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.
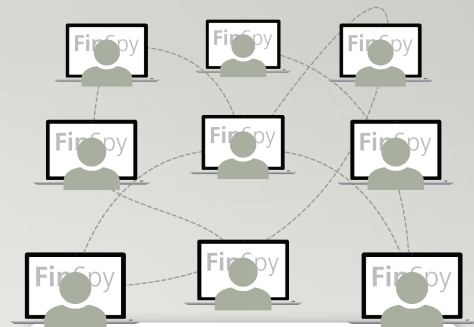
### Capabilities

» 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