FINFISHER™
EXCELLENCE IN
IT INVESTIGATION

Cyber solutions for the **fight against crime**

FinFisher GmbH
Baierbrunner Str. 15
81379 Munich

Tel: +49 89 785 76 175
Fax: +49 89 785 76 1792

contact@finfisher.com
www.finfisher.com

www.**finfisher**.com

FINFISHER™
EXCELLENCE IN
IT INVESTIGATION

FinFisher solutions help government law enforcement and intelligence agencies identify, locate and convict serious criminals. With its cutting-edge technology FinFisher closes the gap in traditional investigative methods.

"Made in Germany" and dedicated to the operational needs of its customers, FinFisher is known for innovative products, high quality of service and customer confidentiality. All solutions are developed by world-class IT intrusion specialists with over ten years of experience and participation in red teams in the private and government sectors.

FinFisher is the number one partner for many of the world's leading intelligence agencies. The complete portfolio has proven to be successful and is currently being used by governmental customers across the globe.

FinFisher covers three main areas of operation:

Intrusion Tools

An easy-to-use tactical solution portfolio supports covert agents in the field.

FinFisher addresses ongoing developments in the area of IT intrusion to enhance the capabilities of its governmental customers. State-of-the-art techniques complement the intelligence community's know-how and allow them to overcome challenges like encryption technologies, password protection or international mobility.

Remote Monitoring Solutions

High-end remote monitoring and deployment solutions access data and follow communication from targets' devices – tailored to individual customer requirements.

With full access to target systems, agencies can take control over locally stored information to the point of capturing encrypted data and communication.

Training and After-Sales Services

With its dedicated support services FinFisher delivers end-to-end solutions to meet all customer specific challenges.

Training Academy covers product knowledge as well as practical IT intrusion methods and techniques. With years of experience in this field, FinFisher aims to maximize the customers' capabilities and operational successes.

FINFISHER™
EXCELLENCE IN IT INVESTIGATION

Intrusion Tools

FinFisher's tactical solution portfolio was designed with the agent in mind. Easy-to-use, un-recognizable and undetectable, the kits ensure that even IT-untrained agents can extract key information without arousing any suspicion. Most importantly, they overcome many of today's challenges that traditional investigative methods face, e.g. encryption technologies or online anonymity.

» **Fin**Intrusion Kit » **Fin**USB Suite » **Fin**FireWire

Remote Monitoring Solutions

With remote monitoring and deployment solutions, governmental agencies can substantially increase the success rate of their operations. As they can be tailored to nearly all specific situations and challenges, the range of usage is extremely wide. The high-end solutions apply the latest cyber technology and are easy to use.

Monitoring solutions
» **Fin**Spy PC » **Fin**Spy Mobile

There are several options to deploy the monitoring solutions.

Deployment solutions
» **Fin**Fly USB » **Fin**Fly LAN » **Fin**Fly Web
» **Fin**Fly Exploit » **Fin**Fly ISP » **Fin**Fly NET

Training and After-Sales Services

FinFisher is recognized as the world leader in terms of training and support. With its end-to-end approach, customers will receive the ideal combination of product knowledge and practical intrusion methods and techniques gained through long-lasting experience in the field of governmental operations.

» **Fin**Training » **Fin**Support

FinIntrusion Kit
Bypasses security or encryption and remotely monitors web activities

FinUSB Suite
Quickly gathers forensic information from computer systems

FinFireWire
Covertly accesses running computer systems with password protected screensavers or before the target has logged in

FinSpy PC
Monitors security-aware targets that regularly change location, use encryption and travel extensively

FinSpy Mobile
Monitors most smartphones of security-aware targets

FinFly USB
Deploys remote monitoring solution on insertion

FinFly LAN
Deploys remote monitoring solution on target system through a Local Area Network

FinFly Web
Deploys remote monitoring solution on target system through websites

FinFly Exploit
Installs remote monitoring solution on target system using a software exploit

FinFly ISP
Deploys remote monitoring solution on target system through the Internet Service Provider

FinFly NET
Deploys remote monitoring solution on target system in „friendly" LAN environment

FinTraining
World class experts share their know how openly and give insights into best practice scenarios

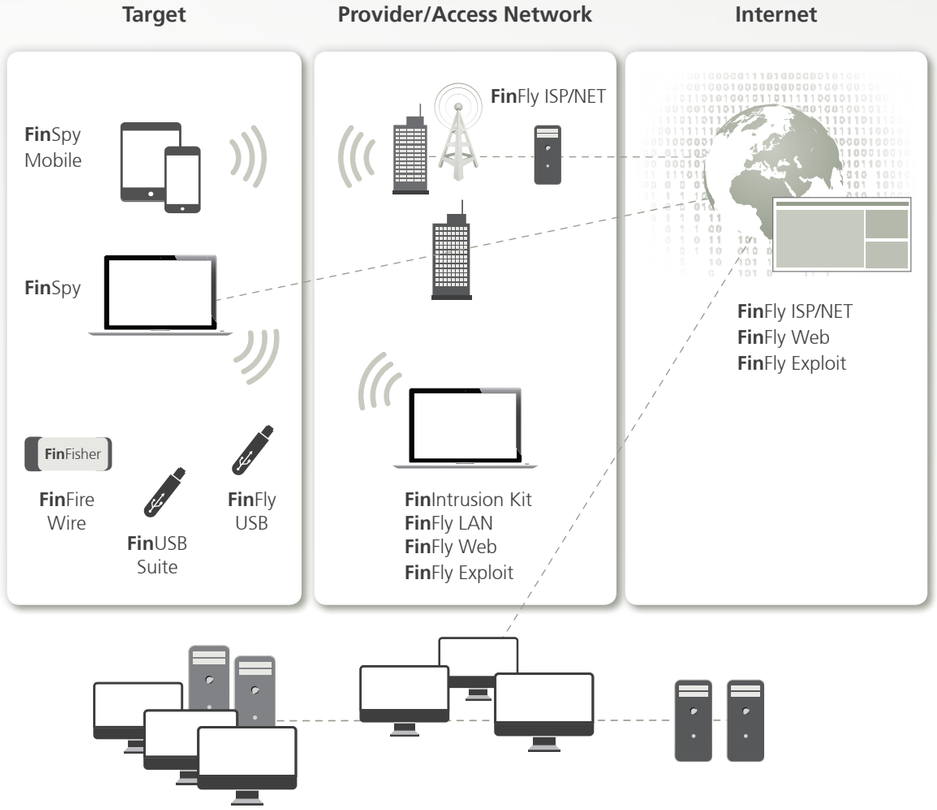
FinSupport
FinFisher's global support structure can ensure that no customer is ever left alone during critical operations

Operational Environment

FINFISHER™
EXCELLENCE IN IT INVESTIGATION

The solutions and know how can be applied individually or as a full offensive cyber security portfolio within the customer's organization. Depending on the operational scenario the solutions can be tailored to achieve the best results.

The graphic below shows in which environment the FinFisher solutions can be used.



Governmental agency's headquarters / LEMF

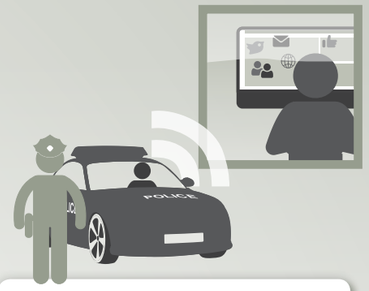
The variety of solutions is designed to address the dynamics of the environment, behavior of the target and operational needs. Driven by those factors the relevant solution can be applied. The choice of a tactical or strategic approach is determined by the closeness and accessibility of the target's system.

FinTraining & **Fin**Support

FinIntrusion Kit

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.

The kit comes as a portable covert tactical unit that includes many common IT intrusion devices, all necessary adapters and antennas.



Capabilities

» Scans and intercepts wireless networks
» Decodes encryption
» Extracts credentials

FinIntrusion Kit proven in action

The paedophile
Police found out about a local paedophile but lacked evidence to convict him. They suspected he was conducting unlawful activities from his home-based computer.
Parked outside his house, the police decoded the WPA encryption of his wireless network with the FinIntrusion Kit. From headquarters, they monitored his webmail and social media activities. Three days later the suspect was arrested.

The unlawful traveller
Special agents were following a suspect but couldn't get physical access to his notebook. He regularly used WLAN at the coffee shop, in his hotel room, in the lobby and at the airport.
Watching him with the FinIntrusion notebook, an agent blocked his WLAN access. The agent's notebook appeared in the suspect's WLAN options when he tried to regain access. Unknowingly, the suspect connected his notebook to the agent's and let him obtain all information sent through the network like passwords and emails.

FinIntrusion Kit features

» Discovers WLAN and Bluetooth devices
» Breaks passphrases (WEP within minutes, WPA1 and WPA2 using dictionary attacks)
» Catches close-by WLAN devices and records traffic and passwords
» Extracts user names and passwords (even for TLS/SSL encrypted sessions)
» Captures SSL encrypted data like webmail, video portals, online banking and more
» Assesses and validates network security

FinUSB Suite

The FinUSB Suite is a flexible product that enables law enforcement agencies to quickly and securely extract forensic information from computer systems without the requirement of IT trained agents.

The suite consists of a headquarter notebook and ten encrypted USB dongles. They look just like any common USB stick and are easy to use, as they are pre-programmed to search exactly the data that is needed. The user interface makes it easy to configure the dongle's operational options and to decrypt and analyse the gathered data.

Capabilities

» Gains complete system access
» Gathers forensic information

FinUSB Suite proven in action

The organized crime group
A covert agent got to know the leader of an organized crime group. Although the group regularly exchanged information like photos or office documents, he had no direct access to their computers or notebooks.
The agent handed the leader a USB stick with pictures and videos from his recent holiday locations. When entered into the suspect's device, the USB stick secretly extracted account credentials and office documents. After being returned to headquarters, the gathered data was decrypted and analyzed. The crime group could be constantly monitored from then onwards.

The money launderer
The suspect was active in money laundering activities. He saved the files listing his criminal trans-actions in a password-protected folder on the hard drive of his password-protected note-book.
A law enforcement agency had a source that identified this suspect, but no solid proof to get him behind bars.
A cleaning maid inserted a USB stick into the suspect's notebook. It bypassed the password protection twice and left no trace. Back at headquarters, agents had all the time they needed to analyze and process the files on the USB.

FinUSB Suite features

» Extracts user names and passwords for all common software like webmail, messengers, browsers or remote administration tools
» Silently copies files (searches disks and recycle bins, last files opened/created/edited)
» Contains network information such as chat logs, browsing history, WEP/WPA2 keys and more

FINFISHER™
EXCELLENCE IN
IT INVESTIGATION

FinFireWire

FinFireWire enables the user to quickly and covertly by-pass password protected screens or enter systems where the login screen is active. The target system can then be accessed without leaving a trace or harming essential forensic evidence.

FinFireWire consists of a complete tactical unit including adapter cards and cable set and can be managed by an easy point-and-click user interface.

Capabilities

» Bypasses user password
» Accesses covertly computer systems
» Recovers passwords from RAM
» Enables live forensics

FinFireWire proven in action

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. For legal reasons they were not allowed to use a remote monitoring system.

With FinFireWire the unit unlocked the running system in a matter of minutes and copied all files without leaving a trace of any action.

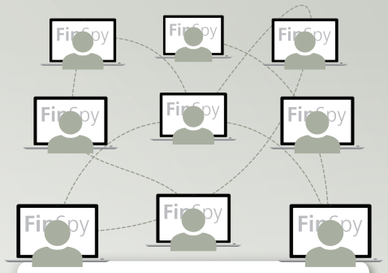
FinFireWire features

» Unlocks the user login without changing the password
» Unlocks password protected screensavers
» Dumps full RAM for forensic analysis
» Enables live forensics without rebooting the system
» Supports Windows, Mac OSX and Linux
» Works with FireWire/1394, PCMCIA and Express Card

FINFISHER™
EXCELLENCE IN IT INVESTIGATION

FinSpy PC

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 travel internationally.
When FinSpy is installed on a computer system it can be remotely controlled and accessed as soon as it is connected to Internet, no matter where in the world the system is located.



Capabilities

» Deploys remote monitoring solution on target system using a software exploit
» Monitors encrypted communication

FinSpy PC proven in action

Internet cafes
A government was trying to reduce the crime rate in its poorest metropolitan area. FinSpy PC was installed on several computer systems inside Internet cafes in this region in order to monitor them for suspicious activity, especially international VoIP communication. Using the webcam, pictures of the targets were taken while they were using the system.

Organized crime meetings
Several covert agents had failed to enter the inner circle of trust of an organized crime group. But they managed to deploy FinSpy PC on the systems of several members of this group. Using the country tracing and remote microphone functionalities, essential information could since be gathered from every meeting that they held.

FinSpy PC features

» Covertly transmits data to headquarters
» Allows live remote forensics of target's systems
» Records target's communication activities like e-mails and chats
» Monitors VoIP calls, chats, videos, contacts and file transfers
» Executes live surveillance through webcam and microphone
» Traces the target's location in almost every country
» Uses advanced filters to record only relevant information
» Supports most common operating systems (Windows, Mac OSX and Linux)
» Bypasses almost 40 regularly tested antivirus systems
» Delivers valid evidence according to European standards
» Fully integrates into law enforcement monitoring functionalities
» Allows agents to receive different user rights according to security clearances
» Makes use of anonymising proxies to avoid public detection

FinSpy Mobile

FinSpy Mobile is a field-proven remote monitoring solution for most smartphones. It 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 travel internationally. FinSpy Mobile is a very attractive solution for customers with limited access to mobile network infrastructure, as it allows them to monitor mobile phones with enhanced capabilities.

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.

Capabilities

» Remotely monitors most smartphones
» Monitors encrypted communication

FinSpy Mobile proven in action

Human trafficking gang
FinSpy Mobile was covertly deployed on smart phones belonging to several members of a human traffic gang operating across several countries. The police managed to intercept communication including SMS, MMS, e-mails and chats. Using the GPS tracking data and silent calls essential information could be gathered from every meeting that was held by this group. The data delivered sufficient evidence to convict the gang.

FinSpy Mobile features

» Covertly transmits data to headquarters
» Allows live remote forensics of target's systems
» Records target's communication activities like calls, SMS, MMS, e-mails and chats
» Downloads contact, calendar and picture files, even if they are not transmitted over any network
» Executes live surveillance through silent calls
» Traces the target's location in almost every country through GPS and cell ID
» Offers access to encrypted communication e.g. messengers, e-mails or PIN messages
» Uses advanced filters to record only relevant information
» Supports most common operating systems: Windows Mobile, iOS (iPhone/iPad), BlackBerry OS, Android and Symbian
» Delivers valid evidence according to European standards
» Fully integrates into law enforcement monitoring functionalities
» Allows agents to receive different user rights according to security clearances
» Makes use of anonymising proxies to avoid public detection

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. The FinFly USB can be used in multiple systems before being returned to headquarters.

Capabilities

» Deploys remote monitoring solutions on target systems

FinFly USB proven in action

Technical surveillance unit
The FinFly USB was successfully used by technical surveillance units in several countries to deploy remote monitoring solutions 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 were equipped with full hard-disk encryption.

Domestic terror group
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.

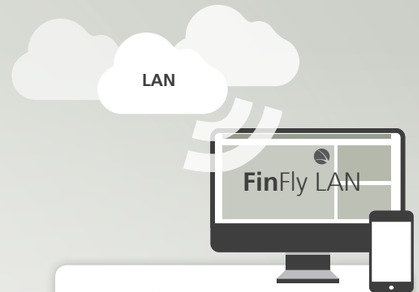
FinFly USB features

» Covertly installs remote monitoring solution on insertion in target system
» Works even when the system is switched off or has full hard-disk encryption
» Requires little or no user-interaction
» Conceals its functionality when regular files like music or office documents are placed on the device
» Looks like a common and non-suspicious USB stick

FinFly LAN

Some of the major challenges law enforcement agencies are facing are mobile targets that don't allow any physical access to their computers and do not open any unknown files they receive. Security-aware targets are almost impossible to monitor as they keep their systems up-to-date and successfully resist common exploits or intrusion techniques.

FinFly LAN covertly deploys remote monitoring solutions on target systems in Local Area Networks (Wired and Wireless). It patches files that are downloaded by the target on-the-fly, sends fake software updates or deploys the monitoring solution into visited websites.



Capabilities

» Deploys remote monitoring solutions on target systems in LAN environments

FinFly LAN proven in action

Tactical team
A tactical team had been following a target for weeks without being able to physically access his notebook. 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 to download a software update.

Anti-corruption case
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.

FinFly LAN features

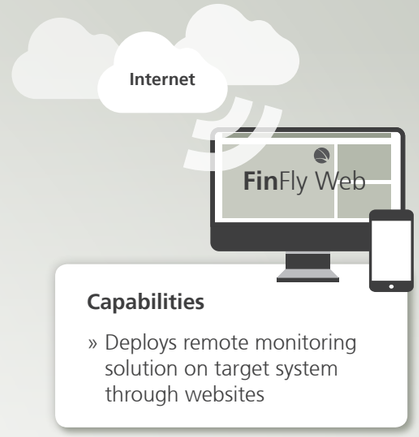
» Discovers all computer systems connected to a Local Area Network
» Works in wired and wireless networks
» Can be combined with FinIntrusion Kit for covert network access
» Deploys a remote monitoring solution in downloads of targets
» Injects remote monitoring solution as a software update
» Remotely installs a remote monitoring solution through websites visited by the target

FinFly Web

One of the major challenges in investigative monitoring is to install the solution onto the target system; especially when only a little information, like an e-mail 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 enables the agent to easily create a customised website. The solution is deployed as soon as the target visits this prepared website.



FinFly Web proven in action

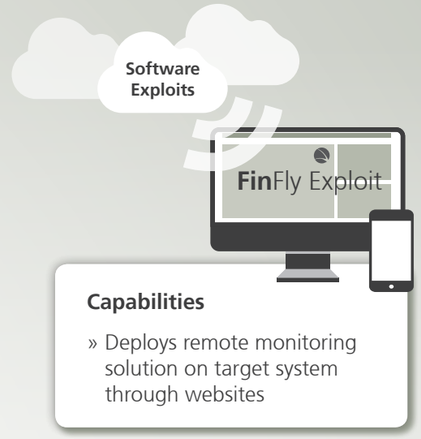
The frequent Internet user
After profiling a terrorist and getting to know his online behaviour, a technical surveillance unit created a website of interest to him and sent him the link via a discussion board. Upon opening the unit's website, a remote monitoring solution was installed on his system and monitored him from within headquarters.

FinFly Web features

» Comes with customizable web modules
» Installs itself into every website
» Can be integrated with FinFly LAN, FinFly NET and FinFly ISP to be deployed even via popular websites like webmail or video portals
» Installs remote monitoring solutions even if only the e-mail address is known
» Can target every or selected persons visiting the configured website
» Is easy to use thanks to a point-and-click interface

FinFly Exploit

Security aware targets that are familiar with common deployment techniques require advanced methods. FinFly Exploit provides an extremely powerful and reliable way to deploy remote monitoring solutions by exploiting unpatched vulnerabilities in the software the target is using. The FinFly Exploit solution offers access to a large collection of 0-day exploits for popular office programmes, Internet browsers and several other types of software.



FinFly Exploit proven in action

The 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 the target a prepared file via e-mail. The remote monitoring solution was automatically deployed once he opened the file.

Intelligence agency
A target was identified within a discussion board but no direct or e-mail contact was possible. The agency created a web server containing an Internet Explorer 0-day exploit, which deployed the solution on the target system after he opened the URL that was sent to him through a private message in the discussion board.

FinFly Exploit features

» Delivers government grade 0-day exploits

» Functions on multiple systems and patch levels without further modification

» Guarantees at least four major exploits

» Includes 6 months (1 replacement) or 12 months (2 replacements) warranty for every exploit

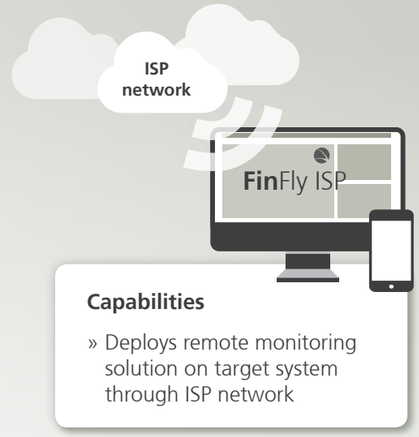
FinFly ISP

In many real-life operations, physical access to 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 solution that can be integrated into the national Internet Service Provider's access 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.

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 FinFisher's powerful remote deployment application FinFly Web that can release a remote monitoring solution via any website.



Capabilities

» Deploys remote monitoring solution on target system through ISP network

FinFly ISP proven in action

Intelligence agency
An intelligence agency used FinFly ISP in the main national Internet Service Provider network. It was enough for the system to only know the target's log-in information into the ISP network to be able to deploy a remote monitoring solution on his computer and monitor him from then onwards.

FinFly ISP features

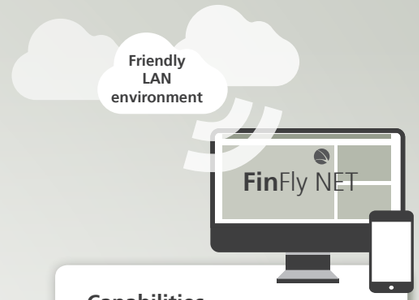
» Can be installed on an Internet Service Provider´s networks
» Handles all common protocols
» Targets selected systems by IP address (v4/v6), radius login name, DHCP or MSISDN
» Hides remote monitoring solution in downloads of targets
» Deploys a remote monitoring solution as a software update
» Remotely installs a remote monitoring solution through websites visited by the target

FinFly NET

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

To solve this, a covert remote installation of a remote monitoring solution is required.

FinFly NET is a tactical/portable solution to be deployed in a „friendly“ LAN environment on short notice. This could be in hotels, hot spots or companies where the customer has the support of the network owner. Via LAN a remote monitoring solution can be remotely installed on selected target systems.



Capabilities

» Deploys remote monitoring solution on target system in “friendly” LAN environment

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. Each method can be used either stand-alone or combined, to provide maximum success of identifying the targets of interest. Files that are downloaded by the target on-the-fly, send fake software updates for popular software or install the solution through websites.

FinFly NET proven in action

Secret service
FinFly NET was deployed in a hotel’s LAN in front of the DSL modem before the IP-traffic was transmitted to the Internet Service Provider’s network. Targets of interest could be identified in the IP-traffic by various passive profiling and identification methods and the remote monitoring solution was deployed on the positively identified target systems.

FinFly NET features

» Can be installed inside a LAN environment (e.g. in a hotel, hotspot or company)
» Works with Ethernet (1000Base-T, 1000Base-SX, 1000Base-LX)
» Identifies targets using different passive profiling and identification methods
» Hides a remote monitoring solution in downloads of targets
» Deploys a remote monitoring solution as a software update
» Installs a remote monitoring solution through websites visited by the target
» Performs IP Monitoring (PCAP files)

FINFISHER™
EXCELLENCE IN
IT INVESTIGATION

FinTraining

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

Topics like cyber war, 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-users in order to solve their daily challenges.

FinFisher combines individual training courses into a professional training and consulting program that builds up or enhances the capabilities of IT intrusion teams. The training courses are fully customized according to the end-users' operational challenges and requirements.

Capabilities

» Technical knowledge
» Operational know how

Sample Course Subjects

» Profiling targets and websites
» Tracing anonymous e-mails
» Remotely accessing webmail accounts
» Assessing the security of web servers and web services
» Using practical software exploits
» Accessing wireless communication
» Understanding attacks on critical infrastructures
» Sniffing data and user credentials of networks
» Monitoring hot spots, Internet cafés and hotel networks
» 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
» Operational Support

FINFISHER™
EXCELLENCE IN
IT INVESTIGATION

FinSupport

FinSupport delivers upgrades and updates of the FinFisher portfolio in combination with an annual support contract.

The FinFisher support webpage and support team provide the following services to customers

Online and secure access to:
» Latest user manuals
» Latest product specifications
» Latest product training slides
» Bug reporting frontend
» Latest anti virus test reports
» Feature request frontend

Regular software updates
» Bug fixes
» New features
» New major versions

Technical support via messenger:
» Bug fixing
» Partial operational support

Capabilities

» Updates of features and capabilities, operational support

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

Software Upgrades
The FinLifelineSupport also 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 functionalities, as per the customer´s roadmap (excluding hardware).