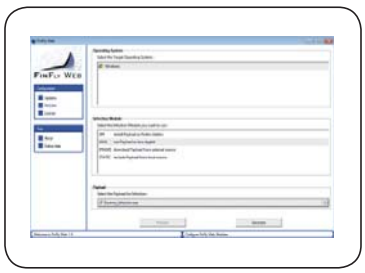
Présentation Des Fonctionnalités

- Des modules Web **entièrement personnalisables**
- Directement installables secrètement **dans chaque site Web**
- Intégration complète avec **FinFly LAN** 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 toute personne visitant les **sites web configurés**

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

FINFLY WEB

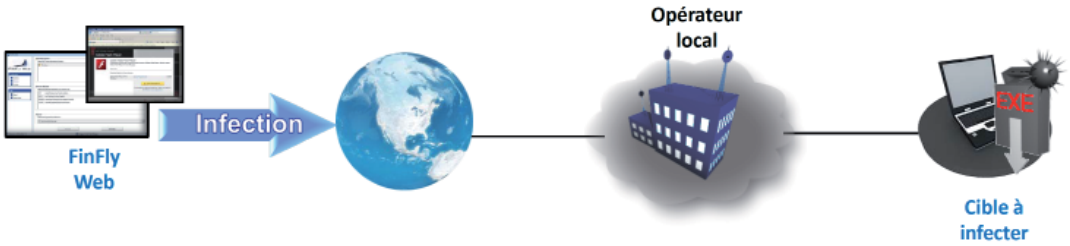
Composants Du Produit



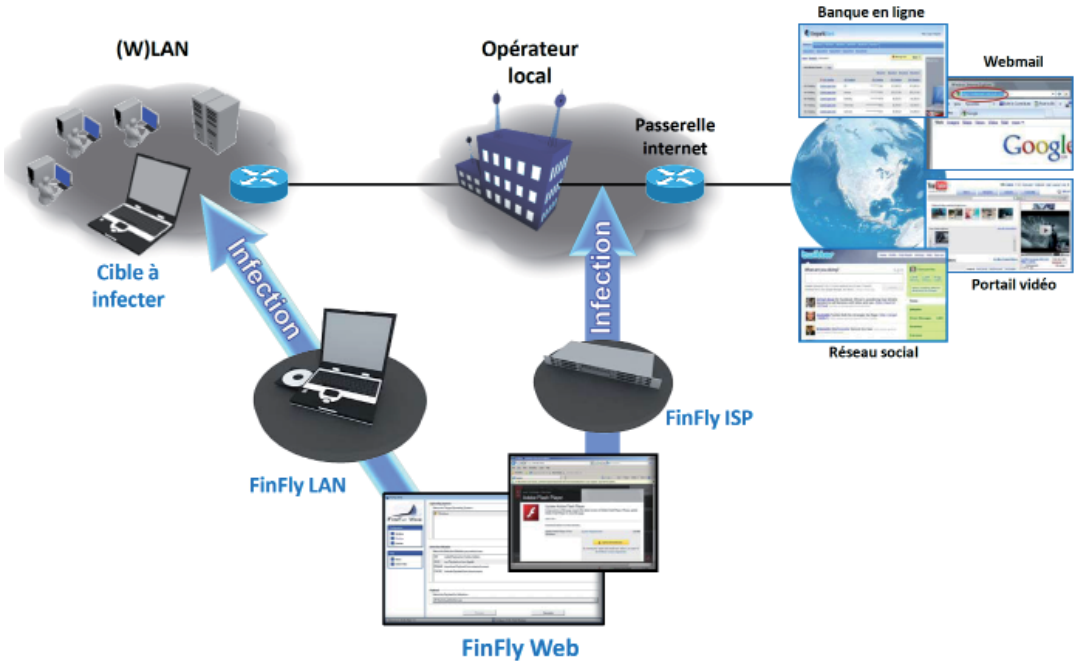
FinFly Web

- Logiciel à base de cliquer-pointer pour créer des sites d'infection personnalisés

Infection directe FinFly Web



Integration complète avec FinFly LAN Et FinFly ISP

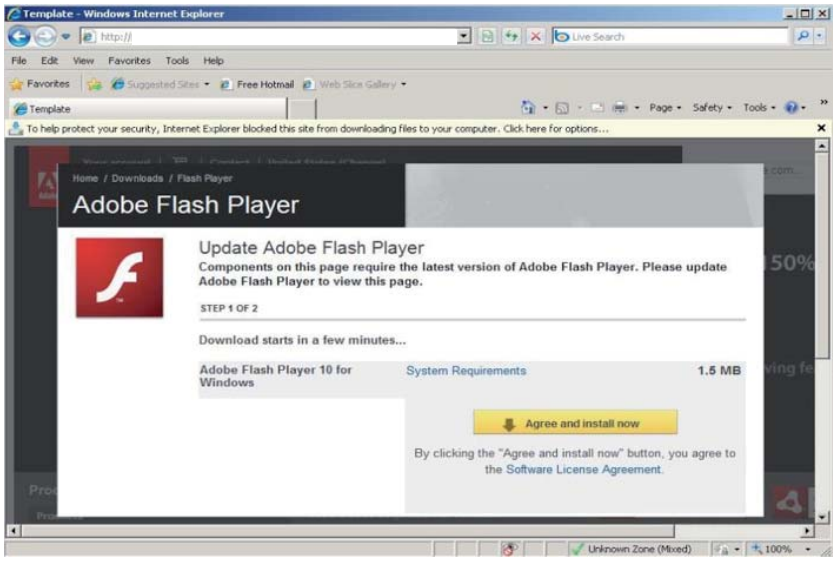


Exemple : Applet Java (Internet Explorer, Firefox, Opera, Safari)

Le site va demander à la cible d'accepter un plug-in Java qui peut être signé avec n'importe quel nom de société (par exemple «Microsoft Corporation»)

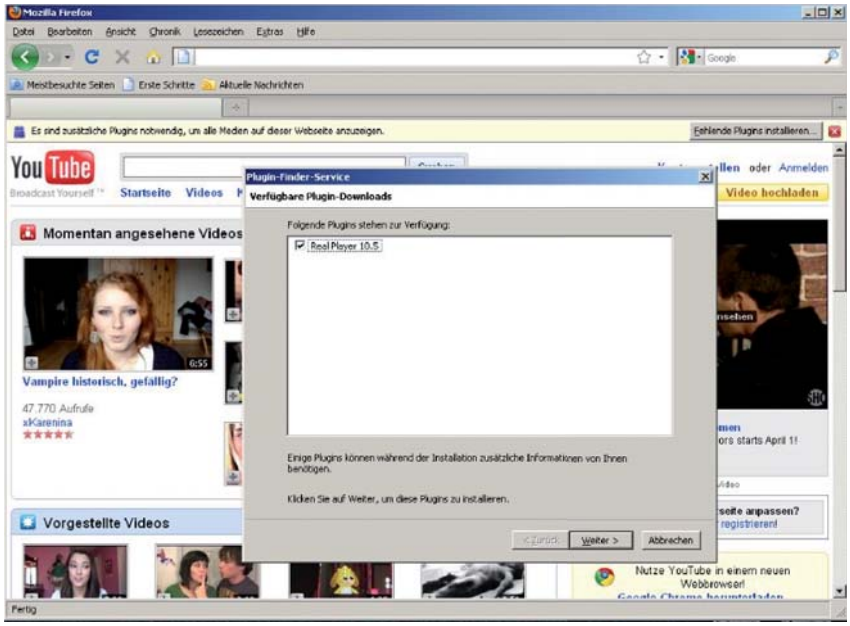
Exemple : Composant Manquant (IE, Firefox, Opera, Safari)

Le site web va prétendre qu'un plug-in ou un codec est absent du système cible, et demander à télécharger et installer le logiciel manquant.



Exemple : XPI Manquante (Firefox Uniquement, Toutes Plateformes)

Ce module demandera à la cible d'installer des plug-in supplémentaires pour arriver à consulter le site web



GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

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**, 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 est fourni au processus d'infection.

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**

FinFly ISP est capable **d'infecter à la volée les fichiers** qui sont téléchargés par la cible, ou d'infecter la cible en **envoyant des fausses mises à jour logicielles de logiciels** courants. La nouvelle version intègre désormais la puissante application d'infection à distance **FinFly Web** de Gamma, pour infecter des cibles à la volée quand elles **visitent n'importe quel site web**.

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.

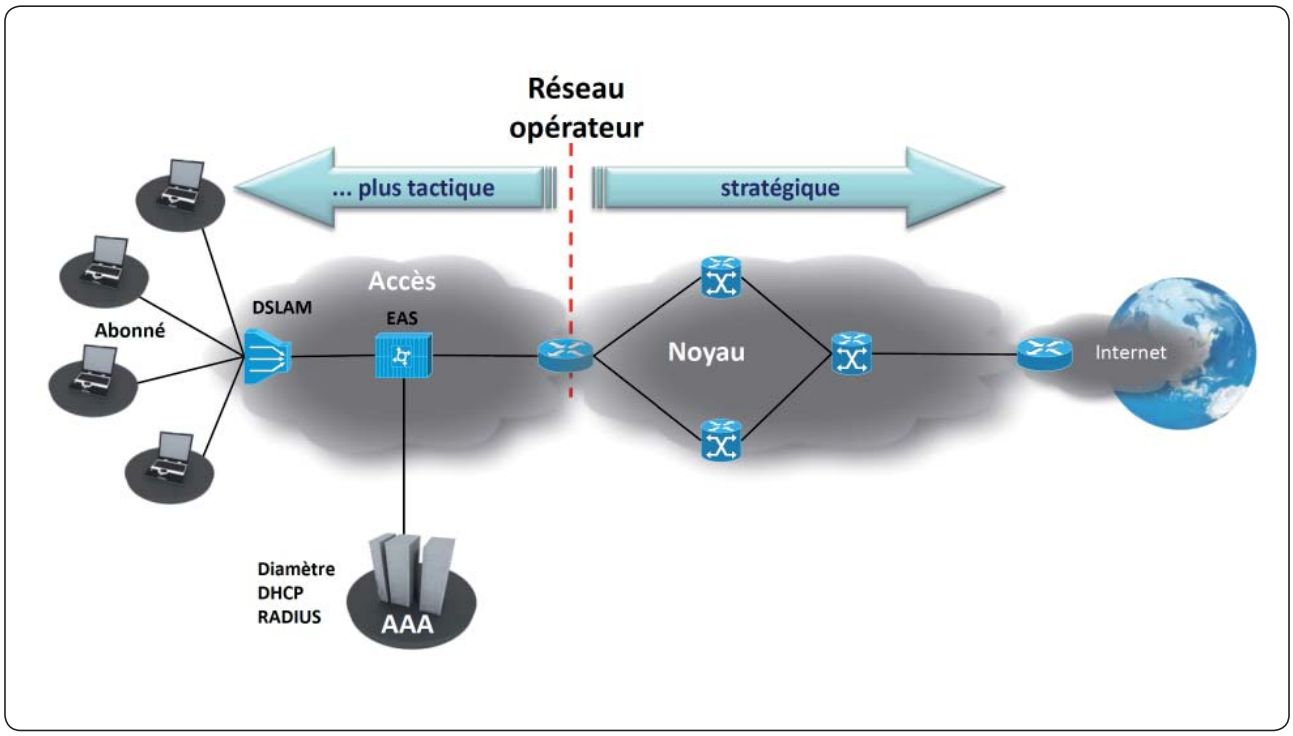
Présentation Des Fonctionnalités

- Peut être installé au sein du **réseau de l'opérateur**
- Gère **tous les protocoles courants**
- Cibles sélectionnées **par adresse IP ou par compte Radius**
- 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



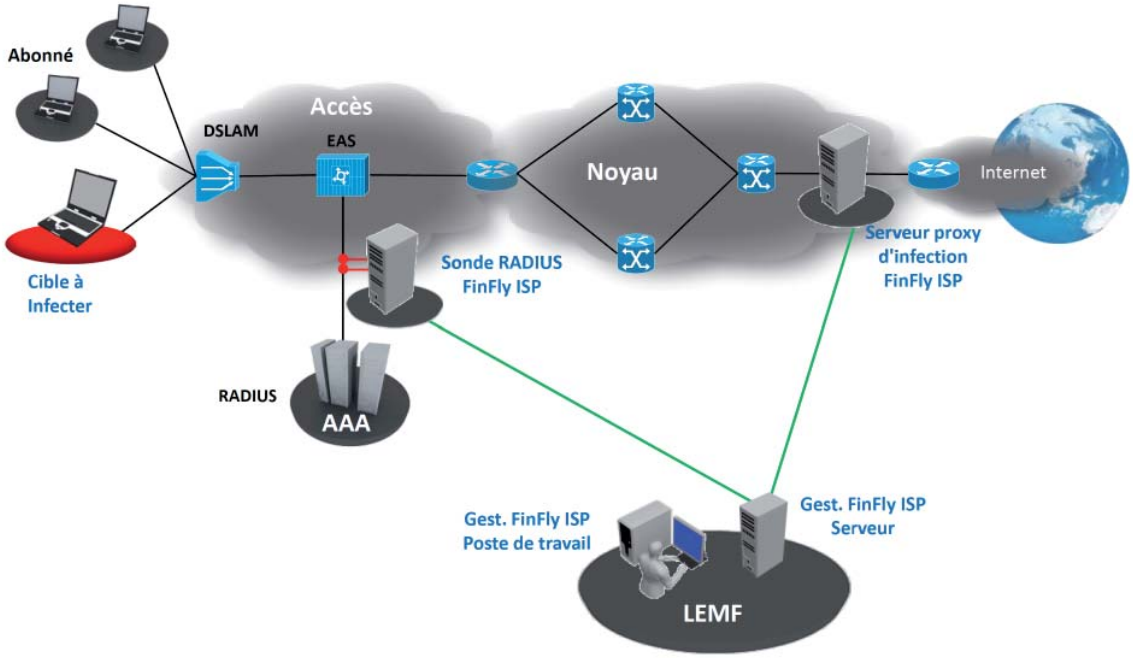
Une solution tactique est mobile. Le matériel est dédié aux tâches d'infection au sein du réseau d'accès près des points d'accès des cibles. Elle peut être déployée rapidement pour répondre aux exigences tactiques focalisées sur une cible précise ou un nombre réduit de cibles dans une zone particulière.

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

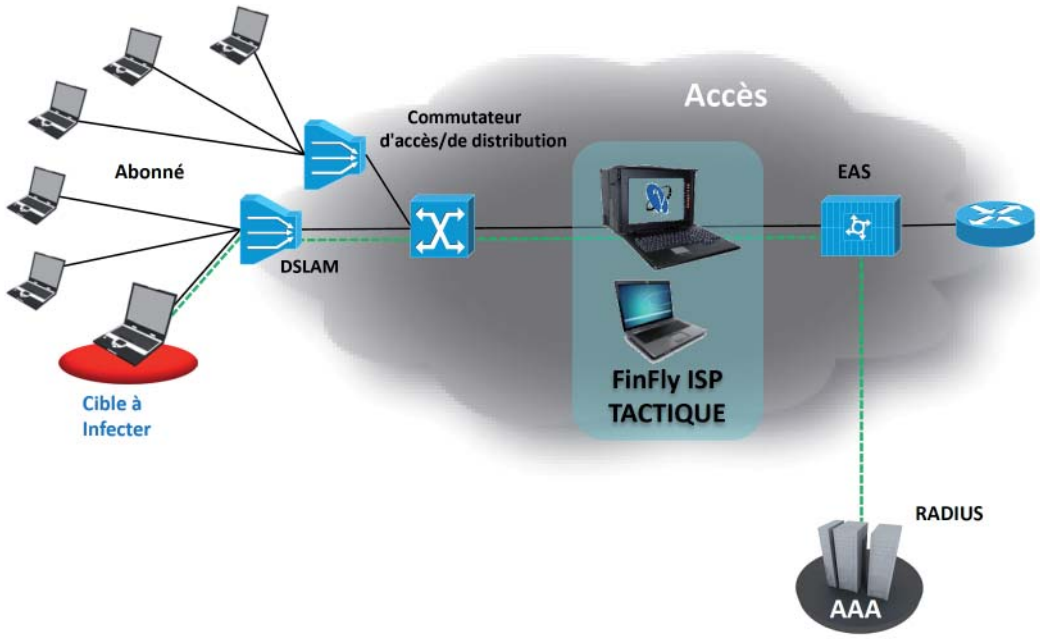
Il est bien sûr possible de combiner des solutions tactiques et stratégiques pour atteindre un maximum de souplesse au niveau des opérations d'infection.

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 d'infection au niveau, par exemple, de la ou des passerelles internet

Serveurs FinFly ISP
Poste de travail
HP ProLiant DL-Series G7
Business WS

FinFly ISP
HP Série Z

FinFly ISP Tactical

Un système FinFly ISP tactique consiste en ce qui suit :

- Serveur proxy d'identification et d'infection des cibles
- Ordinateur portable pour le système de gestion

FinFly ISP Tactique
Gestion Portable
Atlas A9 17" Portable

FinFly ISP Tactical
Lenovo Thinkpad
Série T

Les spécifications et données techniques peuvent être modifiées sans préavis.

Débit	> 20 Gbps
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

Débit	5 Gbits/s
Nb. max de cartes réseau :	3 cartes réseaux
Interfaces:	1GE cuivre / fibre SONET / SDH OC-3 / -12 STM-1 / -4 ATM AAL5
Processeurs :	2 x Intel Core i7
Noyau	6 cœurs par processeur
RAM:	12 Go
Capacité disque dur :	2 x 1 To SATA
Lecteur optique	DVD+/-RW SATA
Moniteur	1 x 17" TFT
Fonctionnalités	Fonction Bypass Switch pour les cartes réseau
Système d'exploitation	GNU Linux (Debian 5.0) durci

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

FINSUPPORT

FinSupport

L'assistance FinSupport fournit les mises à niveau et les mises à jours 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
  - Frontal de demande de nouvelles fonctionnalités

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

- Assistance technique via Skype :
  - 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 FinFisherTM 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.

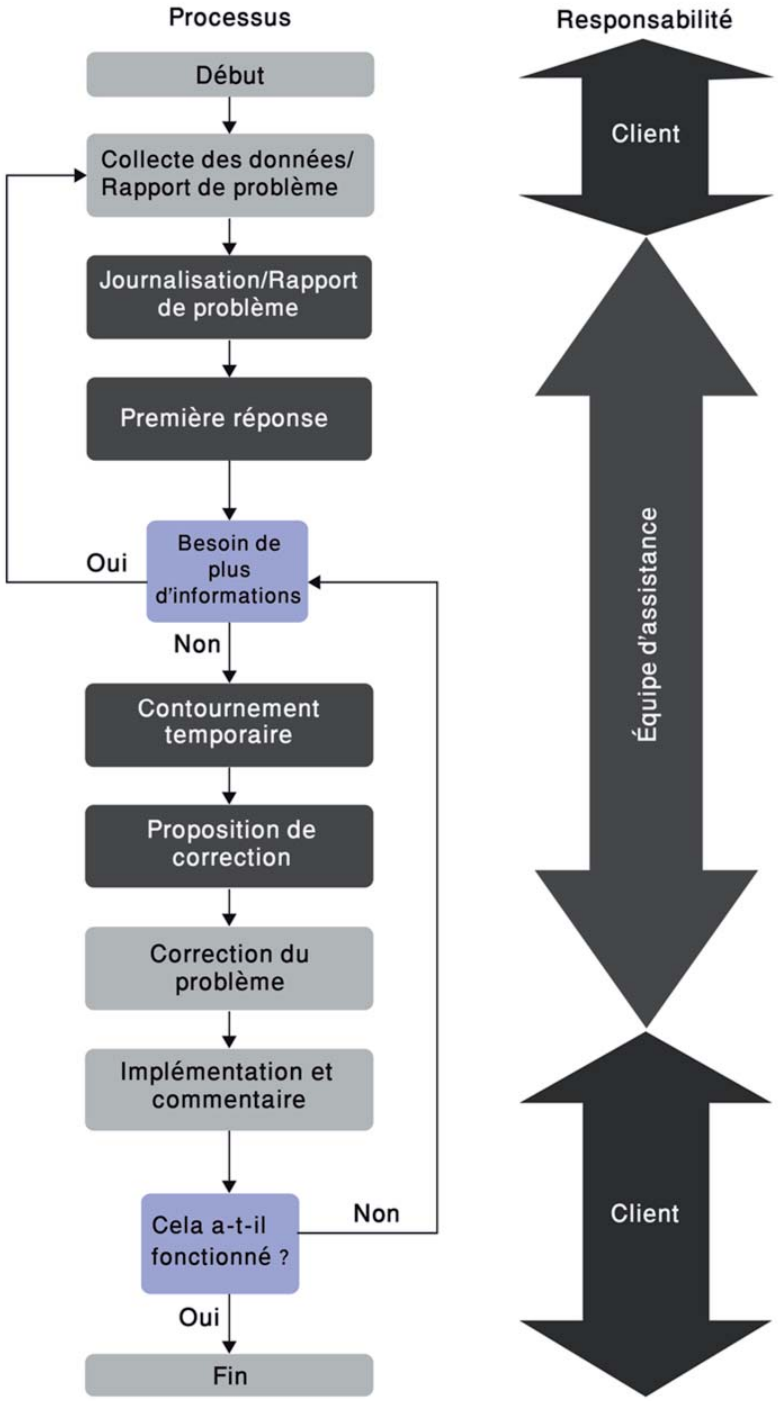
Corrections de bugs

FinSupport est une organisation d'assistance orientée produit. Un responsable service après-vente hautement qualifié traite les questions sur le produit par mail ou par téléphone. Le responsable du service après vente se trouve en Allemagne. Il est disponible de 9h00 à 17h00 CET (heure de l'Europe Centrale).
Avec FinLifelineSupport, l'assistance est accessible de 9h00 à 17h00 CET. Si une demande d'assistance est enregistrée en dehors des horaires de bureau habituels, cette demande sera traitée immédiatement le jour ouvrable suivant.

Lorsque le consommateur rapporte un incident, nous le notons dans un rapport d'incident, ou IR (Incident Report), et établissons la priorité de l'incident. Dans un délai déterminé, les actions correctives suivront en fonction de la priorité attribuée. L'équipe de FinFisher™ a alors la responsabilité de coordonner les recherches et la résolution de l'IR, et également de communiquer l'état et toute nouvelle information à l'auteur de l'IR.

Dans le cas de problèmes prioritaires, nous garantissons la continuité de fonctionnement du système en fournissant rapidement des solutions de contournement et des corrections de bugs testées. Lorsque l'équipe de FinFisher™ livre un contournement, en parallèle, elle fait aussi remonter le rapport de problème, ou PR (Problem Report), au Département R&D pour garantir une résolution rapide du problème. Ces mesures d'assistance professionnelle garantissent que le logiciel répond aux attentes les plus élevées.

Le schéma suivant illustre une procédure opérationnelle typique et les périmètres de responsabilité (remarque : dans ce schéma, « le client » représente l'auteur de l'IR) :



Le tableau suivant décrit la procédure normale de traitement d'un incident client :

Client	**Traitement des rapports d'incident (IR) et tâches correspondantes**
	FinFisher™ a mis à disposition une assistance par téléphone, fax ou mail pour rapporter les incidents.
En cas de soupçon d'anomalie logicielle/matérielle, la réception du rapport d'incident (IR) se fait suivant les méthodes de communication définies. L'IR doit comprendre : - le numéro de contrat - le nom du client - le système ou la technologie concerné(e) - la description de l'anomalie - la priorité (voir la définition ci-dessous) - les symptômes d'erreur constatés	
Le client peut être amené à fournir, sur demande, d'autres symptômes d'erreur	Sous un jour ouvrable, le client reçoit le numéro de ticket comme accusé de réception et pour le suivi de l'IR, ainsi que les premiers résultats d'analyse
	FinLifelineSupport prend en charge la collecte des symptômes d'erreur, sur demande
	FinLifelineSupport aide avec des solutions temporaires de contournement
	FinLifelineSupport fournit, après l'analyse de l'incident, une proposition de correction pour l'IR comprenant un planning des mesures correctives et un délai d'intervention
	FinLifelineSupport prévoit la livraison d'une correction logicielle ou matérielle, si l'incident signalé le nécessite
Le client applique la modification matérielle/logicielle. Le client confirme que la correction résout effectivement le problème.	FinLifelineSupport aide à la mise en œuvre de la modification matérielle(i)/logicielle.

(i) matériel facturé à part s'il n'est pas sous garantie.

Définitions de la priorité des demandes et des anomalies

FinLifelineSupport traite les demandes et les rapports de problèmes au fur et à mesure de leur arrivée et en fonction de leur urgence. Deux facteurs permettent d'évaluer l'urgence d'un incident, et ces deux facteurs sont inclus dans chaque IR :

- « Priorité » basée seulement sur la portée technique de l'erreur
- « La gravité pour le client » est un facteur plus objectif basé sur l'impact résultant pour le client

Le tableau des « Priorités » suivant fournit un aperçu de la portée technique correspondante :

Priorité	Définition	Exemple
1	problème critique : un élément essentiel du système ne fonctionne pas	Le proxy est en panne, ce qui empêche d'établir la communication avec la cible FinSpy.
2	problème majeur sans contournement	Une mise à jour d'antivirus détecte une solution d'écoute à distance déjà installée, laquelle nécessite une mise à jour immédiate afin de rester opérationnelle au sein du système infecté.
3	problème majeur avec contournement	La fonctionnalité de la cible FinSpy ne fonctionne pas correctement, mais peut être corrigée au moyen d'une solution de contournement.
4	problème mineur avec peu d'impact sur le système	Icône erronée pour un fichier téléchargé

Temps de réponse

Dans 90 % des incidents, notre temps de réponse s'inscrira dans les limites indiquées dans le tableau ci-dessous.

« Jour(s) ouvrable(s) » = tel(s) que défini(s) dans le calendrier allemand, étant ainsi exclus les jours considérés comme fériés en Allemagne.

Nos temps de réponse se décomposent en trois phases :

- Réponse initiale
- Résumé des actions correctives
- Résolution du problème (ou abaissement du niveau de priorité)

La durée de « réponse initiale » est le temps écoulé entre le moment où nous enregistrons un incident et le moment où nous envoyons au client l'accusé de réception de l'incident. Dans le cadre de la « réponse initiale », des informations plus détaillées peuvent être demandées ou, dans les cas moins complexes, le problème peut être résolu immédiatement.

Temps de réponse	Réponse initiale	Résumé des actions correctives	Résolution de PROBLÈMES (ou abaissement du niveau de PRIORITÉ)
Prio 1 - problème critique	Même jour ouvrable	1 jour ouvrable	2 jours ouvrables Remarque : En fonction du problème et des recherches nécessaires, la résolution du problème peut prendre plus de temps.
Prio 2 - problème majeur sans contournement	Même jour ouvrable	2 jours ouvrables	5 jours ouvrables Remarque : En fonction du problème et des recherches nécessaires, la résolution du problème peut prendre plus de temps.
Prio 3 - problème majeur avec contournement	Même jour ouvrable	3 jours ouvrables	14 jours ouvrables Remarque : En fonction du problème et des recherches nécessaires, la résolution du problème peut prendre plus de temps.
Prio 4 - problème mineur	Même jour ouvrable	7 jours ouvrables	prochaine mise à jour logicielle

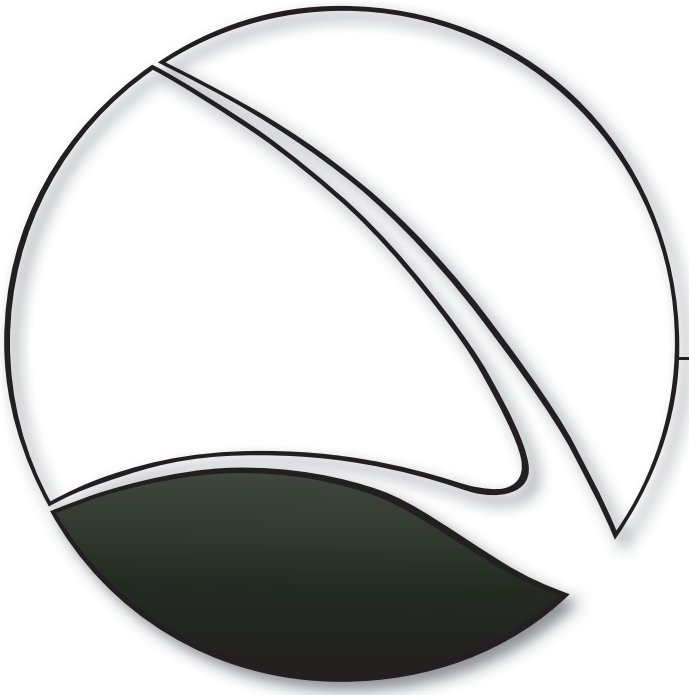
Mises à niveau logicielles

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).

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.GAMMAGROUP.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 les infrastructures informatiques, 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** prennent 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**.

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

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. Afin de garantir la complète utilisabilité du savoir-faire transféré, une **assistance opérationnelle locale** est prévue durant le programme.

Exemples de sujets abordés pendant la formation

- **Profilag** 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 d'hôtels
- **Intercepte 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
- Les sessions de formation pratique mettent l'accent sur les **opérations en condition réelle**
- **Conseil opérationnel** local

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

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

WWW.GAMMAGROUP.COM