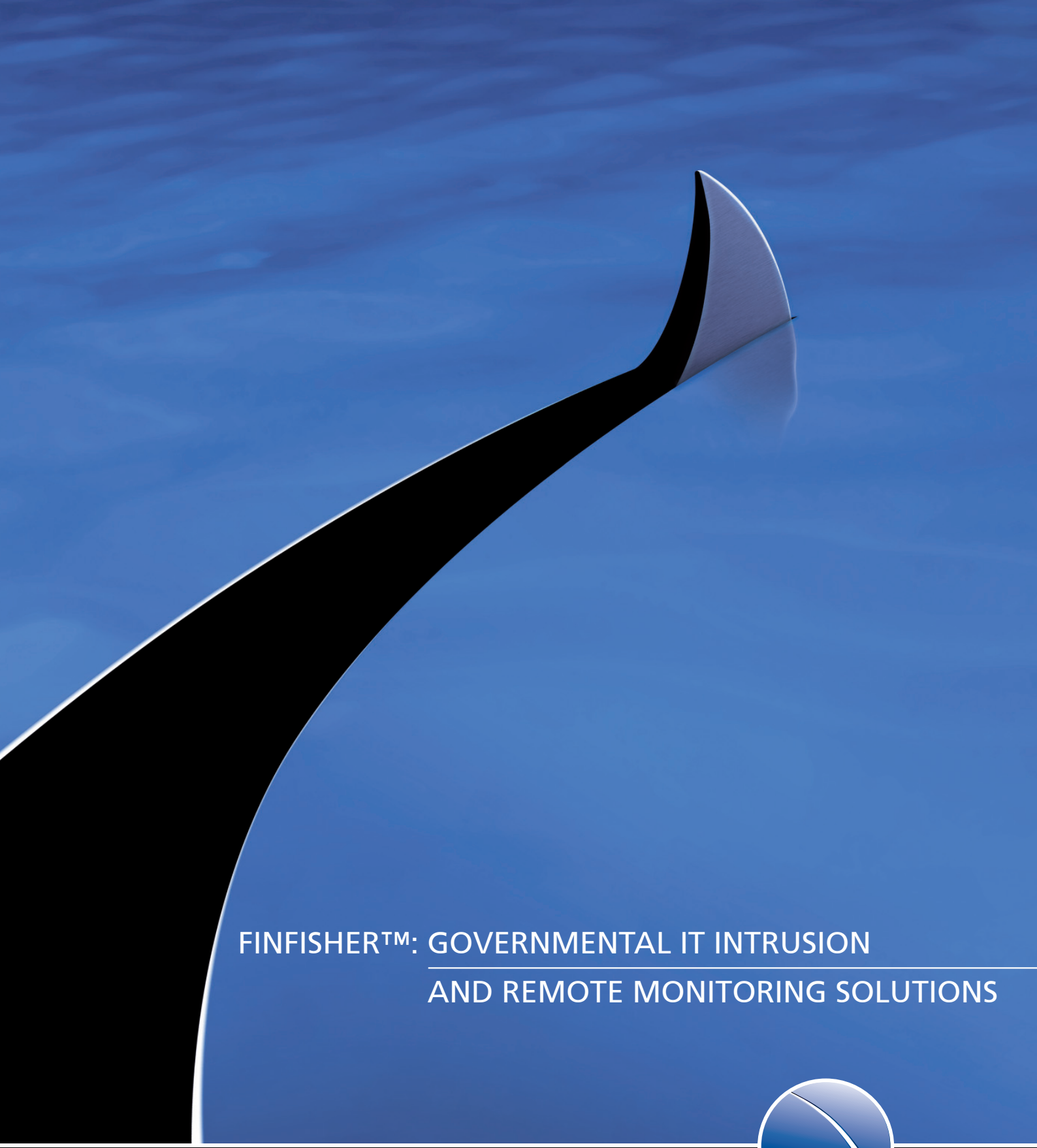
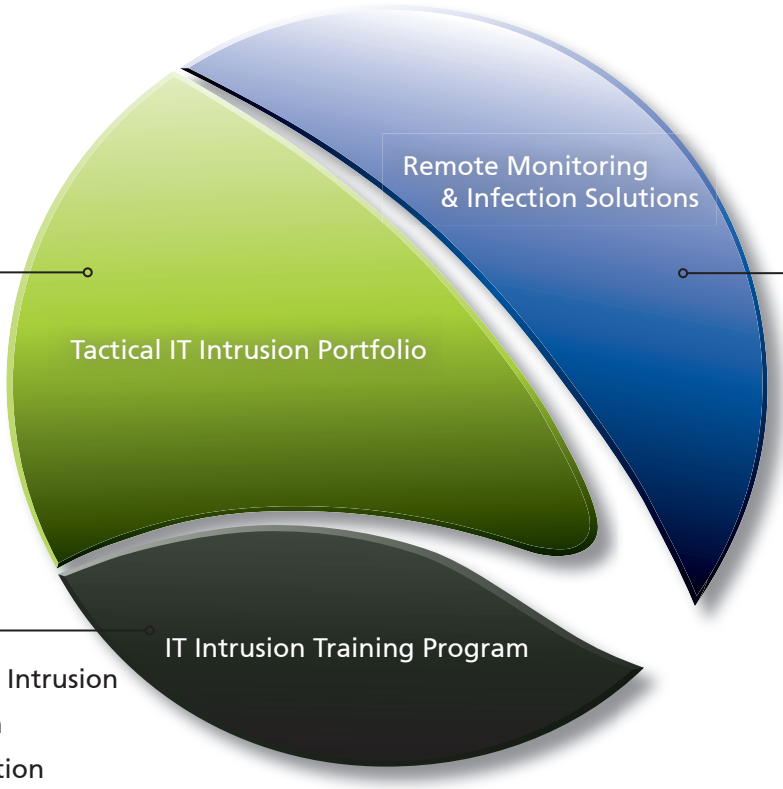


FINFISHER™: GOVERNMENTAL IT INTRUSION AND REMOTE MONITORING SOLUTIONS

WWW.GAMMAGROUP.COM

FINFISHER™
IT INTRUSION



· FinIntrusion Kit
· FinUSB Suite
· FinFireWire

FinSpy · FinSpy
· FinSpy Mobile
FinFly · FinFly USB
· FinFly LAN
· FinFly Web
· FinFly ISP

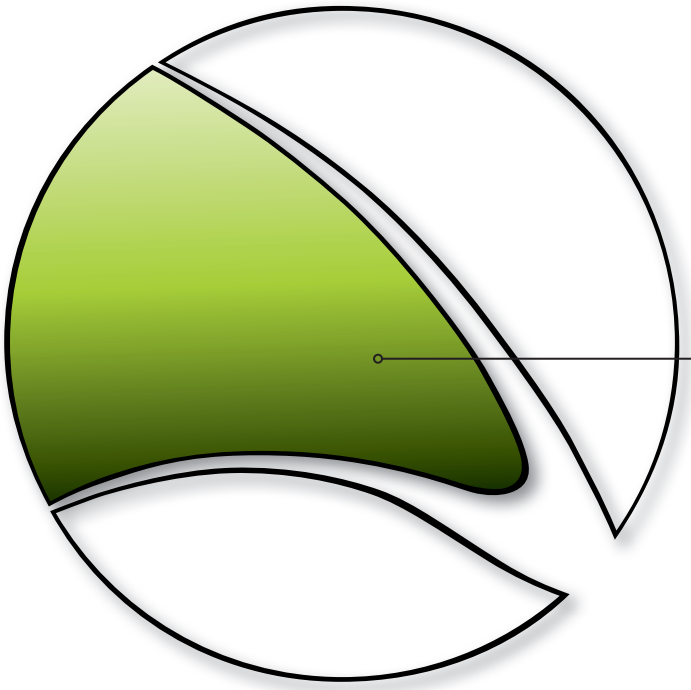
· Basic & Advanced Intrusion
· Wireless Intrusion
· Practical Exploitation
· Web Application Penetration
· Custom IT Intrusion Training & Consulting

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.GAMMAGROUP.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 Operations · Tactical Operations
Capabilities:	· Break 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 break **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 **compromise 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 (e.g. Blogs, Discussion Boards) 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**
- Emulates **Rogue Wireless Access-Point** (802.11)
- Remotely **breaks into Email Accounts** using Network-, System- and Password-based Intrusion Techniques
- **Network Security Assessment** and Validation

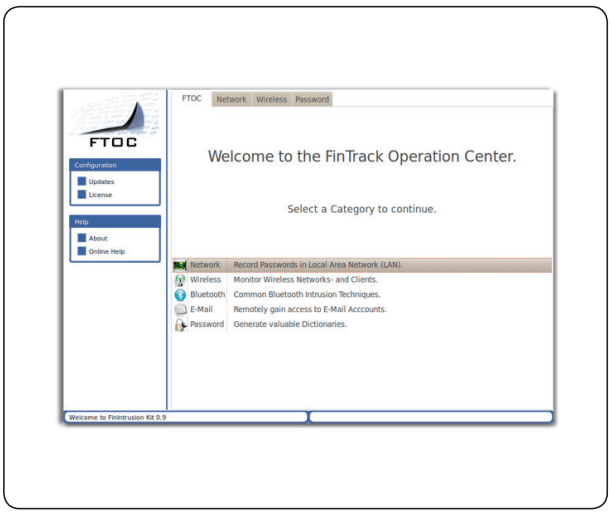
For a full feature list please refer to the Product Specifications.

FININTRUSION KIT

Product Components

FinIntrusion Kit - Covert Tactical Unit

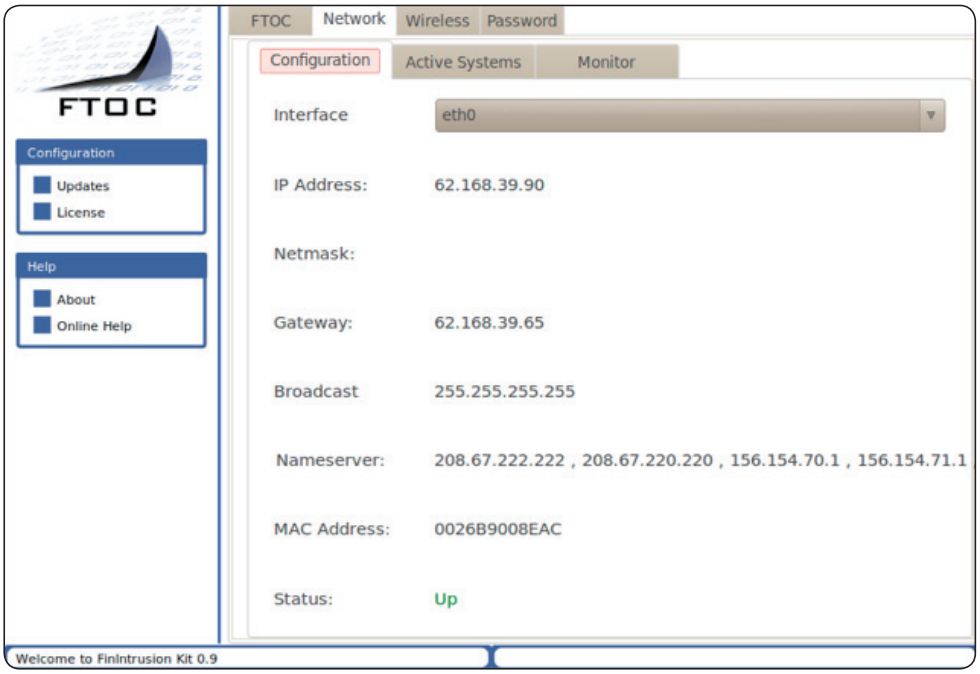
Basic IT Intrusion Components:
- High-Power WLAN Adapter
- High-Power Bluetooth Adapter
- 802.11 Antennas
- Many Common IT Intrusion Devices



FinTrack Operation Center

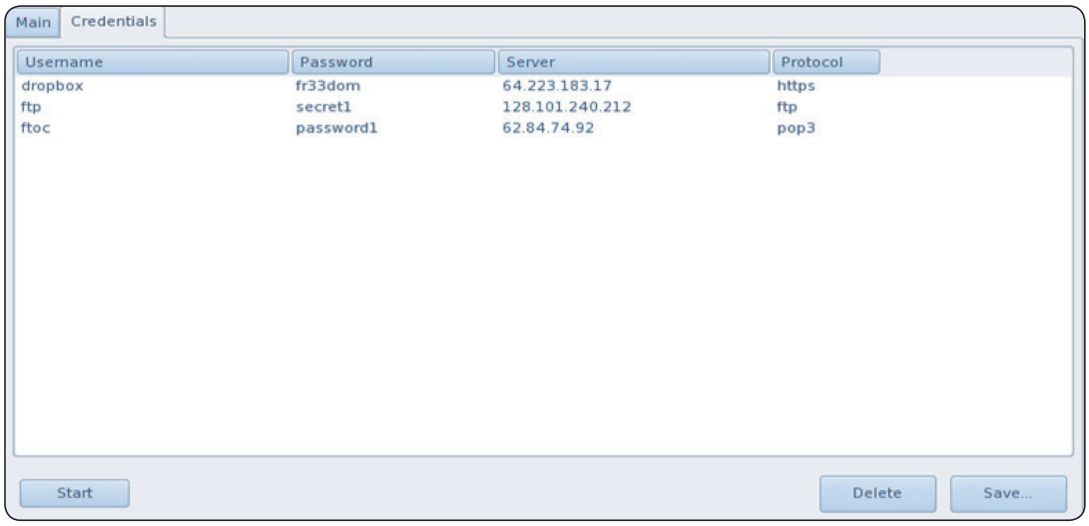
- Graphical User Interface for Automated IT Intrusion Attacks

Automated LAN/WLAN Monitoring



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**
- **Secure Encryption** with RSA and AES
- 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
- Encrypts Data on-the-fly

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

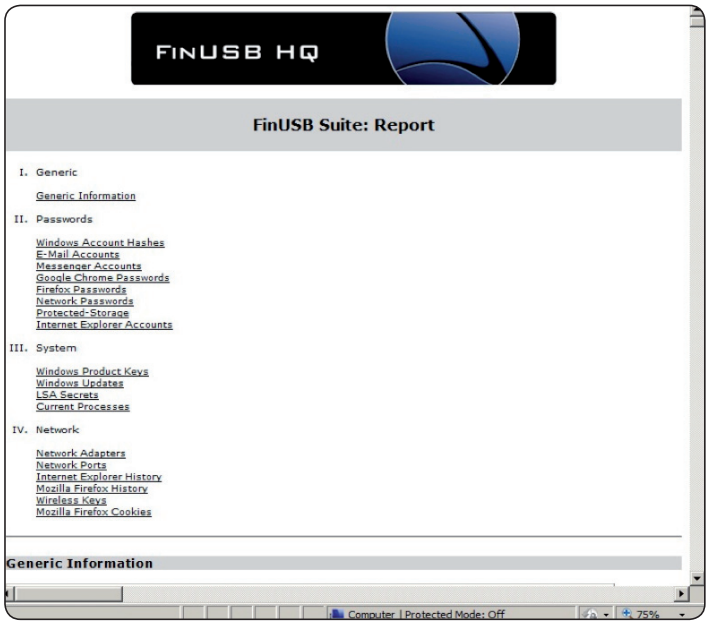
5. Wait until all data is transferred

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:	· Bypass User Password · Covertly Access System · Recover Passwords from RAM · Enable 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**
- Full Access to **all Network Shares** of User
- **Dumps full RAM** for Forensic analysis
- Enables live forensics **without rebooting** the Target System
- User password is **not changed**
- Supports **Windows, Mac and Linux systems**
- Works with **FireWire/1394, PCMCIA and Express Card**

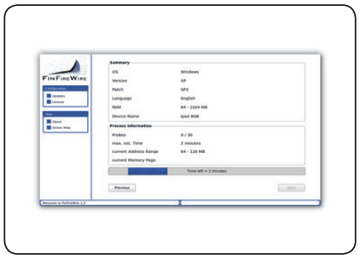
For a full feature list please refer to the Product Specifications.

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

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

FINSPY

FINSPY MOBILE

FINFLY USB

FINFLY LAN

FINFLY WEB

FINFLY ISP

The Remote Monitoring and Infection 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 infection methods, Government Agencies will have the capability to remotely infect 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 Operations** · **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 communication** 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 communication** 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
· Security Data Encryption and Communication using **RSA 2048 and AES 256**
· Hidden from Public through **Anonymizing Proxies**
· Can be **fully integrated** with Law Enforcement Monitoring Functionality (LEMF)

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

Product Components

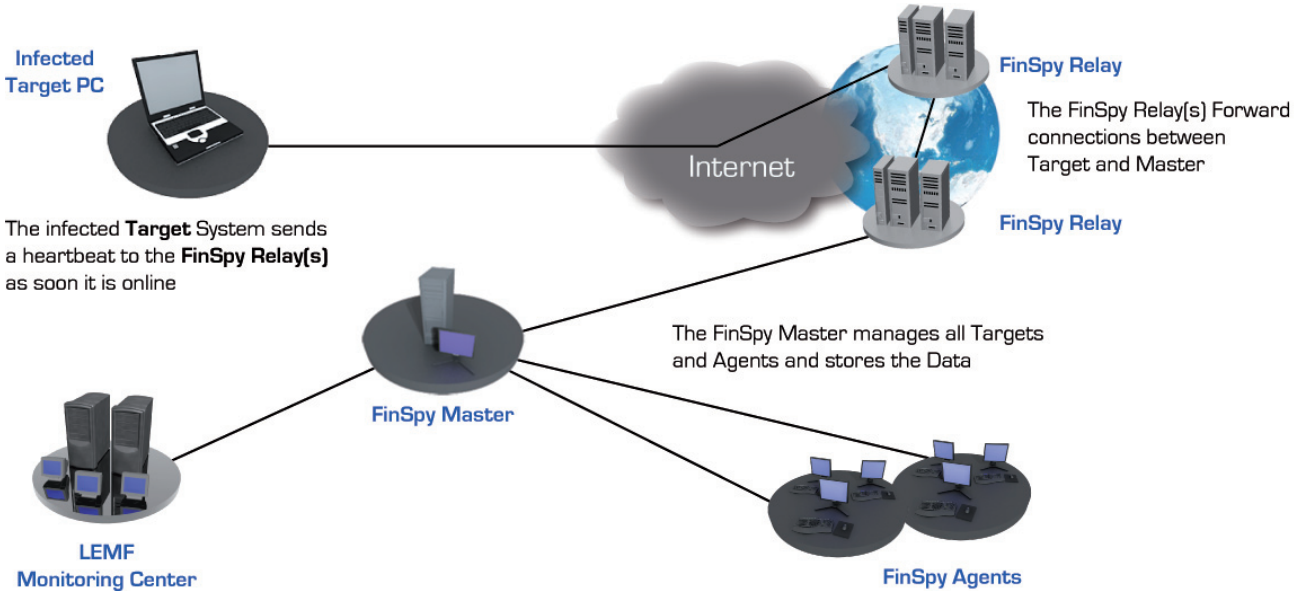
FinSpy Master and Proxy

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

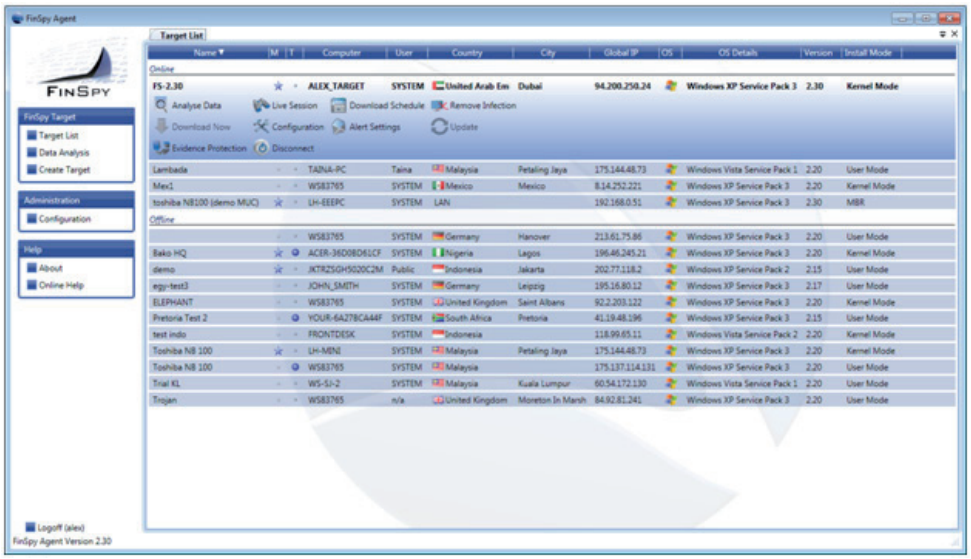
FinSpy Agent

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

Access Target Computer Systems around the World

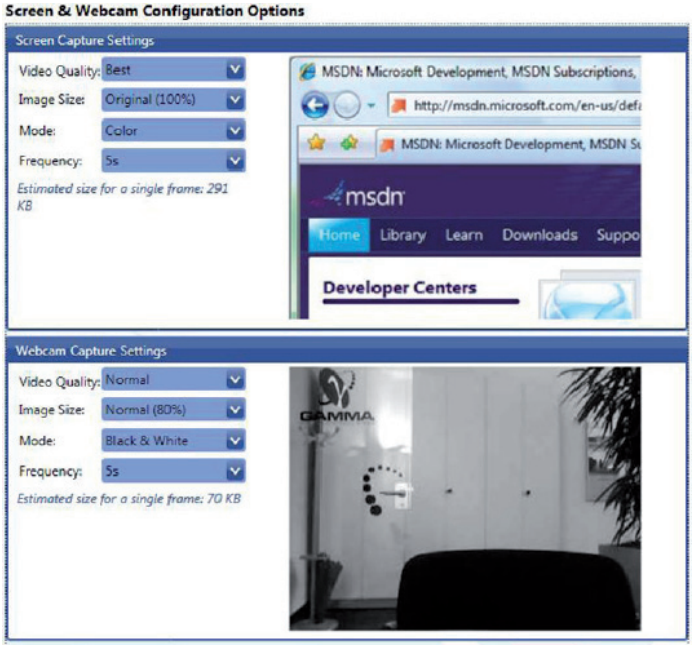


Easy to Use User Interface

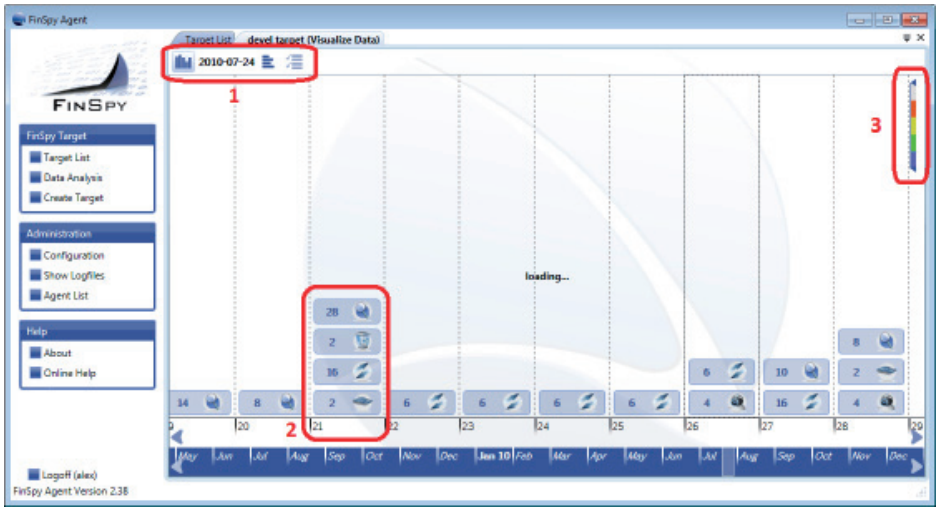


Live and Offline Target Configuration

Screen & Webcam Configuration Options



Full Intelligence on Target System



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

FINSPY LICENSES

Outline

The FinSpy solution contains 3 types of product licenses:

A. Update License

The Update License controls whether **FinSpy** is able to retrieve new updates from the Gamma Update server. It is combined with the **FinFisher™ After Sales Support** module.After expiry, the **FinSpy** system will still be **fully functional** but no longer able to retrieve the newest versions and bug-fixes from the FinSpy Update server.

B. Agent License

The Agent License controls how many **FinSpy Agents** can login to the **FinSpy Master** in parallel.

Example:

- **5 Agent Licenses** are purchased.
- **FinSpy Agent** licenses can be installed on an unlimited number of systems, however
- Only 5 **FinSpy Agent** systems can login to the **FinSpy Master** and work with the **data at the same time**

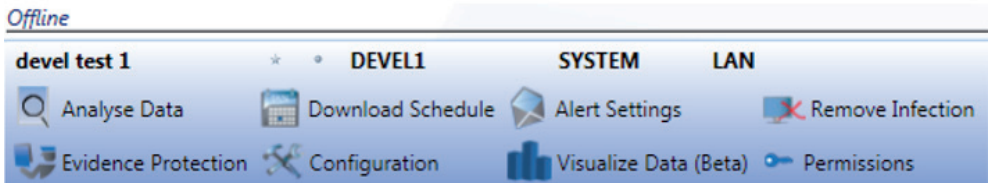
C. Target License

The Target License controls how many **FinSpy Targets** can be **active** in parallel.

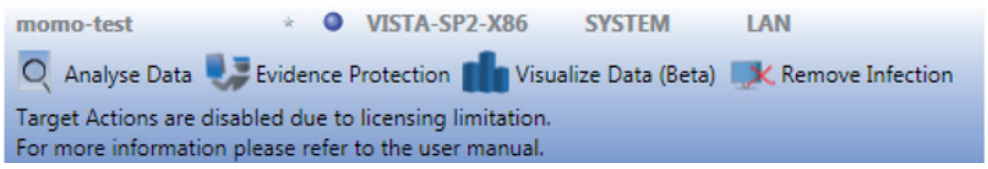
Active refers to **activated FinSpy Target** installations no matter whether the Target System is online or offline.

When **FinSpy Target** is deployed on a Target System and no Target Licenses are available, the **FinSpy Target** gets temporary deactivated and no recording and live access will be possible. As soon as a new License is available (e.g. by upgrading the existing License or de-infecting one of the active **FinSpy Targets**), the Target will be assigned the free license and it will be activated and begin recording and providing live access.

Screenshot active Target with License



Screenshot inactive Target without License



FINSPY MOBILE

FinSpy Mobile is closing the gap of interception capabilities for Governments for most common **smart phone 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 Operations · 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, iOS (iPhone), BlackBerry and Android**

Headquarters – Example Features:

- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Security Data Encryption and Communications using **RSA 2048 and AES 256**
- 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

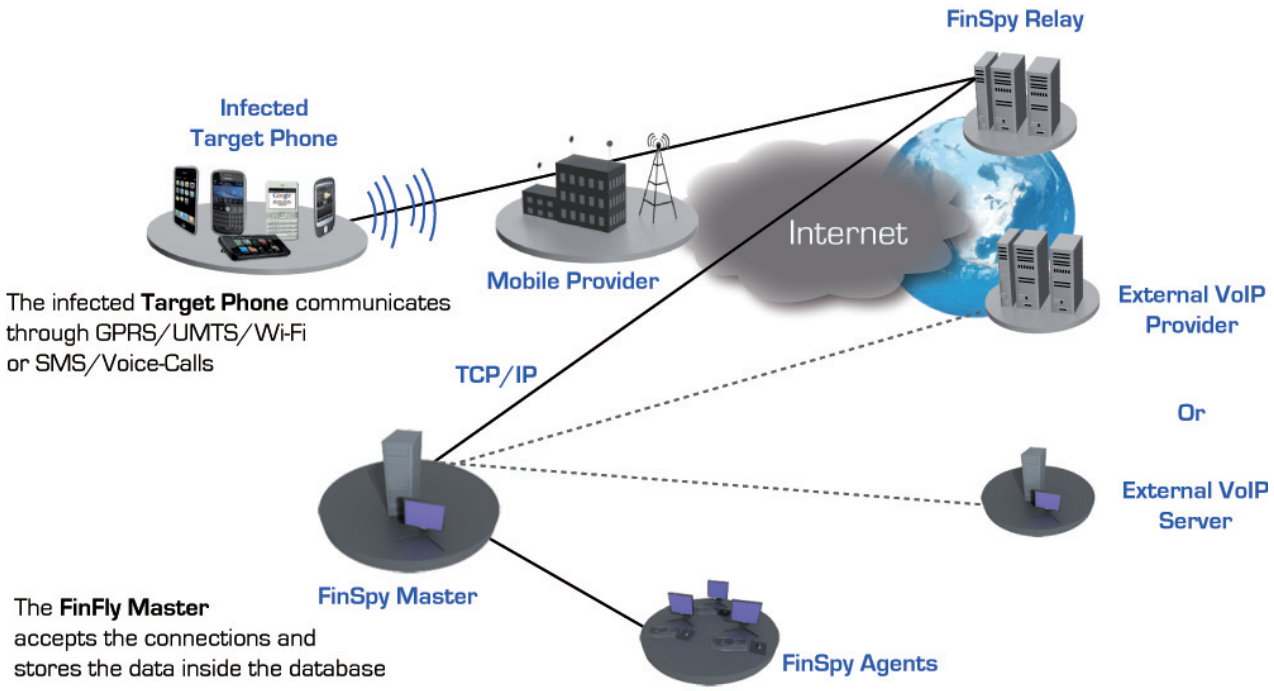
FinSpy Master and Proxy

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

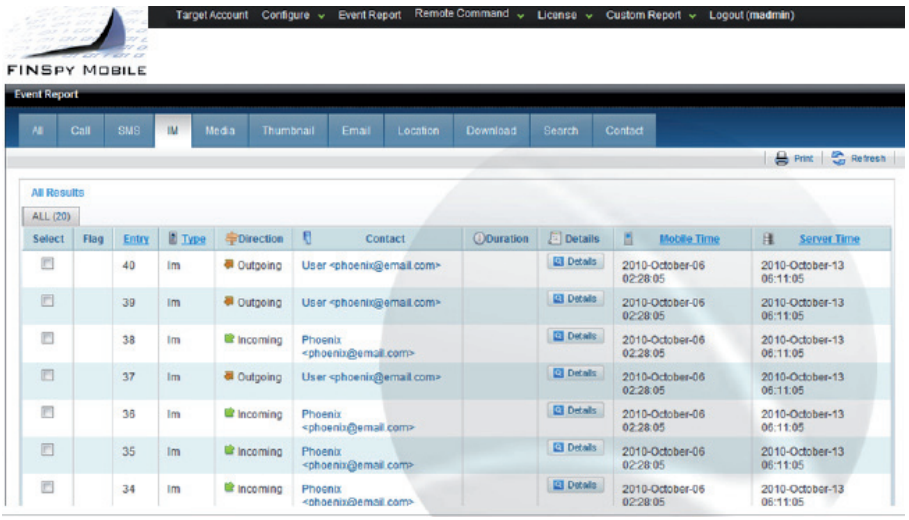
FinSpy Agent

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

Access Target Mobile Phones around the World



Easy to Use User Interface



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**.

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.

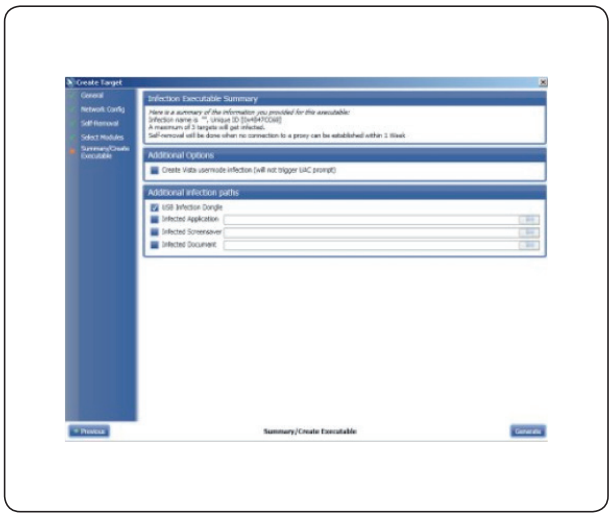
Feature Overview

- **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
- Infection of **switched off Target System** when **booting from USB**
- 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

- SanDisk USB Dongle (16GB)
- 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

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

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 as well as Targets who **do not open any infected Files** that have been sent via email to their accounts.

In particular, security-aware Targets are **almost impossible to infect** 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 **infect Files that are downloaded** by the Target on-the-fly, infect the Target by **sending fake Software Updates** for popular Software or infect the Target by **injecting 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 computer when 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.

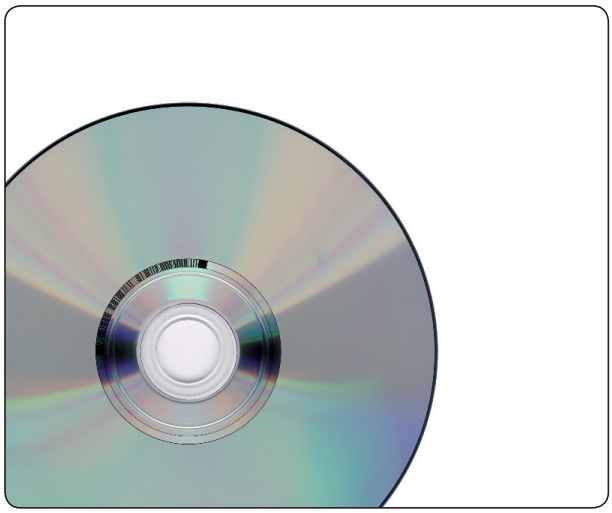
Feature Overview

· **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



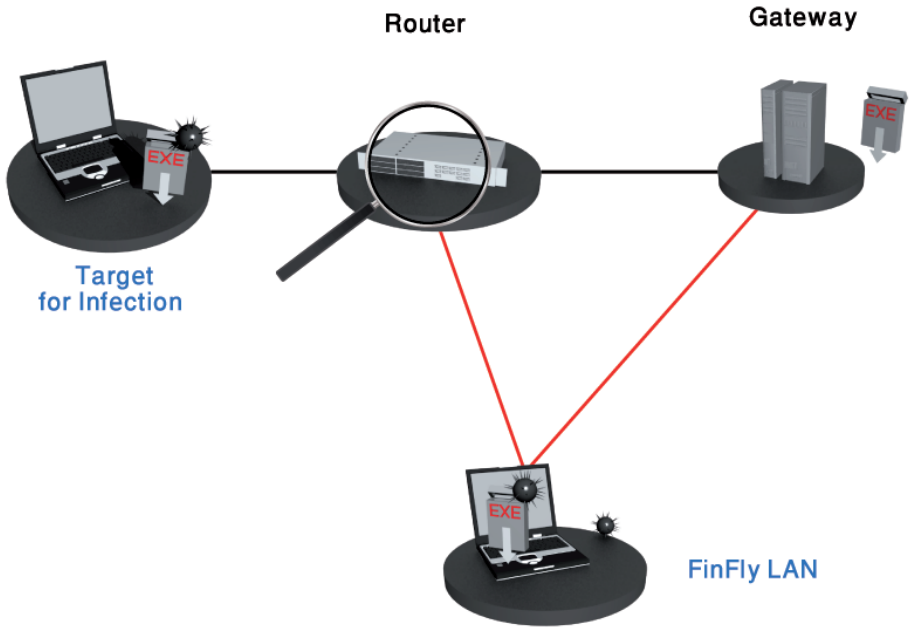
FinFly LAN

· Linux-based Software with simple User-Interface

FinIntrusion Kit - Integration (Optional)

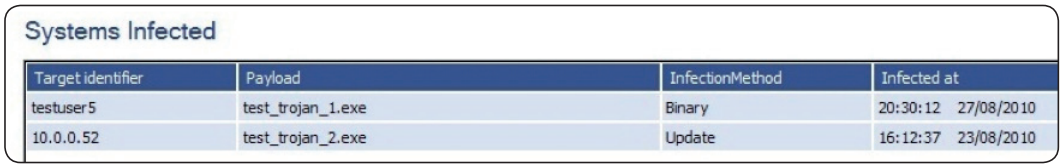
· FinFly LAN will be loaded as a module into the FinIntrusion Kit

Infection through Local Area Networks



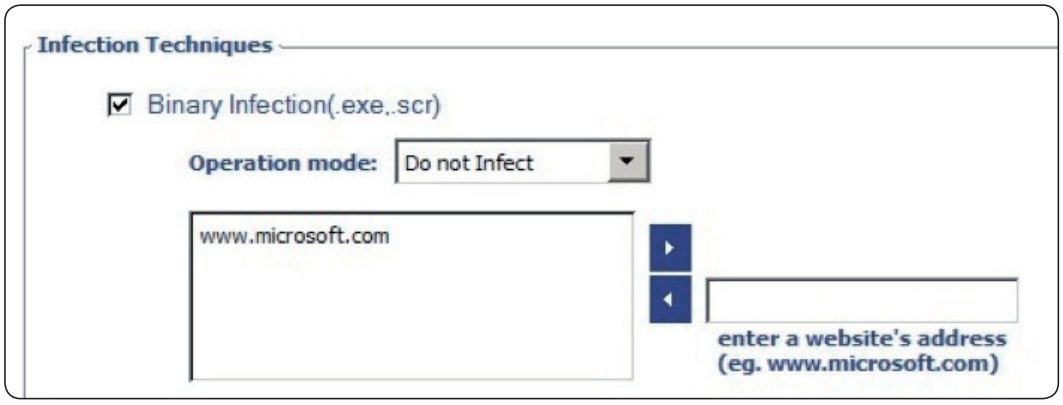
Automated User-Interface

· 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** infection of 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 infection code** according to selected modules.

Target Systems visiting a prepared website with the implemented infection code will be **covertly infected** with the configured software.

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

The customer deployed **FinFly ISP within the main Internet Service Provider** of their country. It was **combined with FinFly Web** to remotely **infect Targets that visited government offensive websites** by covertly injecting the FinFly Web code into the targeted websites.

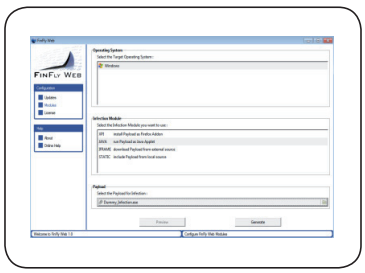
Feature Overview

- **Fully-Customizable** Web Modules
- Can be covertly **installed into every Website**
- Full integration with **FinFly LAN** 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

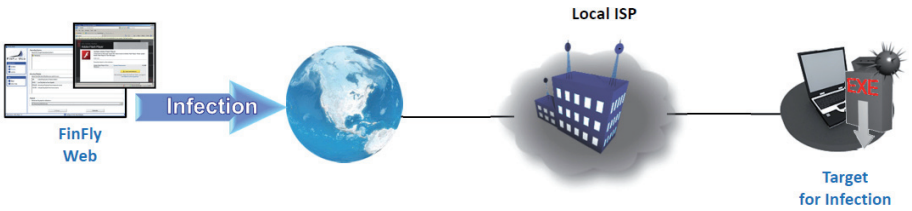
Product Components



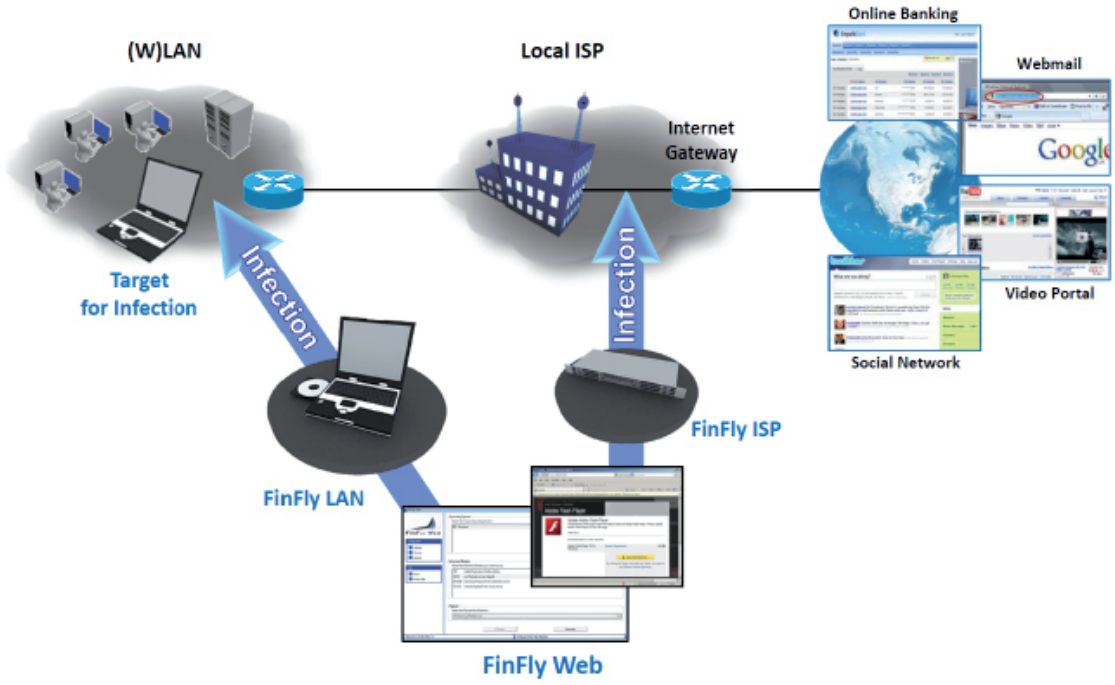
FinFly Web

· Point-and-click software to create custom infection Websites

FinFly Web direct infection

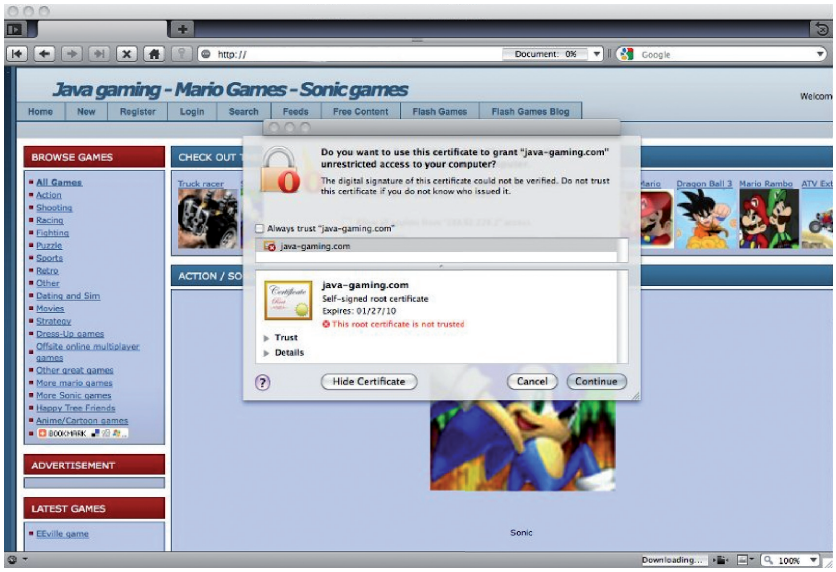


Full integration with FinFly LAN and FinFly ISP



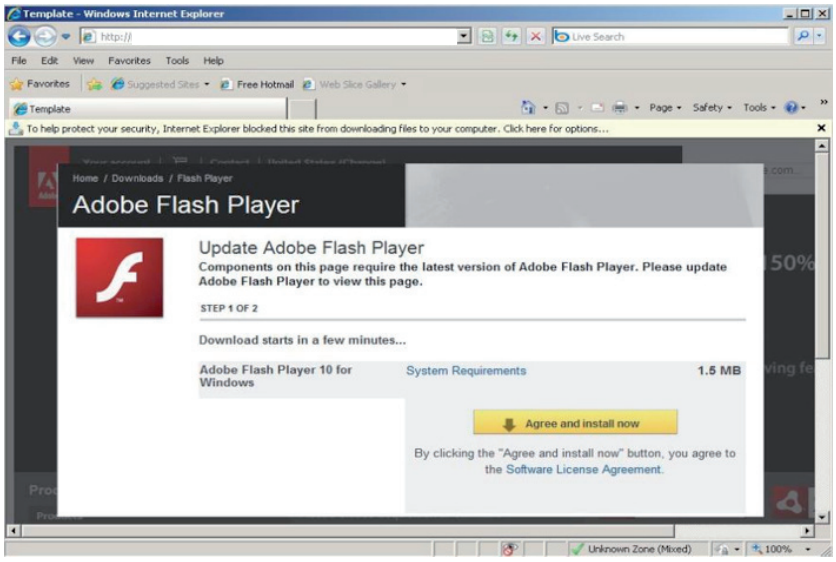
Example: Java Applet (Internet Explorer, Firefox, Opera, Safari)

The website will prompt the Target to accept a Java plug-in that can be signed with any company name (e.g. "Microsoft Corporation")



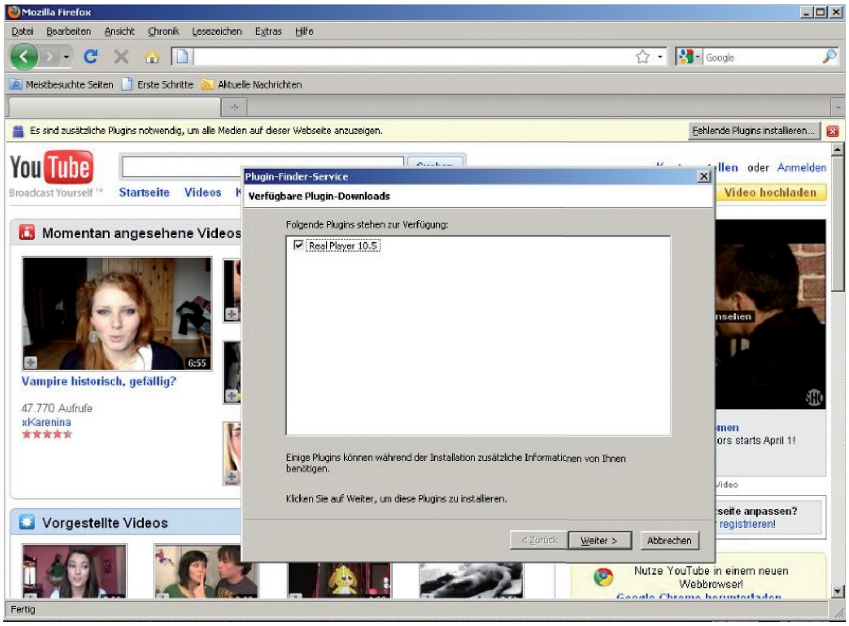
Example: Missing Component (IE, Firefox, Opera, Safari)

The website will pretend that a plug-in/codec etc. is missing on the Target System and prompt it to download and install this software



Example: Missing XPI (Firefox only, all platforms)

This module will prompt the Target to install additional plug-ins in order to be able to view the website.



GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

FINFLY ISP

In many real-life operations, physical access to in-country Target Systems cannot be achieved and covert **remote installation** of a Remote Monitoring Solution is required to be able to **monitor the Target from within the 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 the maximum **reliability and scalability** to meet almost every challenge related to network topologies. A wide-range of Network Interfaces – all **secured with bypass functions** – are available for the required active network connectivity.

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

FinFly ISP is able to **infect Files** that are downloaded by the Target **on-the-fly** or infect the Target by **sending fake Software Updates** for popular Software. The new release now integrates Gamma's powerful remote infection application **FinFly Web** to infect Targets on-the-fly by just **visiting any website.**

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.

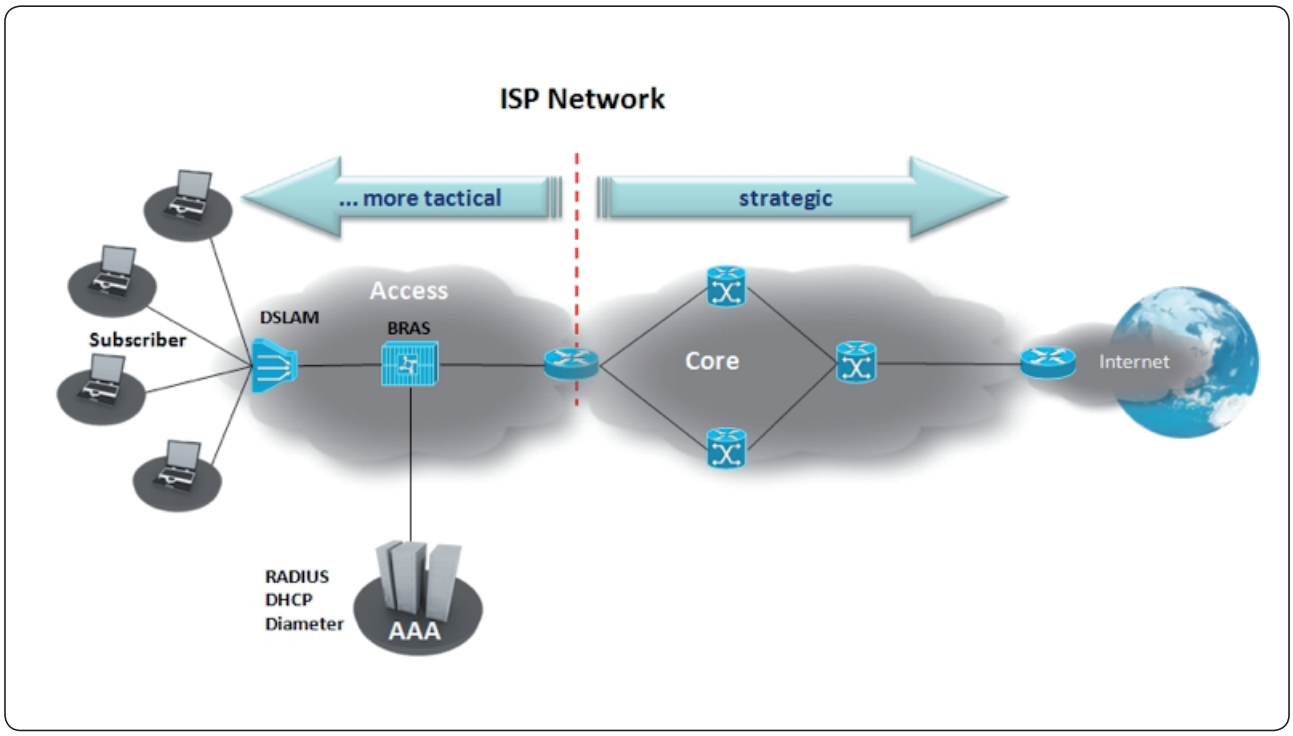
Feature Overview

· Can be installed inside the **Internet Service Provider Network**
· Handles **all common Protocols**
· Selected Targets by **IP address or Radius Logon Name**
· Hides Remote Monitoring Solution in **Downloads by 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.

Different Location Possibilities

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



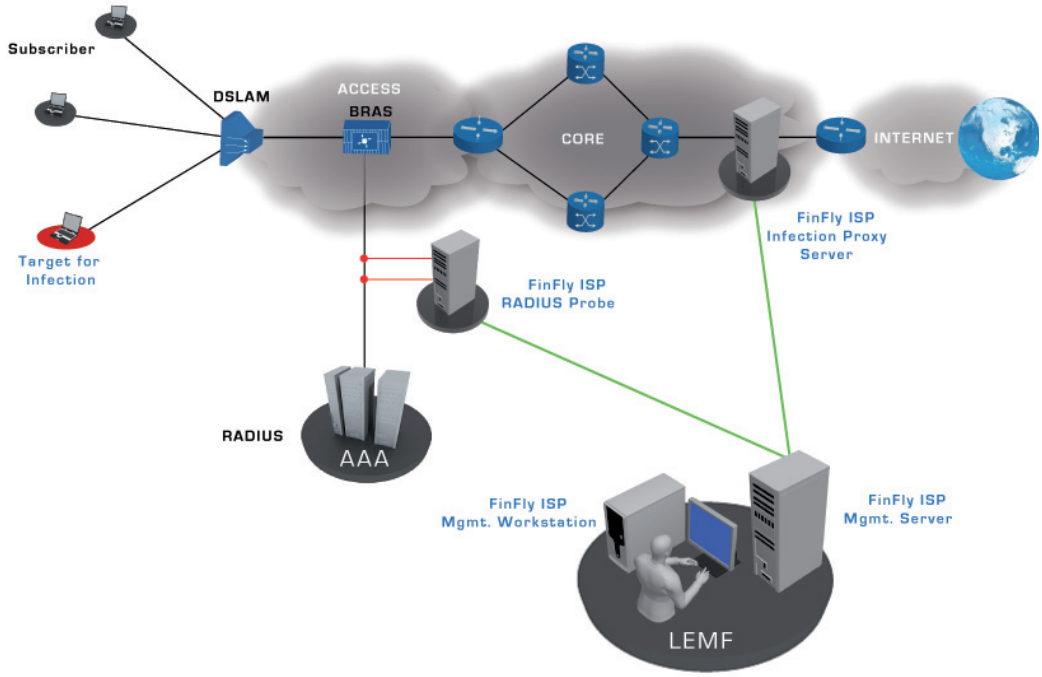
A tactical solution is mobile and the hardware is dedicated to the infection tasks inside the access network close to the targets' access points. It can be deployed on a short-term basis to meet tactical requirements focused on either a specific target or a small number of targets in an area.

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

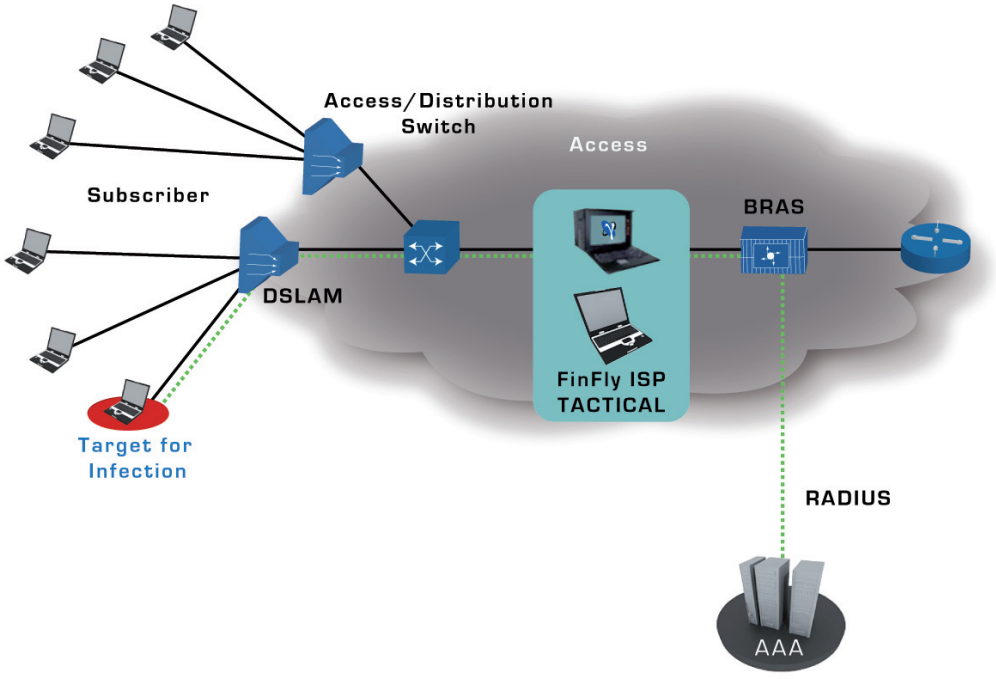
Of course, it is possible to combine tactical and strategic solutions to reach a maximum of flexibility for the infection operations.

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
· Infection Proxy Server(s) at, for example, the Internet Gateway(s)

FinFly ISP Servers
Workstation
HP ProLiant DL-Series G7
Business WS

FinFly ISP
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 & Infection Proxy Server Portable
· Management System Notebook

FinFly ISP Tactical
Portable Mgmt.
Atlas A9 17" Portable

FinFly ISP Tactical
Lenovo Thinkpad
T-Series

Throughput:	5 Gbps
Max. no. of NICs:	3 NICs
Interfaces:	1GE Copper / Fiber SONET / SDH OC-3 / -12 STM-1 / -4 ATM AAL5
Processors:	2 x Intel Core i7
Core:	6 Cores / Processor
RAM:	12GB
HDD Capacity:	2 x 1TB SATA
Optical Drive:	DVD+/-RW SATA
Monitor:	1 x 17" TFT
Features:	Bypass Switch Function for NICs
Operating System:	Linux GNU (Debian 5.0) hardened

The technical data /specifications are subject to change without notice.

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

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 our clients:

- Online access to:
  - Latest User Manual
  - Latest Product Specifications
  - Latest Product Training Slides
  - Bug Reporting Frontend
  - Feature Request Frontend

- Regular Software Updates:
  - Bugfixes
  - New Features
  - New Major Versions

- Technical Support via Skype:
  - Bugfixing
  - 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™ SW 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.

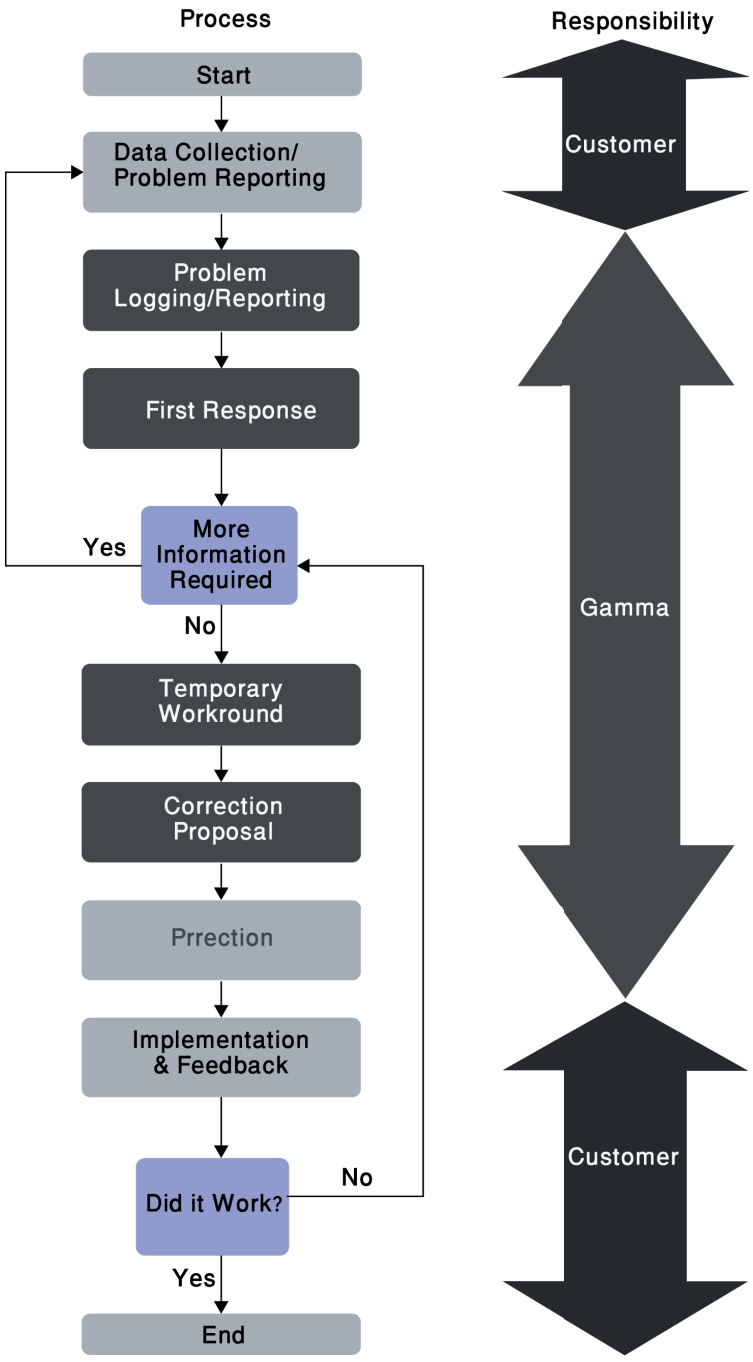
Bug Fixes

FinSupport is a product driven support organization whereby a highly skilled after-sales support manager receives related queries by email or telephone. The after sales support manager is based in Germany and his hours of operation are 09:00 – 17:00 Central European Time (CET).
With the FinLifelineSupport, support is available from 09:00–17:00 CET. If a request for support is logged outside of standard office hours it will be addressed immediately on the next working day.

When the customer reports an incident, we log an Incident Report (IR) and document the priority of the incident. Within a specified period, corrective actions will follow based on the assigned priority. The FinFisher™ team then has the responsibility of coordinating the investigation and resolution of the IR, as well as communicating the status and new information to the IR originator.

For high priority issues, we ensure that the system continues to work smoothly by quickly delivering workaround solutions and tested bug fixes. When the FinFisher™ team delivers a workaround, in parallel it also escalates the Problem Report (PR) to the Research and Development (R&D) department to ensure a quick resolution. These professional support measures ensure that the software meets the highest expectations.

The following flow chart provides an illustration of the typical operational procedure and areas of responsibility (**Note**: in this flow chart, 'customer' represents the originator of the IR):



The following table provides the normal customer incident handling procedure:

Customer	**Incident Report (IR) Processing and Tasks**
	FinFisher™ has dedicated email, phone/fax hotline contact info for incident reporting.
In cases of a (suspected) hardware/software defect, receive Incident Report (IR) as per the defined communication methods. IR should include: - contract id - customer's name - affected system/ technology - description of defect - priority (see definition below) - available error symptoms	
Customer cooperates by providing further error symptoms, upon request	Within one working day, customer receives the ticket number to confirm receipt and tracks the IR, and also the initial analysis results
	FinLifelineSupport supports collecting error symptoms, upon request
	FinLifelineSupport helps with temporary workaround solution
	FinLifelineSupport provides correction proposal on IR with planned corrective measures & response time, after incident analysis
	FinLifelineSupport provides issue of hard- or software modification, if reported incident requires correction
Customer implements delivered hardware/ software modification. Customer confirms successful correction.	FinLifelineSupport helps with implementing hardware(i)/ software modification

(i) Hardware charged separately if not under warranty.

Definitions of query and fault priority

FinLifelineSupport processes the incoming queries and problem reports according to their urgency. Two factors rate the urgency of an incident, and both are included in each IR:

· 'Priority' based solely on the technical scope of the error
· 'Customer Severity' is a more objective factor and based on the resultant customer impact

The following 'Priority' table provides an overview of the corresponding technical scope:

Priority	Definition	Example
1	critical issue: crucial aspect of system not working	The Proxy is down and no communication to the FinSpy Target can be established.
2	major issue with no workaround	An Antivirus update detects an already installed RMS which requires an immediate update in order to stay operational within the infected system.
3	major issue with workaround	FinSpy Target functionality doesn't operate properly but can be fixed with a workaround solution.
4	minor issue with little impact on system	Wrong icon shown for a downloaded file

Response Times

In 90 percent of all incidents, we will keep our response times as depicted in the table below.

'Working day(s)' = as defined in the German calendar, and thus, excludes holidays observed in Germany.

There are three phases in our response times:
· Initial Response
· Corrective Action Feedback
· Problem Resolution (or Priority De-Escalation)

The time for the 'Initial Response' is from the moment we log an incident to the actual confirmation response sent to the customer acknowledging receipt of the incident.

The 'Initial Response' may also ask for more detailed information or, in less complex cases, may immediately solve the problem.

Response Times	Initial Response	Corrective Action Feedback	PROBLEM Resolution/ PRIORITY De-Escalation
Prio 1 - critical issue	Same working day	1 working day(s)	2 working day(s) Please note: Depending on the problem and research required it may take longer to resolve the issue.
Prio 2 - major issue without workaround	Same working day	2 working day(s)	5 working day(s) Please note: Depending on the problem and research required it may take longer to resolve the issue.
Prio 3 - major issue with workaround	Same working day	3 working day(s)	14 working day(s) Please note: Depending on the problem and research required it may take longer to resolve the issue.
Prio 4 - minor issue	Same working day	7 working day(s)	next software update

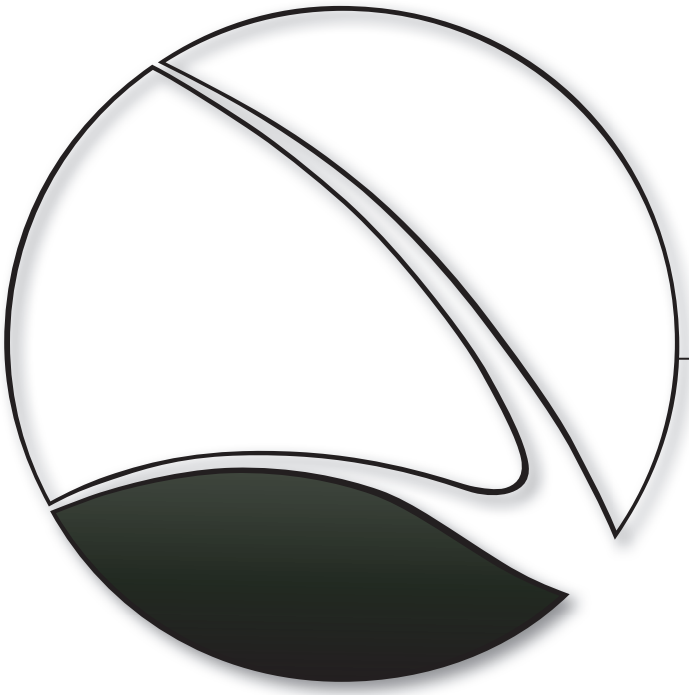
Software Upgrades

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).

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.

FINFISHER™
IT INTRUSION

WWW.GAMMAGROUP.COM

IT Intrusion Training Program

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. In order to ensure full usability of the transferred know-how, **operational in-country support** is provided during the program.

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
- Practical Training Sessions focus on **Real-Life Operations**
- In-Country **Operational Consulting**

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

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

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

info@gammagroup.com

WWW.GAMMAGROUP.COM