

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

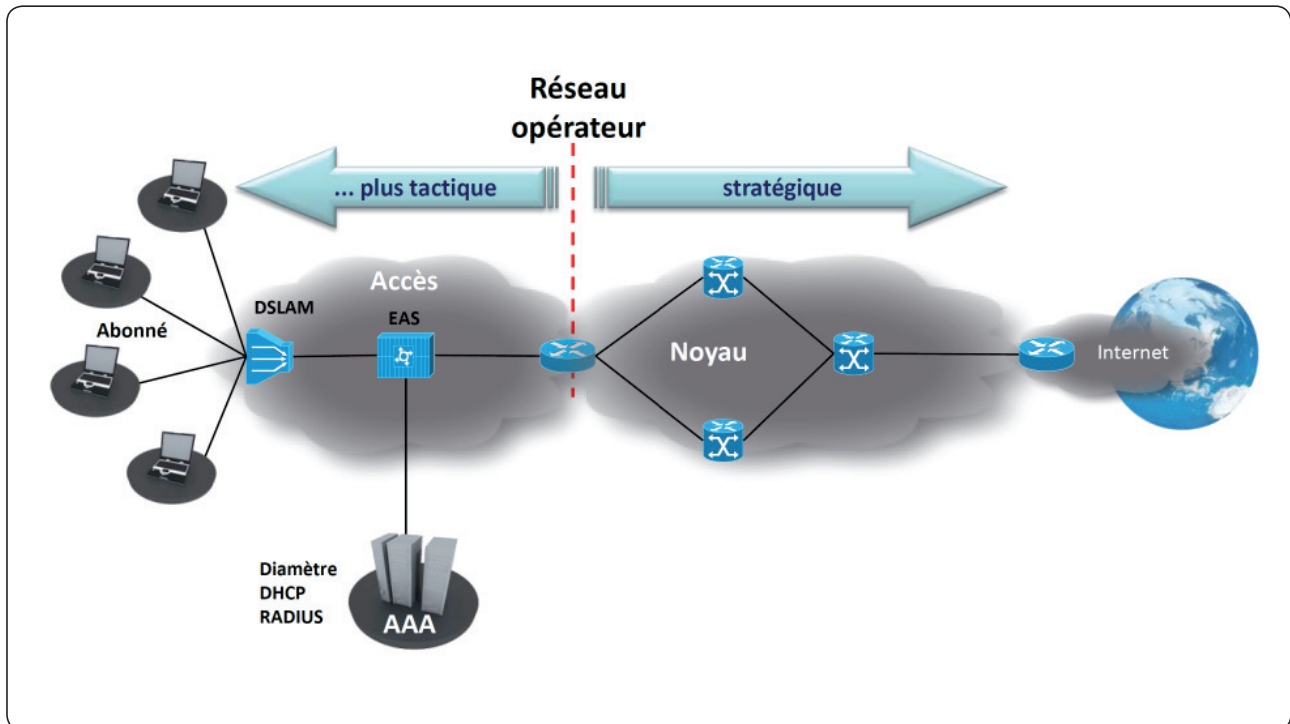
- Peut être installé au sein du **réseau de l'opérateur**
- Gère **tous les protocoles courants**
- Cibles sélectionnées **par adresse IP ou par compte Radius**
- Cache la solution d'écoute à distance dans les **téléchargements des cibles**
- Injecte une solution d'écoute à distance sous la forme de **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.

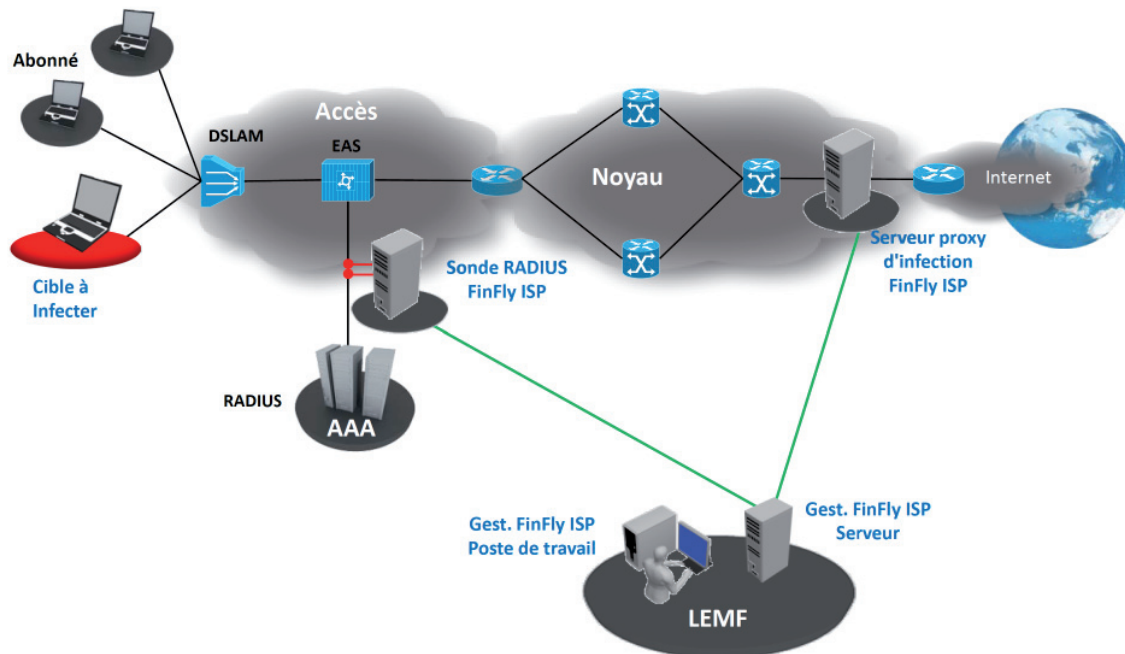
Une solution stratégique serait une installation permanente

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.

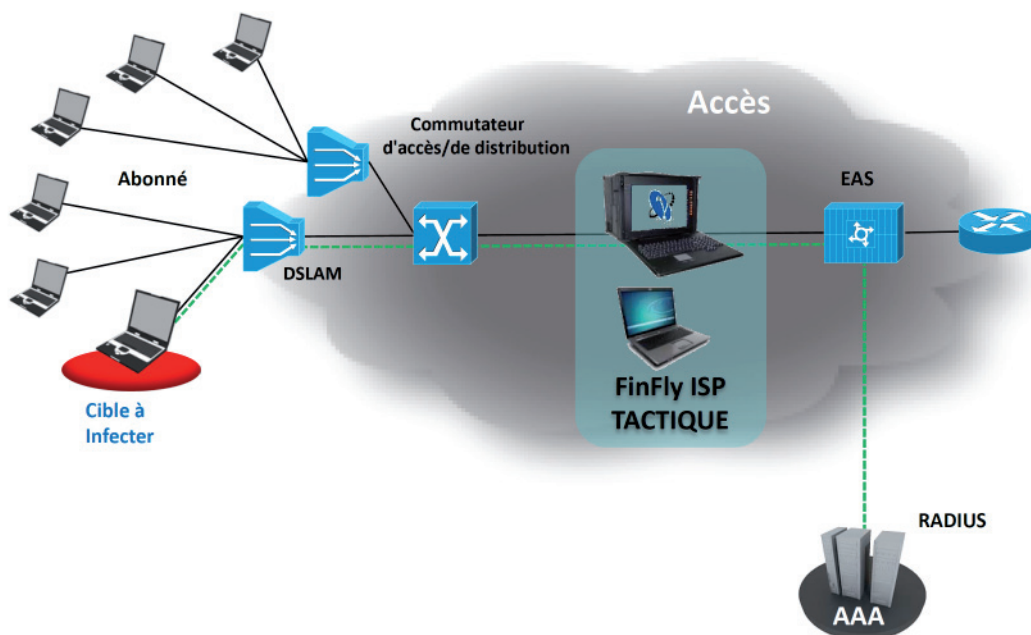
Il est bien sûr possible de combiner des solutions tactiques et stratégiques pour atteindre un maximum de souplesse au niveau des opérations d'infection.

Configuration réseau

Déploiement stratégique



Déploiement tactique



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



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

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



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

Les spécifications et données techniques peuvent être modifiées sans préavis.