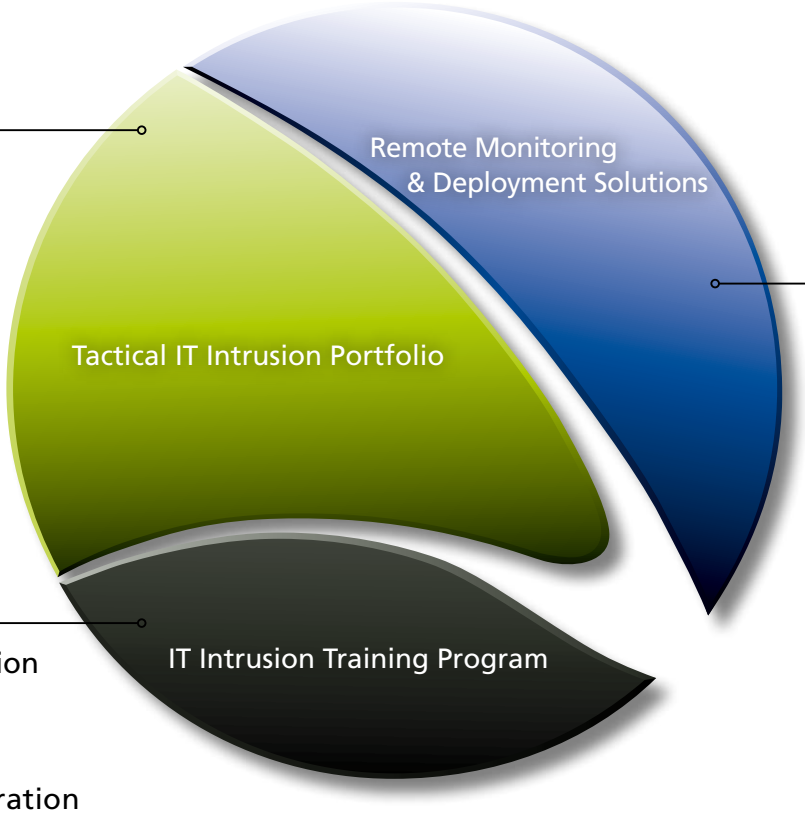
FINFISHER™: GOVERNMENTAL IT INTRUSION AND REMOTE MONITORING SOLUTIONS

WWW.FINFISHER.COM

FINFISHER™
IT INTRUSION



- FinIntrusion Kit
- FinUSB Suite
- FinFireWire

FinSpy
- FinSpy
- FinSpy Mobile

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

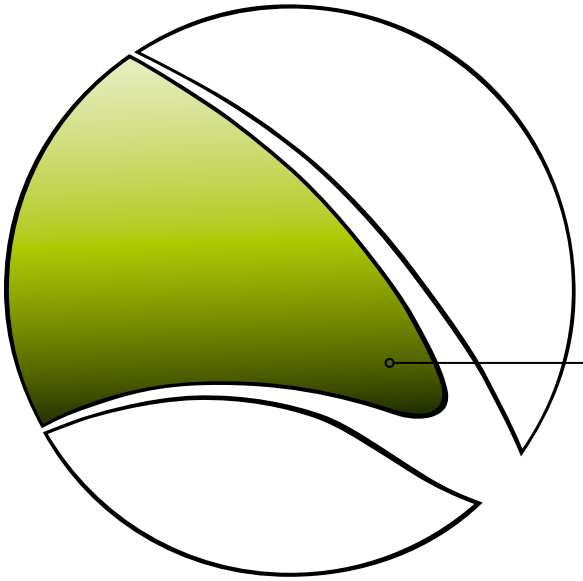
- Basic & Advanced Intrusion
- Wireless Intrusion
- Practical Exploitation
- Web Application Penetration
- Custom IT Intrusion Training & Consulting

Tactical IT Intrusion Portfolio

FININTRUSION KIT

FINUSB SUITE

FINFIREWIRE



Gamma addresses ongoing developments in the IT Intrusion field with solutions to enhance the capabilities of our clients. Easy to use high-end solutions and techniques complement the intelligence community's knowhow enabling it to address relevant Intrusion challenges on a tactical level.

FINFISHER™
IT INTRUSION

WWW.FINFISHER.COM

FINFINTRUSION KIT

FinIntrusion Kit was designed and developed by world-class IT Intrusion specialists, who have over 10 years of experience in their area through their work in several Tiger Teams (Red Teams) in the private and government sector assessing the security of different networks and organizations.

The FinIntrusion Kit is an **up-to-date and covert** operational Kit that can be used for most common **IT Intrusion Operations** in defensive and offensive areas. Current customers include **Military CyberWar Departments, Intelligence Agencies, Police Intelligence and other Law Enforcement Agencies**.

QUICK INFORMATION	
Usage:	· Strategic/Tactical Operations
Capabilities:	· Decodes WEP/WPA Encryption · Network Monitoring (including SSL Sessions) · IT Intrusion Attacks
Content:	· Hardware/Software

Usage Example 1: Technical Surveillance Unit

The FinIntrusion Kit was used to decode **the WPA encryption** of a Target's home Wireless network and then monitor his **Webmail (Gmail, Yahoo, ...) and Social Network (Facebook, MySpace, ...) credentials**, which enabled the investigators to **remotely monitor** these accounts from Headquarters without the need to be close to the Target.

Usage Example 2: IT Security

Several customers used the FinIntrusion Kit to successfully **bypass the security** of networks and computer systems for **offensive and defensive** purposes using various Tools and Techniques.

Usage Example 3: Strategic Use-Cases

The FinIntrusion Kit is widely used to remotely gain access to Target Email Accounts and Target Web-Servers and monitor their activities, including Access-Logs and more.

Feature Overview

- Discovers **Wireless LANs (802.11) and Bluetooth® devices**
- Recovers WEP (64 and 128 bit) Passphrases **within 2-5 minutes**
- **Breaks WPA1 and WPA2** Passphrases using Dictionary Attacks
- Actively monitors Local Area Network (Wired and Wireless) and **extracts Usernames and Passwords even for TLS/SSL-encrypted sessions**
- **Integrated WiFi Catcher** that can be combined with **Password monitoring functionalities**
- Remotely **breaks into Email Accounts** using Network-, System- and Password-based Intrusion Techniques
- **Network Security Assessment** and Validation

For a full feature list, please refer to the Product Specifications.

FININTRUSION KIT

Product Components

FinIntrusion Kit – Covert Tactical Unit

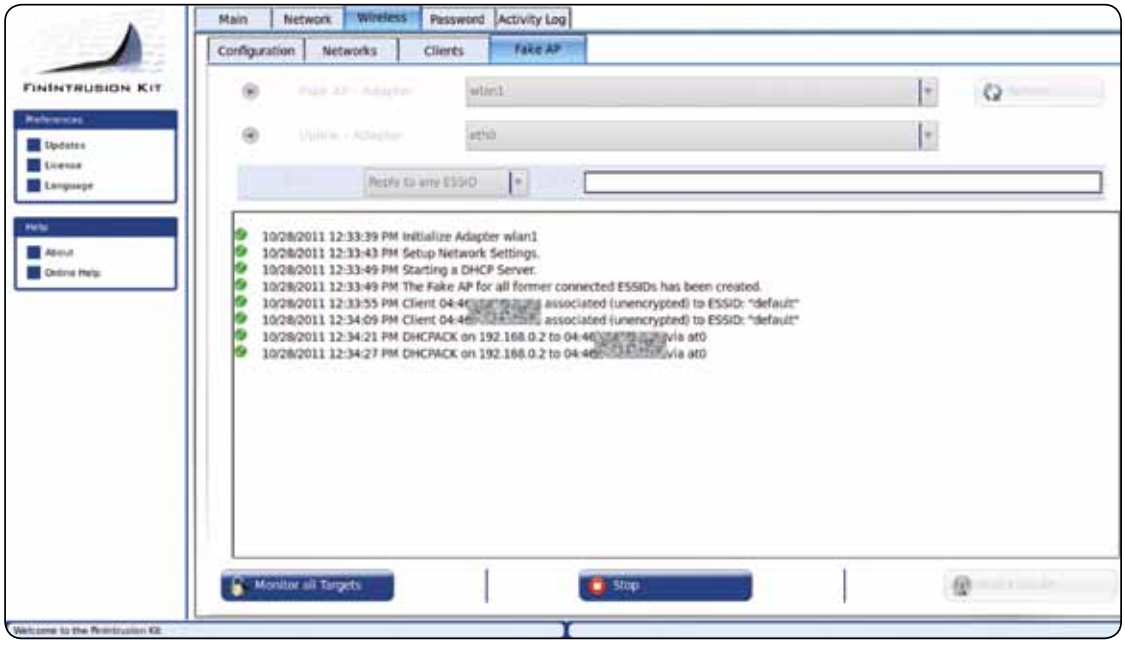
Basic IT Intrusion Components:
- High-Power WLAN Adapter
- High-Power Bluetooth Adapter
- 802.11 Antennas
- Many Common IT Intrusion devices

FinTrack Operation Center

- Graphical User Interface for Automated IT Intrusion Attacks

WiFi Catcher

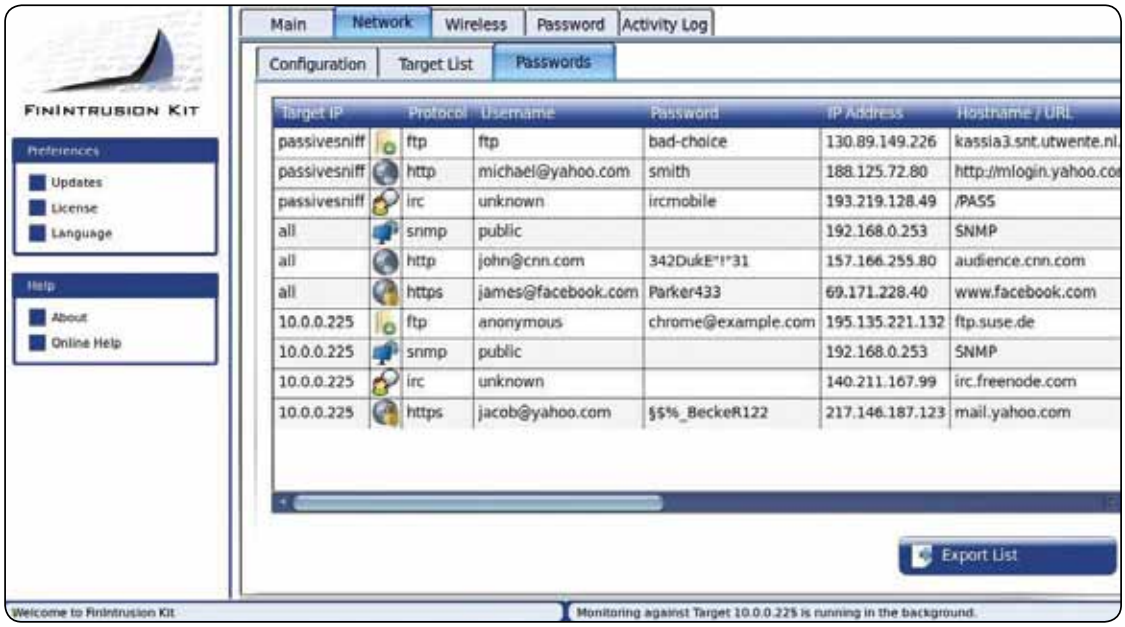
- Catches close-by WLAN Devices and records Traffic and Passwords.



FININTRUSION KIT

LAN/WLAN Active Password Sniffer

- Captures even SSL-encrypted data like Webmail, Video Portals, Online-Banking and more



FINUSB SUITE

The FinUSB Suite is a flexible product that enables Law Enforcement and Intelligence Agencies to quickly and securely extract forensic information from computer systems without the requirement of IT-trained Agents.

It has been used in successful operations around the world where valuable intelligence has been acquired about Targets in covert and overt operations.

QUICK INFORMATION	
Usage:	· Tactical Operations
Capabilities:	· Information Gathering · System Access · Quick Forensics
Content:	· Hardware/Software

Usage Example 1: Covert Operation

A source in an Organized Crime Group (OCG) was given a FinUSB Dongle that secretly extracted Account Credentials of Web and Email accounts and Microsoft Office documents from the Target Systems, while the OCG used the USB device to **exchange regular files** like Music, Video and Office Documents.

After returning the USB device to Headquarters, the gathered data could be decrypted, analyzed and used to constantly monitor the group remotely.

Usage Example 2: Technical Surveillance Unit

A Technical Surveillance Unit (TSU) was following a Target that frequently visited random Internet Cafés making monitoring with Trojan-Horse-like technology impossible. The FinUSB was used to extract the **data left on the public Terminals** used by the Target after the Target left.

Several documents that the Target opened in his web-mail could be recovered this way. The gathered information included crucial Office files, Browsing History through Cookie analysis, and more.

Feature Overview

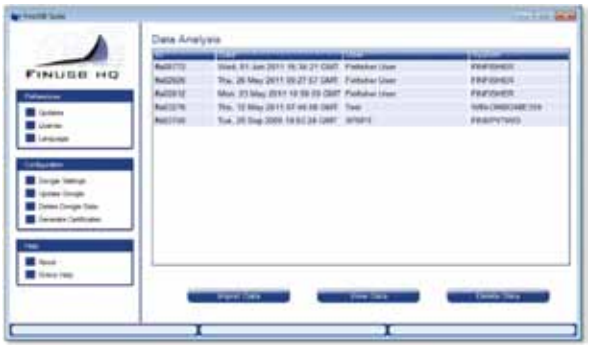
- Optimized for **Covert Operations**
- Easy usability through **automated Execution**
- Extraction of **Usernames and Passwords** for all common software like:
  - Email Clients
  - Messengers
  - Browsers
  - Remote Administration Tools
- **Silent Copying of Files** (Search Disks, Recycle-Bin, Last opened/edited/created)
- Extracting **Network Information** (Chat Logs, Browsing History, WEP/WPA(2) Keys, …)
- Compilation of **System Information** (Running/Installed Software, Hard-Disk Information, …)

For a full feature list, please refer to the Product Specifications.

FINUSB SUITE

Product Components

FinUSB Suite – Mobile Unit



FinUSB HQ

- Graphical User Interface to decrypt and analyze gathered Data
- Configure Dongle Operational Options

10 FinUSB Dongle (U3 - 16GB)

- Covertly extracts data from system

FinUSB – Windows Password Bypass

- Bypass Windows Logon without permanent system modifications

FINUSB SUITE

Easy Usability

1. Pick up a FinUSB Dongle
2. Configure all desired Features / Modules and update your FinUSB Dongle with FinUSB HQ
3. Go to your Target System
4. Plug in your FinUSB Dongle
5. Wait until all data is transferred
6. Go back to your FinUSB HQ
7. Import all Data from FinUSB Dongle
8. Generate Report

Professional Reports

FINFIREWIRE

Technical Surveillance Units and Forensic Experts often face a situation where they need to access a running computer system without shutting it down in order to prevent data loss or save essential time during an operation. In most cases, the Target System is protected with a **password-enabled Screensaver** or the target user is not logged in and the **Login Screen** is active.

FinFireWire enables the Operator to quickly and covertly **bypass the password-protected** screen and access the Target System without leaving a trace or harming essential forensic evidence.

QUICK INFORMATION	
Usage:	· Tactical Operations
Capabilities:	· Bypasses User Password · Covertly Accesses System · Recovers Passwords from RAM · Enables Live Forensics
Content:	· Hardware/Software

Usage Example 1: Forensic Operation

A **Forensic Unit** entered the apartment of a Target and tried to access the computer system. The computer was **switched on but the screen was locked.**
As they were not allowed, for legal reasons, to use a Remote Monitoring Solution, they would have **lost all data** by switching off the system as the **hard-disk was fully encrypted.** FinFireWire was used to **unlock the running Target System** enabling the Agent to **copy all files** before switching the computer off and taking it back to Headquarters.

Usage Example 2: Password Recovery

Combining the product with **traditional Forensic applications** like Encase®, Forensic units used the **RAM dump functionality** to make a snapshot of the current RAM information and **recovered the Hard-Disk encryption passphrase** for TrueCrypt's full disk encryption.

Feature Overview

- **Unlocks User-Logon** for every User-Account
- Unlocks **Password-Protected Screensaver**
- **Dumps full RAM** for Forensic analysis
- Enables live forensics **without rebooting** the Target System
- User password is **not changed**
- Supports **Windows, Mac OSX and Linux**
- Works with **FireWire/1394, PCMCIA and Express Card**

For a full feature list, please refer to the Product Specifications.

FINFIREWIRE

Product Components

FinFireWire – Tactical Unit

· Complete Tactical System

Point-and-Click User Interface

· Easy-to-use User Interface

Connection Adapter Cards

· PCMCIA and ExpressCard Adapter for Target Systems without FireWire port

Universal FinWire CableSet

· 4 pin to 4 pin
· 4 pin to 6 pin
· 6 pin to 6 pin

Usage

1. Go to your Target System

2. Start FinFireWire

3. Plug in FireWire Adapter & Cable

4. Select a Target

5. Wait until System is unlocked

FINSPY

FINSPY MOBILE

FINFLY USB

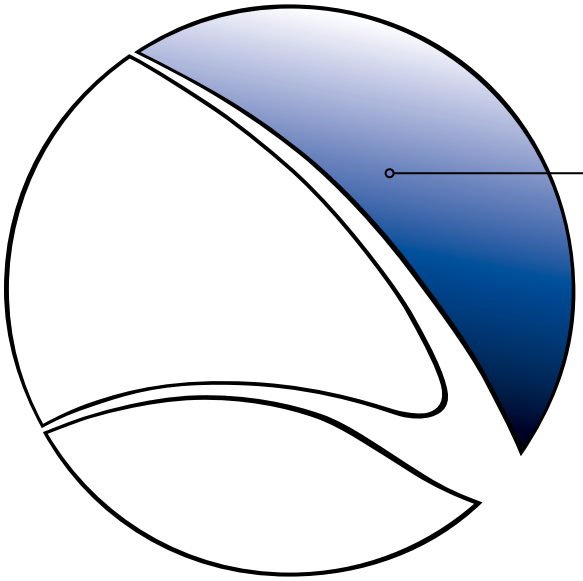
FINFLY LAN

FINFLY WEB

FINFLY EXPLOIT PORTAL

FINFLY ISP

FINFLY NET



The Remote Monitoring and Deployment Solutions are used to access target systems to give full access to stored information with the ability to take control of target system's functions to the point of capturing encrypted data and communications. When used in combination with enhanced remote deployment methods, Government Agencies will have the capability to remotely deploy software on target systems.

FINSPY

FinSpy is a field-proven Remote Monitoring Solution that enables Governments to face the current challenges of **monitoring Mobile and Security-Aware Targets** that regularly **change location**, use **encrypted and anonymous communication** channels and **reside in foreign countries**.

Traditional Lawful Interception solutions **face new challenges** that can only be **solved using active systems** like FinSpy:

- Data not transmitted over any network
- Encrypted Communications
- Targets in foreign countries

FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

QUICK INFORMATION	
Usage:	· Strategic/Tactical Operations
Capabilities:	· Remote Computer Monitoring · Monitoring of Encrypted Communications
Content:	· Hardware/Software

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communications** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Feature Overview

Target Computer – Example Features:

- Bypassing of 40 regularly tested Antivirus Systems
- **Covert Communication** with Headquarters
- Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)
- Recording of **common communications** like Email, Chats and Voice-over-IP
- **Live Surveillance** through Webcam and Microphone
- **Country Tracing** of Target
- **Silent extracting of Files** from Hard-Disk
- **Process-based Key-logger** for faster analysis
- **Live Remote Forensics** on Target System
- **Advanced Filters** to record only important information
- Supports most common Operating Systems (**Windows, Mac OSX** and **Linux**)

Headquarters – Example Features:

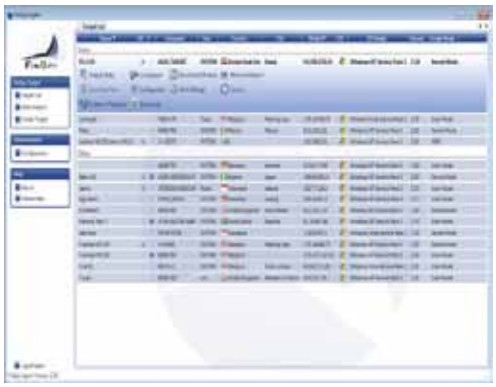
- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Hidden from Public through **Anonymizing Proxies**
- Can be **fully integrated** with Law Enforcement Monitoring Functionality

For a full feature list, please refer to the Product Specifications.

Product Components

FinSpy Master and Proxy

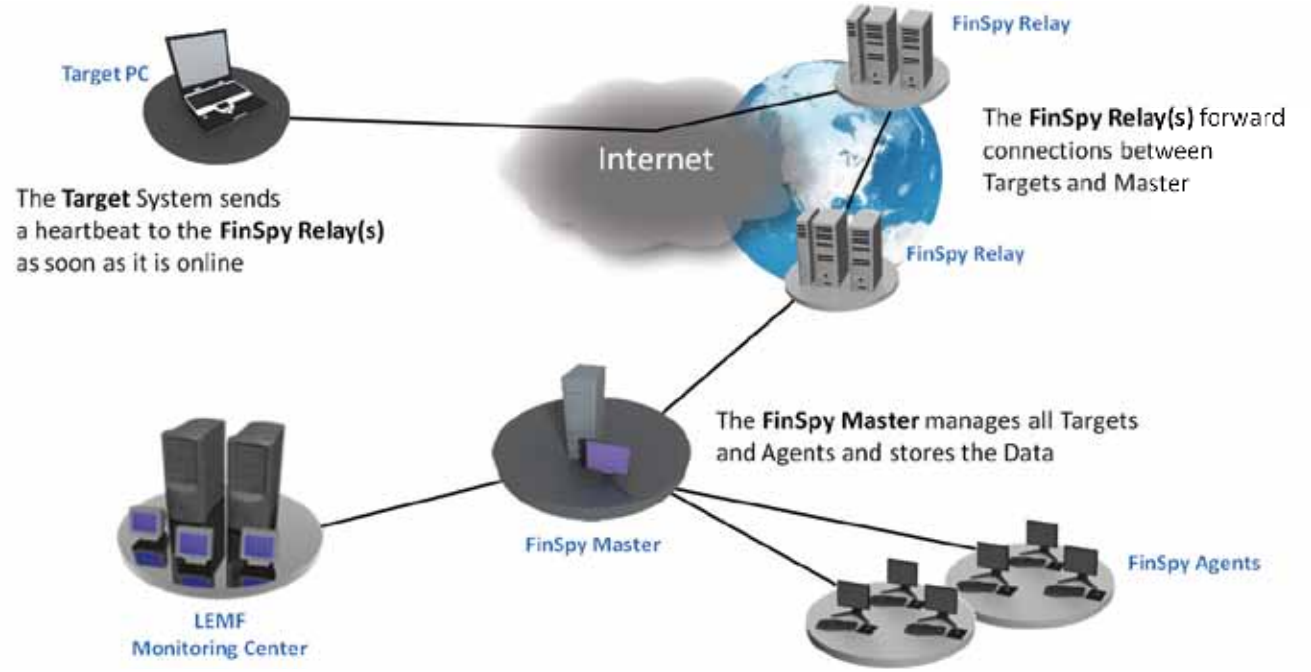
- Full Control of Target Systems
- Evidence Protection for Data and Activity Logs
- Secure Storage
- Security-Clearance based User and Target Management



FinSpy Agent

- Graphical User Interface for Live Sessions
- Configuration and Data Analysis of Targets

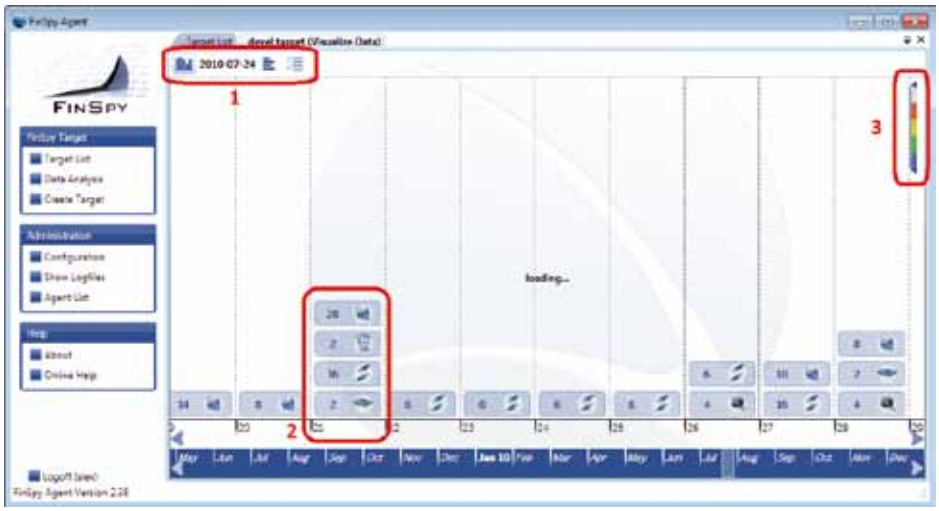
Access Target Computer Systems around the world



Easy-to-use User Interface

Live and Offline Target Configuration

Full Intelligence on Target System



1. Multiple Data Views
2. Structured Data Analysis
3. Importance Levels for all Recorded Files

FINSPY MOBILE

FinSpy Mobile is closing the gap of interception capabilities for Governments for most common **smartphone platforms**.

Specifically, organizations **without network or off-air based interception** capabilities can access Mobile Phones and intercept the devices with enhanced capabilities. Furthermore, the solution offers **access to encrypted communications** as well as **data stored on the devices** that is not transmitted.

Traditional tactical or strategic Interception solutions **face challenges** that can only be **solved using offensive systems** like FinSpy Mobile:

- Data not transmitted over any network and kept on the device
- Encrypted Communications in the Air-Interface, which avoid the usage of tactical active or passive Off-Air Systems
- End-to-end encryption from the device such as Messengers, Emails or PIN messages

FinSpy Mobile has been giving successful results to Government Agencies who gather information **remotely from Target Mobile Phones**.

When FinSpy Mobile is installed on a mobile phone it can be **remotely controlled and monitored** no matter where in the world the Target is located.

QUICK INFORMATION	
Usage:	· Strategic/Tactical Operations
Capabilities:	· Remote Mobile Phone Monitoring
Content:	· Hardware/Software

Usage Example 1: Intelligence Agency

FinSpy Mobile was deployed on **BlackBerry mobile phones** of several Targets to monitor all communications, including **SMS/MMS, Email and BlackBerry Messenger**.

Usage Example 2: Organized Crime

FinSpy Mobile was **covertly deployed on the mobile phones** of several members of an Organized Crime Group (OCG). Using the **GPS tracking** data and **silent calls**, essential information could be gathered from **every meeting that was held** by this group.

Feature Overview

Target Phone – Example Features:

- **Covert Communications** with Headquarters
- Recording of **common communications** like Voice Calls, SMS/MMS and Emails
- **Live Surveillance** through silent Calls
- **File Download** (Contacts, Calendar, Pictures, Files)
- **Country Tracing** of Target (GPS and Cell ID)
- Full Recording of all **BlackBerry Messenger communications**
- Supports most common Operating Systems: **Windows Mobile/Phone, iOS (iPhone), BlackBerry OS, Android** and **Symbian**

Heaquarters – Example Features:

- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Hidden from Public through **Anonymizing Proxies**
- Can be **fully integrated** with Law Enforcement Monitoring Functionality

For a full feature list, please refer to the Product Specifications.

FINSPY MOBILE

Product Components

FinSpy Master and Proxy

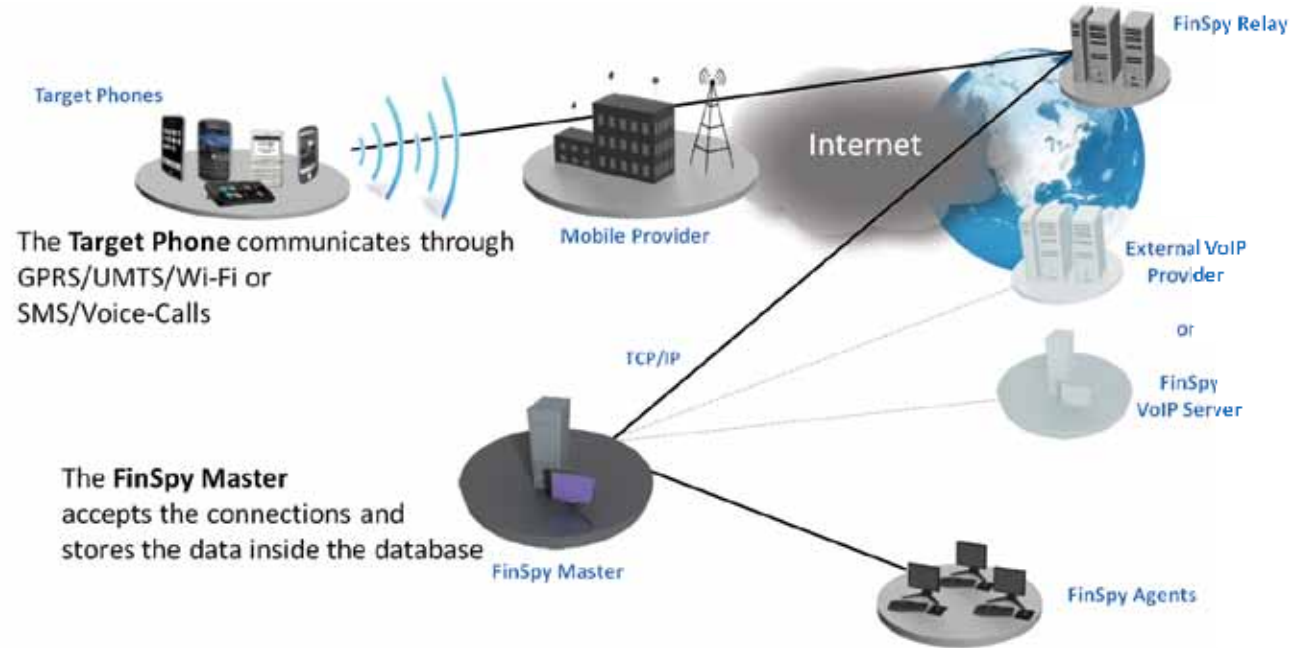
- Full Control of Target Systems
- Evidence Protection for Data and Activity Logs
- Secure Storage
- Security-Clearance based User and Target Management

FinSpy Agent

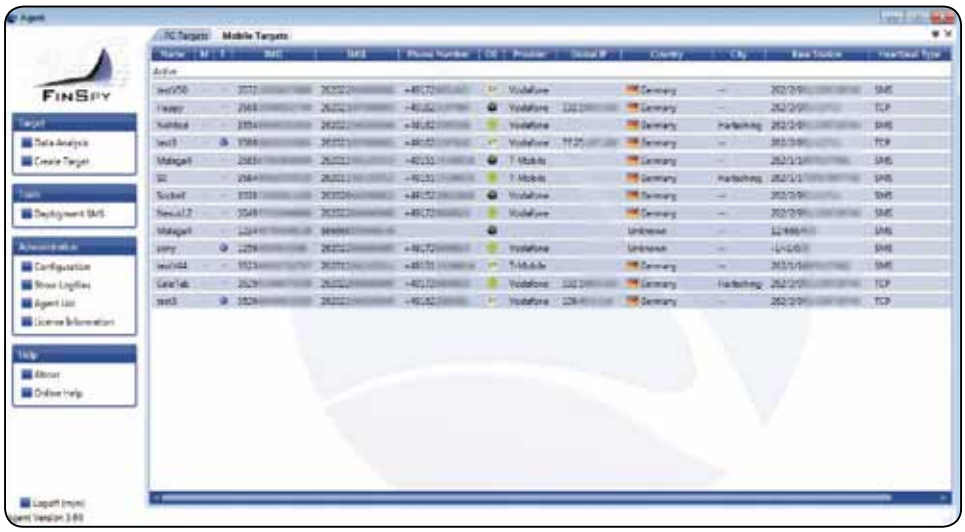
- Graphical User Interface for Live Sessions
- Configuration and Data Analysis of Targets

FINSPY MOBILE

Access Target Mobile Phones around the world

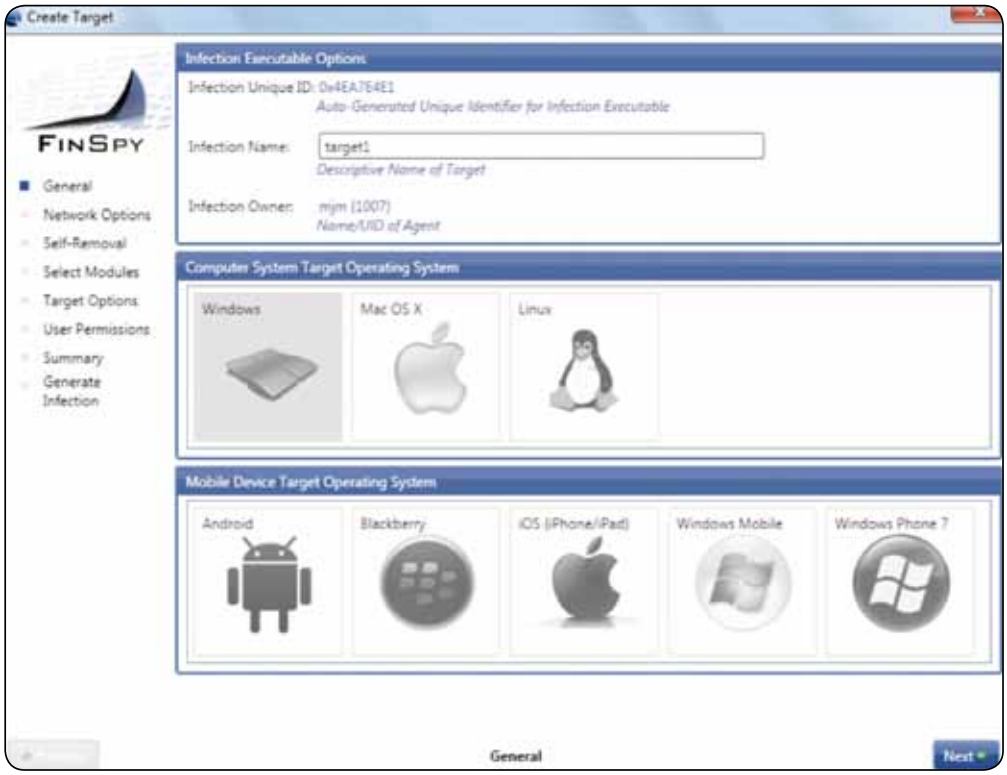


Easy-to-use User Interface



FINSPY MOBILE

Supports all common Mobile Platforms



FINFLY USB

The FinFly USB provides an easy-to-use and reliable way of installing Remote Monitoring Solutions on computer systems when physical access is available.

Once the FinFly USB is inserted into a computer, it **automatically installs the configured software** with little or no user-interaction and **does not require IT-trained Agents** when being used in operations. The FinFly USB can be used against **multiple systems** before being returned to Headquarters.

QUICK INFORMATION	
Usage:	· Tactical Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target
Content:	· Hardware

Usage Example 1: Technical Surveillance Unit

The FinFly USB was successfully used by **Technical Surveillance Units** in several countries to deploy a Remote Monitoring Solution onto Target Systems that were switched off, by simply **booting the system from the FinFly USB device**. This technique worked even for Target Systems that had **full hard-disk encryption** with products like TrueCrypt enabled.

Usage Example 2: Intelligence Agency

A Source in a domestic terror group was given a FinFly USB that **secretly installed a Remote Monitoring Solution** on several computers of the group when they were using the device to exchange documents between each other. The Target Systems could then be **remotely monitored from Headquarters,** and the FinFly USB was later returned by the Source.

Feature Overview

- Can deploy even on **powered off systems with full hard-disk encryption** (e.g. TrueCrypt)
- **Covertly installs Remote Monitoring Solution** on insertion in Target System
- **Little or no user-interaction** is required
- Functionality can be **concealed by placing regular files** like music, video and office documents on the device
- Hardware is a **common and non-suspicious USB device**

For a full feature list, please refer to the Product Specifications.

FINFLY USB

Product Components

FinFly USBs

- USB Dongle
- Deploys a Remote Monitoring Solution on Insertion into Target Systems
- Deploys Remote Monitoring Solution during Boot Process

Full FinSpy Integration

- Automatic generation and activation through FinSpy Agent

FINFLY LAN

Some of the major challenges Law Enforcement Agencies are facing are **mobile Targets**, where **no physical access** to a computer system can be achieved and Targets **do not open any Files** which have been sent via email to their accounts.

In particular, security-aware Targets are **almost impossible to monitor** as they keep their systems **up-to-date** and **no exploits** or Basic Intrusion techniques will lead to success.

FinFly LAN was developed to deploy a Remote Monitoring Solution covertly on Target Systems in Local Area Networks (Wired and Wireless/802.11). It is able to **patch Files that are downloaded** by the Target on-the-fly, **send fake Software Updates** for popular Software or **inject the Payload into visited Websites**.

QUICK INFORMATION	
Usage:	· **Tactical Operations**
Capabilities:	· **Deploys Remote Monitoring Solution on Target System in Local Area Network**
Content:	· **Software**

Usage Example 1: Technical Surveillance Unit

A Technical Surveillance Unit was following a Target for weeks without being able to physically access the target computer. They used FinFly LAN to install the Remote Monitoring Solution on the Target System while he was using a **public Hotspot** at a coffee shop.

Usage Example 2: Anti-Corruption

FinFly LAN was used to remotely install the Remote Monitoring Solution on the computer of a Target while he was using it **inside his hotel room**. The Agents were in another room **connected to the same network** and manipulated the Websites the Target was visiting to trigger the installation.

Feature Overview

- **Discovers all computer systems** connected to Local Area Network
- Works in **Wired and Wireless (802.11)** networks
- Can be combined with FinIntrusion Kit for **covert Network access**
- Hides Remote Monitoring Solution in **Downloads of Targets**
- Injects Remote Monitoring Solution as **Software Updates**
- Remotely installs Remote Monitoring Solution through **Websites visited by the Target**

For a full feature list, please refer to the Product Specifications.

FINFLY LAN

Product Components

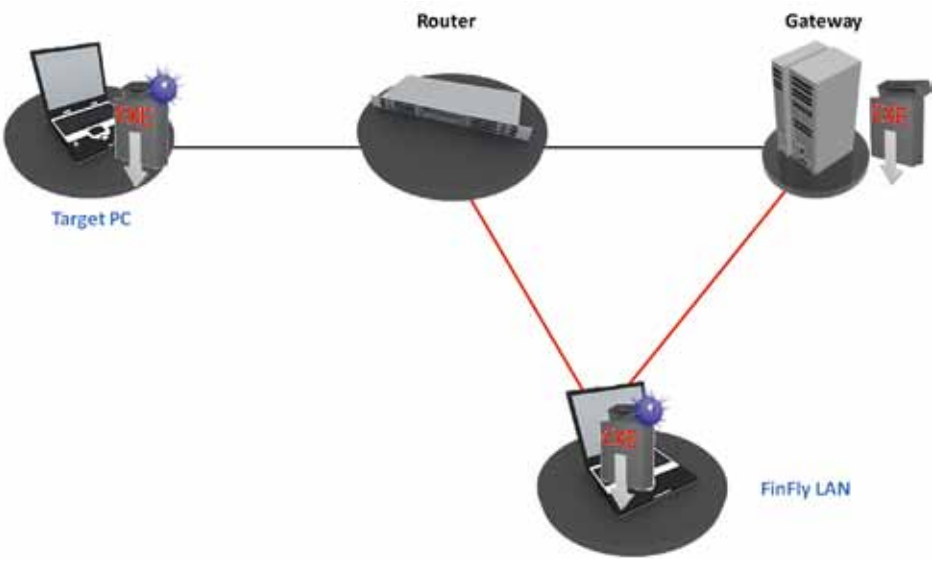
FinFly LAN

- Linux-based Software with simple User-Interface

FinIntrusion Kit - Integration (optional)

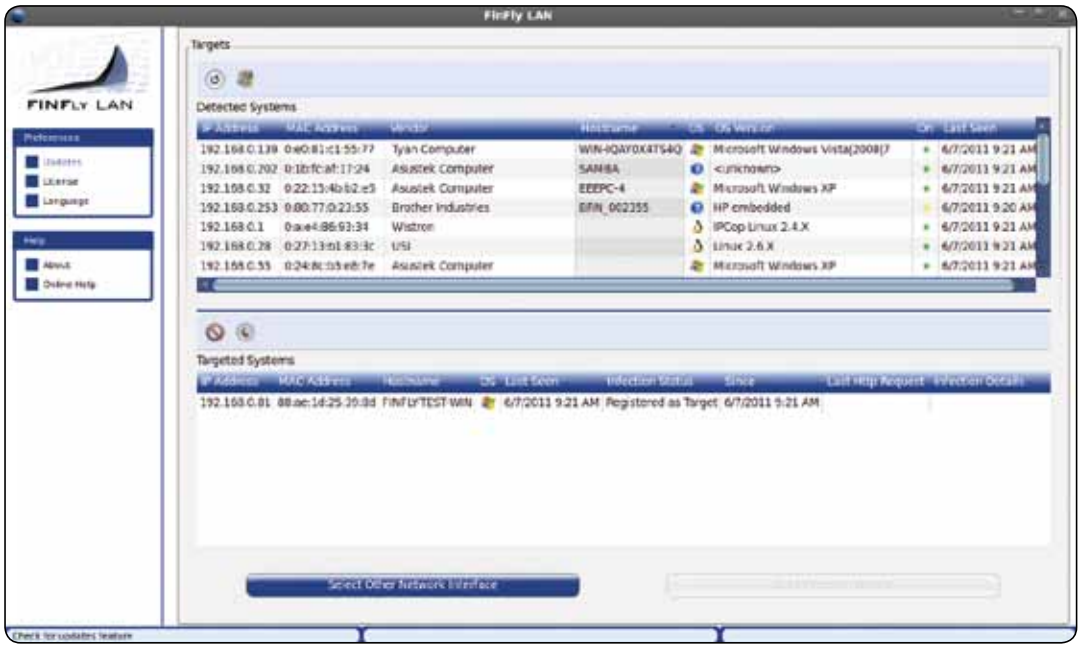
- FinFly LAN will be loaded as a module into the FinIntrusion Kit

Deployment through Local Area Networks



Automated User-Interface

· Simple to use without extensive training



Multiple-Target and Payload Support

· Different Executables can be added for each Target

FINFLY WEB

One of the major challenges in using a Remote Monitoring Solution is to install it onto the Target System, especially when only a little information, like an **Email-address**, is available and **no physical access** can be achieved.

FinFly Web is designed to provide **remote and covert** deployment on a Target System by using a wide range of **web-based attacks**.

FinFly Web provides a **point-and-click interface**, enabling the Agent to easily **create a custom deployment code** according to selected modules.

The Payload will be deployed when the Target System visits the prepared website with the customized code.

QUICK INFORMATION	
Usage:	· **Strategic Operations**
Capabilities:	· **Deploys Remote Monitoring Solution on Target System through Websites**
Content:	· **Software**

Usage Example 1: Technical Surveillance Unit

After profiling a Target, the unit created a **website of interest** for the Target and sent him the **link through a discussion board**. Upon opening the Link to the unit's website, a Remote Monitoring Solution was installed on the Target System and the Target was **monitored from within Headquarters**.

Usage Example 2: Intelligence Agency

A customer deployed **FinFly ISP within the main Internet Service Provider** of his country. It was **combined with FinFly Web** to remotely **deploy the payload when the Target visited a trusted website**.

Feature Overview

- **Fully-Customizable** Web Modules
- Can be covertly **installed into every Website**
- Full integration with **FinFly LAN, FinFly NET** and **FinFly ISP** to deploy even inside popular Websites, like Webmail, Video Portals, and more
- Installs Remote Monitoring Solution **even if only email address is known**
- Possibility to target every person visiting **configured Websites**

For a full feature list, please refer to the Product Specifications.

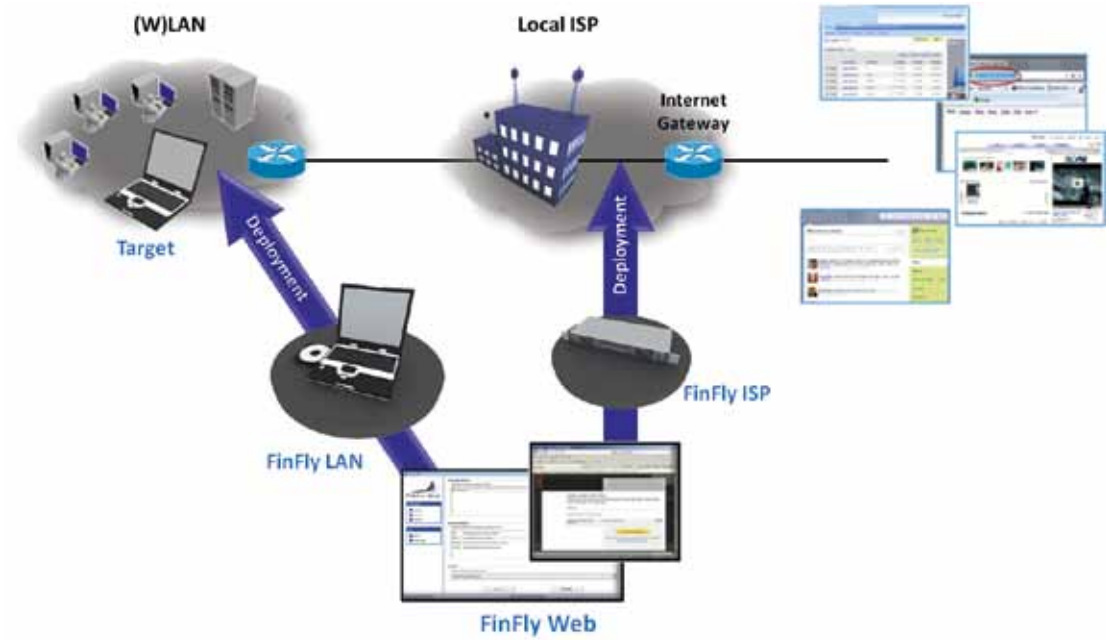
FINFLY WEB

Product Components

FinFly Web

· Custom Website Generator

Full integration with FinFly LAN and FinFly ISP



FINFLY EXPLOIT PORTAL

Standard Deployment methods for Remote Monitoring Solutions can **often not be applied** when dealing **with well-trained and extremely careful Targets** as they are familiar with common Deployment techniques and tools.

In most scenarios, **0-Day Exploits** provide an extremely powerful and **reliable way to deploy Remote Monitoring Solutions** by exploiting **unpatched vulnerabilities** in Software the Target is using.

The FinFly Exploit Portal offers access to **a large library** of 0-Day and 1-Day Exploits for popular software like **Microsoft® Office, Internet Explorer, Adobe Acrobat Reader, and many more**.

QUICK INFORMATION	
Usage:	· **Strategic Operations**
Capabilities:	· **Deploys Remote Monitoring Solution on Target System through Files and Server**
Content:	· **Web Portal**

Usage Example 1: High-Tech Crime Unit

A High-Tech Crime Unit was **investigating a Cyber-Crime** and needed to deploy a Remote Monitoring Solution on a Target System. They used an Adobe Acrobat Reader 0-Day Exploit and sent a prepared PDF file via Email to the Target. The Remote Monitoring Solution was automatically deployed once the Target opened the file.

Usage Example 2: Intelligence Agency

A Target was identified **within a Discussion Board** but no direct or Email contact was possible. The Agency created a Webserver containing an **Internet Explorer 0-day Exploit** which deployed the Payload on the Target System **once the Target opened the URL** that was sent to him through a private message in the Discussion Board.

Feature Overview

- Full Access to **Web Portal and Exploit Generator**
- **Government-Grade 0-Day Exploits** which function on multiple Systems and Patch-levels **without further modification**
- At least **4 major Exploits** (common Browser/Mail/File-Viewer Software) permanently available
- **30 day warranty** for every Exploit within the Portal
- Permanently updated **1-Day Exploits** for various Software

For a full feature list, please refer to the Product Specifications.

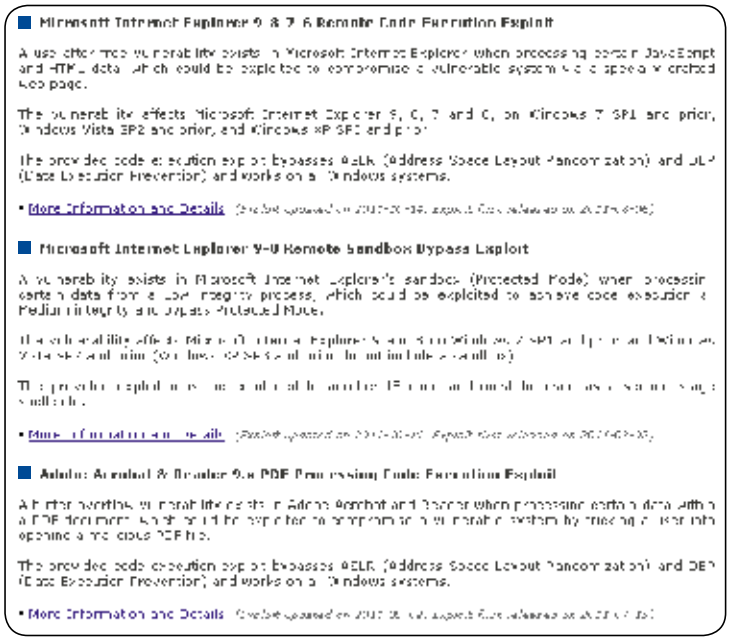
FINFLY EXPLOIT PORTAL

Product Components

FinFly Exploit Portal

- Web Interface Exploit Library

FinFly Exploit Portal Sample



FINFLY ISP

In many real-life operations, physical access to in-country Target Systems cannot be achieved, and a covert **remote installation** of a Remote Monitoring Solution is required to be able to **monitor the Target from within Headquarters**.

FinFly ISP is a strategic, **countrywide, as well as a tactical** (mobile) solution, that can be **integrated into an ISP's Access and/or Core Network**, to remotely install the Remote Monitoring Solution on selected Target Systems.

FinFly ISP appliances are based on **carrier grade server technology**, providing a maximum of **reliability and scalability** to meet almost every challenge related to networks' topologies. A wide range of Network Interfaces – all **secured with bypass functions** – is available for the required active network connectivity.

Several passive and active methods of Target Identification – from **online monitoring** via passive tapping to **interactive communication** between FinFly ISP and the AAA-Servers – ensure that the Targets are identified and their appropriate traffic will be provided for the deployment process.

FinFly ISP is able to **patch Files** that are downloaded by the Target **on-the-fly or send fake Software Updates** for popular Software. The new release integrates Gamma's powerful remote deployment application **FinFly WEB** that injects a Payload to any website visited by the Target.

QUICK INFORMATION	
Usage:	· Strategic Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target System through ISP Network
Content:	· Hardware/Software

Usage Example: Intelligence Agency

FinFly ISP was deployed in the main Internet Service Provider networks of the country and was actively used to remotely deploy a Remote Monitoring Solution on Target Systems. As the Targets have Dynamic-IP DSL Accounts, they are identified with their Radius Logon Name.

Feature Overview

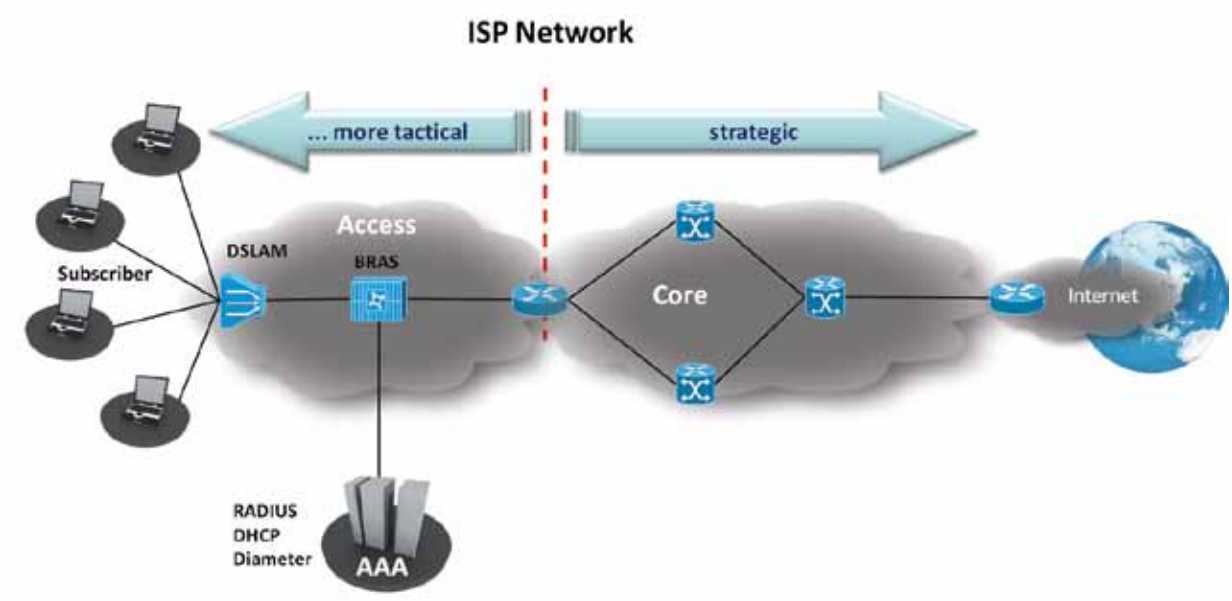
- Can be installed inside an **Internet Service Provider´s Networks**
- Handles **all common Protocols**
- Selected Targets by **IP Address, Radius Login Name, DHCP and MSISDN**
- Hides Remote Monitoring Solution in **Downloads of Targets**
- Injects a Remote Monitoring Solution as **Software Updates**
- Remotely installs a Remote Monitoring Solution through **Websites visited by the Target**

For a full feature list, please refer to the Product Specifications.

FINFLY ISP

Different Location Possibilities

- FinFly ISP can be used as a tactical or strategic solution within ISP networks



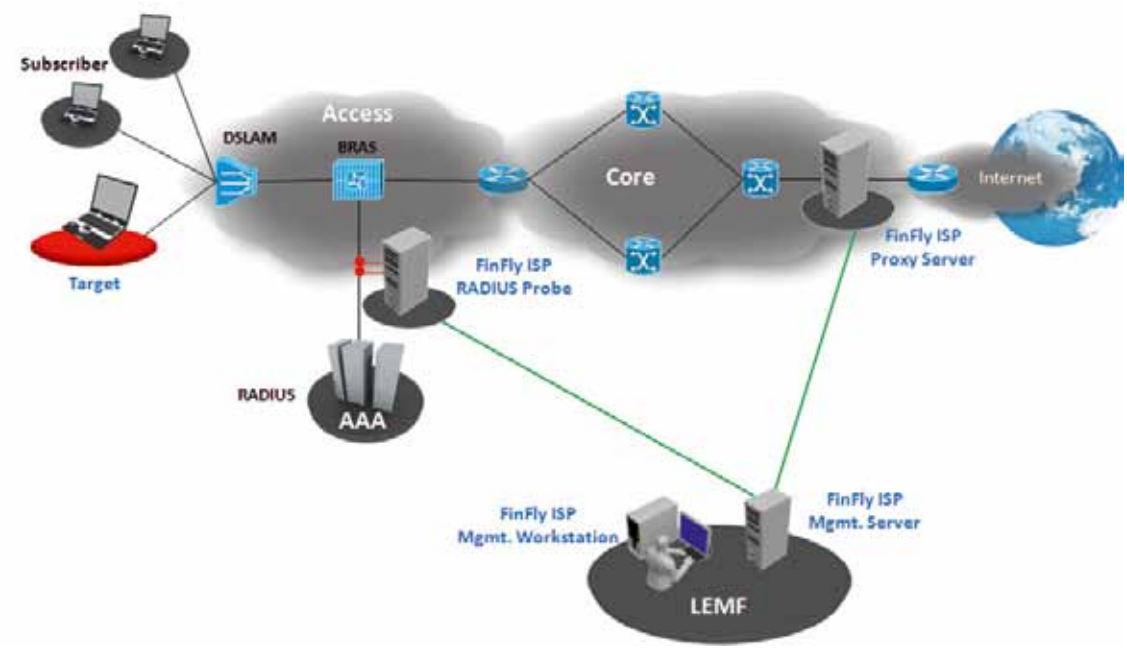
A tactical solution is mobile and the hardware is dedicated to the deployment tasks inside the access network close to the targets' access points. It can be deployed on a short-term basis to meet tactical requirements focused on a specific target or a small number of targets in an area.

A strategic solution would be a permanent ISP/countrywide installation of FinFly ISP to select targets and deploy payloads from the remote headquarters without the need for the LEA to be on location.

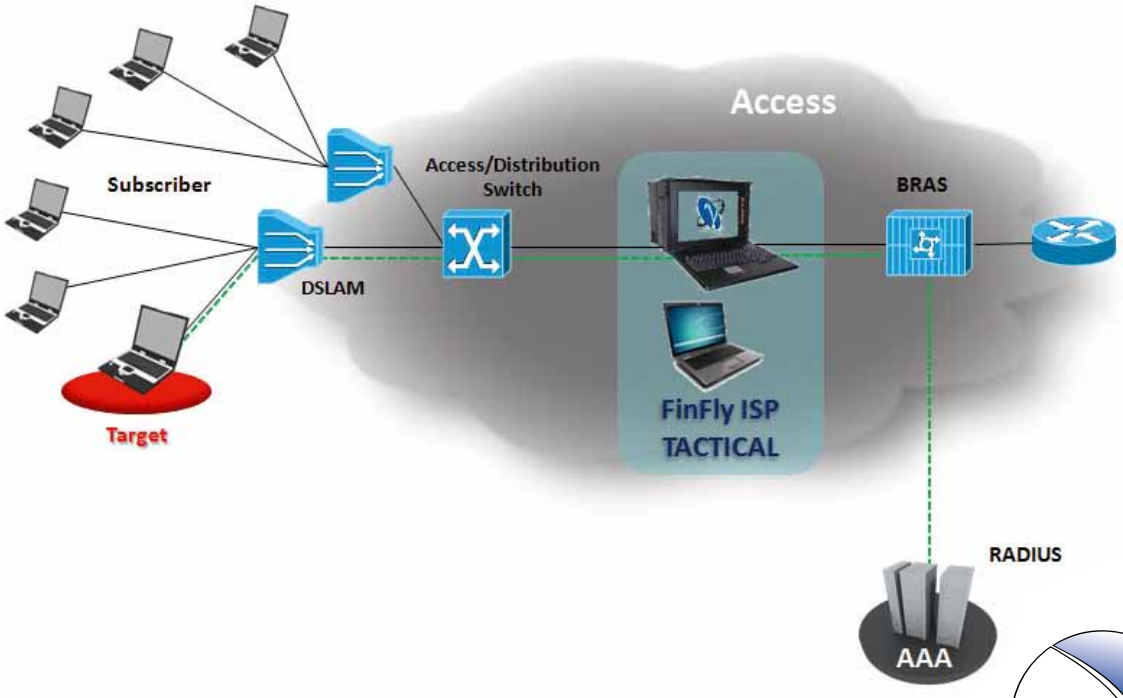
Of course, it is possible to combine tactical and strategic solutions to reach a maximum of flexibility for the deployment operations.

Network Setup

Strategic Deployment



Tactical Deployment



FINFLY ISP

Product Components

FinFly ISP Strategic

A strategic deployment of FinFly ISP consists at least of the following:
- Management System at the LEMF
- Target Identification Probe Server(s) at the AAA-System of the network
- Deployment Proxy Server(s) at, for example, the Internet Gateway(s)

FinFly ISP Servers
HP ProLiant DL-Series G7 Business WS

FinFly ISP Workstation
HP Z-Series

Throughput:	> 20 Gbps
Max. no. of NICs:	2 – 8 NICs
Interfaces:	1GE Copper / Fiber 10GE Copper / Fiber SONET/SDH OC-3 / -192 STM-1 / -64 ATM AAL5
Processors:	1x – 8x Intel XEON
Core:	2 – 8 Cores / Processor
RAM:	12GB – 1TB
HDD Capacity:	3 x 146GB – 4.8TB SAS
Features:	HP iLO 3 Redundant Power Redundant Fans Bypass Switch Function (if applicable)
Operating System:	Linux GNU (Debian 5.0) hardened

FinFly ISP Tactical

A tactical FinFly ISP System consists of the following:
- Target Identification & Deployment Proxy Server Portable
- Management System Notebook

FinFly ISP Portable
Atlas A9 17" Portable

FinFly ISP Mgmt.
Lenovo Thinkpad T-Series

Throughput:	6 Gbps
Max. no. of NICs:	3 NICs (Interfaces)
Interfaces:	1x 1000BASE-T (Copper; 2 ports) 1x 1000BASE-SX (MM-Fiber; 2 ports) 1x 1000BASE-LX (SM-Fiber; 2 ports) Others upon request
Processors:	1x Intel Core i7 Intel Xeon upon request
Cores:	4 Cores / Processor
RAM:	12GB minimum
HDD Capacity:	2 x 1TB SATA
Optical Drive:	DVD+/-RW SATA
Monitor:	1 x 17" TFT, Keyboard, Touchpad
Features:	Bypass Switch Function for NICs
Operating Systems:	Linux GNU (Debian 5.0) hardened Windows 7 Prof. (Management Nb.)

FINFLY NET

In many real-life operations, physical access to in-country target systems cannot be achieved.

To solve this, a **covert remote installation** of a Remote Monitoring Solution is required to be able to **monitor the Target from within Headquarters**.

FinFly NET is a **tactical** (portable) solution to be deployed in a **„friendly" LAN environment** (like hotels, hotspots, companies - with support of the network owner) on short notice, to remotely install the Remote Monitoring Solution on selected target systems.
FinFly NET is based on a **high performance portable PC** combined with a **Management Notebook** to provide maximum mobility and flexibility in the targeted networks. A wide range of Network Interface Cards – all **secured with bypass functions** – is available for the required active network connectivity.

The end-user can select several **sophisticated passive methods of Target and Traffic Identification**. These vary from DHCP/RADIUS Monitoring (MAC-Addresses, User Names), Flow Monitoring and Finger-Printing. Each method can be used either stand-alone or combined, to provide maximum success identifying the targets of interest. Of course fixed IP-Addresses can be used too.
It is able to **patch Files that are downloaded** by the Target on-the-fly, **send fake Software Updates** for popular Software or **inject the Payload into visited Websites**.

QUICK INFORMATION	
Usage:	· Tactical Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target System in a "friendly" LAN Environment
Content:	· Hardware/Software

Usage Example LAN: Intelligence Agency

FinFly NET is deployed i.e. in a hotel's LAN in front of the DSL-Modem before the IP-traffic is transmitted to an Internet Service Provider network.

Targets of interest are **identified in the IP-traffic by various passive profiling** and identification methods and the Remote Monitoring Solution will be deployed on the positively identified Target Systems.

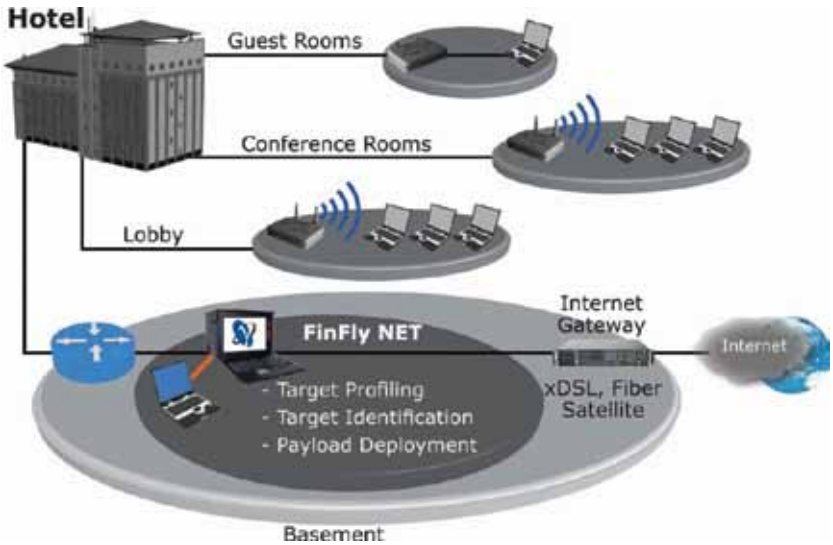
Feature Overview

- Can be installed inside a **LAN environment** (hotel, hotspot, company …)
- Ethernet 1000Base-T, 1000Base-SX, 1000Base-LX
- Identifies Targets using different passive **profiling/identification methods**
- Hides a Remote Monitoring Solution in **Downloads of Targets**
- Injects a Remote Monitoring Solution as **Software Updates**
- Installs a Remote Monitoring Solution through **Websites visited by the Target**

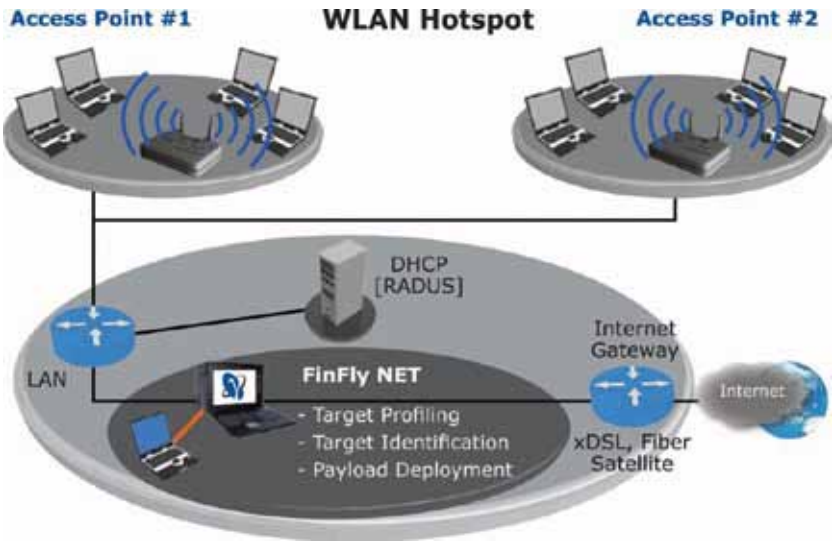
For a full feature list, please refer to the Product Specifications.

DIFFERENT DEPLOYMENT POSSIBILITIES

Deployment in the LAN of a Hotel



Deployment in the LAN of a WLAN Hotspot



FinFly NET will be deployed at the appropriate location inside the facility. After connecting the Portable in-line to the link(s) provided, the user can start analyzing the traffic selecting various different methods to identify the targets of interest and their IP-traffic. The methods to be used for target identification strongly depend on the network setup, features and services provided and used.

TARGET PROFILING AND IDENTIFICATION

HTTP Sniffer Module
Browser and Operating System Types and Versions, History, Languages

Email Sniffer Module
POP3, SMTP

Login Sniffer Module
FTP, HTTP, IMAP, IRC, NNTP, POP, SMTP

TCP/UDP Sniffer Module
Source/Destination IP, Source/Destination Ports

DHCP/RADIUS Sniffer Module
MAC, Hostname, IP Session start/end

TARGET DEPLOYMENT METHODS

Binary/Download
Patching of ".exe" and/or ".scr" files

Update Injection
Fake Updates for different Applications

Website Deployment
Using FinFly Web to deploy during browsing activities

FINFLY NET

Product Components

FinFly NET consists of the following:

- Target Profiling, Identification & Deployment Proxy Server (Portable)
- Management System (Notebook)

FinFly NET Portable
Atlas A9 17" Portable

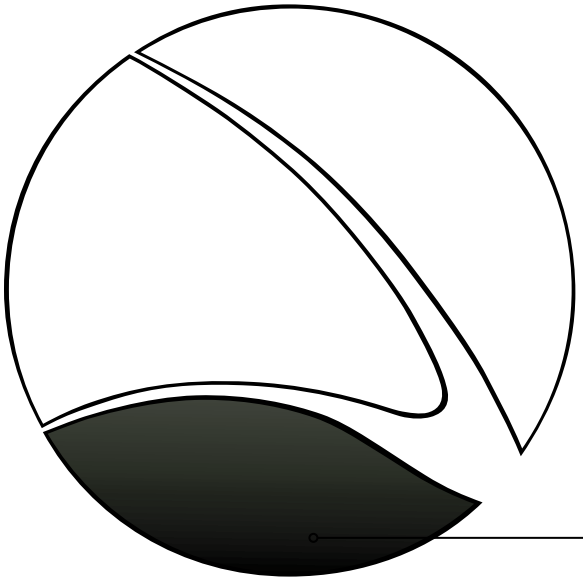
FinFly NET Mgmt.
Lenovo Thinkpad T-Series

Throughput:	6 Gbps
Max. no. of NICs:	3 NICs (Interfaces)
Interfaces:	1x 1000BASE-T (Copper; 2 ports) 1x 1000BASE-SX (MM-Fiber; 2 ports) 1x 1000BASE-LX (SM-Fiber; 2 ports) Others upon request
Processors:	1x Intel Core i7 Intel Xeon upon request
Cores:	4 Cores / Processor
RAM:	12GB minimum
HDD Capacity:	2 x 1TB SATA
Optical Drive:	DVD+/-RW SATA
Monitor:	1 x 17" TFT, Keyboard, Touchpad
Features:	Bypass Switch Function for NICs
Operating Systems:	Linux GNU (Debian 5.0) hardened Windows 7 Prof. (Management Nb.)

Important Note:
Gamma provides next to FinFly NET the same intelligence capabilities integrated within the FinFly ISP solution, whereas the target identification capabilities are implemented into a fixed or portable ISP solution. This solution is characterized by high performance server technology which will be customized and integrated into the relevant ISP environment and related requirements.

IT Intrusion Training Program

FINTRAINING



The IT Intrusion Training Program includes courses on both, products supplied as well as practical IT Intrusion methods and techniques. This program transfers years of knowledge and experience to end-users, thus maximizing their capabilities in this field.

FINTRAINING

Security awareness is **essential for any government** to maintain IT security and successfully **prevent threats** against IT infrastructure, which may result in a loss of confidentiality, data integrity and availability.

On the other hand, topics like **CyberWar**, Active Interception and Intelligence-Gathering through **IT Intrusion** have become more important on a daily basis and require Governments to **build IT Intrusion teams** to **face these new challenges**.

FinTraining courses are given by **world-class IT Intrusion experts** and are held in **fully practical scenarios** that focus on **real-life operations** as required by the end-user in order to solve their **daily challenges**.

Gamma combines the individual training courses into a **professional training and consulting program** that builds up or enhances the capabilities of an IT Intrusion team. The Training courses are **fully customized** according to the end-user's operational challenges and requirements.

QUICK INFORMATION	
Usage:	· **Knowledge Transfer**
Capabilities:	· **IT Intrusion Know-How** · **CyberWar Capabilities**
Content:	· **Training**

Sample Course Subjects

- **Profiling** of Target Websites and Persons
- Tracing **anonymous Emails**
- **Remote access** to Webmail Accounts
- **Security Assessment** of Web-Servers & Web-Services
- Practical **Software Exploitation**
- **Wireless IT Intrusion** (WLAN/802.11 and Bluetooth)
- Attacks on **critical Infrastructures**
- Sniffing **Data and User Credentials** of Networks
- **Monitoring Hot-Spots**, Internet Cafés and Hotel Networks
- **Intercepting and Recording Calls** (VoIP and DECT)
- **Cracking Password** Hashes

Consultancy Program

- Full IT Intrusion **Training and Consulting** Program
- Structured build-up and **Training of IT Intrusion Team**
- Full **Assessment of Team** Members

Customized courses in high-end training facilities worldwide

FINSUPPORT

FinSupport

The FinSupport sustains upgrades and updates of the FinFisher™ product-line in combination with an annual support contract.

The FinFisher™ Support Webpage and Support Team provide the following services to clients:

- Online access to:
  - Latest User Manual
  - Latest Product Specifications
  - Latest Product Training Slides
  - Bug Reporting Frontend
  - Latest Anti Virus Test Report
  - Feature Request Frontend
- Regular Software Updates:
  - Bug fixes
  - New Features
  - New Major Versions
- Technical Support via Messenger:
  - Bug fixing
  - Partial Operational Support

FinLifelineSupport

The FinLifelineSupport provides professional back-office support for trouble resolution and technical queries. It also provides back-office support remotely, for FinFisher™ Software bug fixes and Hardware replacements under warranty. Furthermore, with FinLifelineSupport the client automatically receives new features and functionalities with the standard release of bug fixes.

QUICK INFORMATION	
Usage:	**· Overall Solution & Operational Support**
Capabilities:	**· Bug Fixing, Update of Features and Capabilities**
Content:	**· Hardware/Software**

Software Upgrades

The FinLifelineSupport includes regular Software upgrades and guarantees automatic upgrades to the existing system with Software patches provided via the update system.

These upgrades include new features, new enhancements and new functionality, as per the client's roadmap (excluding hardware).

WWW.FINFISHER.COM

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

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