FINFISHER: IT INTRUSION SEMINAR
Uganda – 19th/20th January 2012
Day 1:
1. Introduction: GammaGroup
2. IT Intrusion: "Hacking"
3. Example Cases
4. Intrusion Techniques
Day 2:
1. Introduction: GammaGroup
2. It Intrusion: "Hacking"
3. Example Cases
4. FinFisher Portfolio
2. Real-Life Operations
Gamma Group

Fields of Operation

- Technical Surveillance Equipment
- Surveillance Vans
- VIP Protection
- Communication Monitoring
- FinFisher - IT Intrusion
- Gamma International
  - IT Intrusion
  - Intelligence Training
- Gamma TSE
  - Technical Surveillance Equipment
Facts, Sales & Support Operation

- Founded: 1996
- Office Locations: 9 offices in 4 continents
- Employees: 78 globally
- Gamma Group Turnover: EUR 80 (in 2010)
- 1996 Founded
Target Clients

Gamma International serves Governmental Customers only

International Conferences & Events

Special Events:
- Gamma International, SIGINT, Intelligence, Army, Navy, Air Force

Military:
- Internal and External Security Departments

Intelligence Agencies:
- Border Security
- VIP Protection, Presidential Guard, Customs, Naval & Police (Intelligence, Special Branch, Anti-Corruption, Law Enforcement Agencies)
History and Background of FinFisher

- Research starting point was the most government used intrusion tool Backtrack (4 Million downloads)
- Generating a team of world class intrusion and research specialists and programmers (well known through public presentations at conventions i.e. Black Hat, DEFCON, SHMOOCON, etc.)
- Made in Germany exclusively by Gamma International

...
FinFisher IT Intrusion Portfolio

Remote Monitoring & Infection Solution

Tactical IT Intrusion Portfolio

IT Intrusion Training Program
Requirement of Governmental IT Intrusion

Due to changes in technology, traditional passive monitoring systems face new challenges that can only be solved by combining them with active solutions.

- Anonymity through Hotspots, Proxies, Webmail, ...
- Global mobility of Devices and Targets
- VPN Connections
- Hard-Disk Encryption (Truecrypt, Safeguard, ...)said, ...
- Data Encryption (PGP, S/MIME, ...)
- Instant Messaging (Skype, SimpLite, Blackberry Messenger, ...)
- SSL/TLS Encryption (Web, E-Mail, Messenger, ...)

Encryption Technologies:

- SSL/TLS Encryption
- PGP, S/MIME
- Truecrypt
- Safeguard
- Blackberry Messenger
- Skypete
Governmental IT Intrusion in the News

IT Intrusion is used worldwide by many governments since several years.

Germany Furious Over Chinese Spy Hackers

Georgia President's website under DDoS attack from Russian hackers

Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?

The Stuxnet malware has infiltrated industrial computer systems worldwide. Now, cyber security analysts say it's a search-and-destroy weapon meant to hit a single target. One expert suggests it may be after Iran's Bushehr nuclear power plant.

The reactor building of Iran's Bushehr nuclear power plant, pictured here on Aug. 20, is located about 750 miles south of Tehran. Is the power plant the target of the malware Stuxnet?

Vahid Salemi/AP
New laws are being established all around the world and Trojan-Horse technology is already legally used in many countries.
Human Intelligence / Online Research

Typical Operations:

- **Search Engines:**
  - Crawls public websites and archives
  - Provides important intelligence for most operations

- **Social Networks:**
  - Link Analysis: See all friends, job history, interests, etc
  - Extract GPS information from photos
  - See current activities
  - Demo: Maltego

- **Demo: Geotag Photos**

- **Demo: Maltego**

- **Demo: Geotag Photos**

1. Introduction
2. Human Intelligence
3. Tactical Operations
4. Client/Server Intrusion
5. Denial of Service
6. Example Cases
7. Conclusion
Typical Operations / USB Forensics

**Typical Operations:**

- **Public Systems:**
  - Quick Forensic Analysis (20-30 seconds)

- **Target Systems:**
  - Essential tool for Technical Surveillance Units
  - Using Sources that have physical access to automatically extract Intelligence
  - Dongle can be used e.g. by housekeeping staff

© GAMMA Group
Typical Operations:

**Wireless Networks:**
- Demo: MITM and SMB shares
- Access systems with enabled shares
- Record user names and passwords

**Lan Systems:**
- Demo: WEP/WPA Crack and FakeAP
- Provide fake access-point
- Break encryption and record all traffic

**Tactical Operations / Local Area Networks**
Table of Content

1. Introduction
2. Human Intelligence
3. Tactical Operations
4. Client/Server Intrusion
5. Denial of Service
6. Conclusion
Client Intrusion / Malicious Files

Typical Operations:

- Social Engineering:
  - Prepare files with malicious content
  - Examples: Macros for Office, Java Popups for PDF (fixed)

- Exploits:
  - Use vulnerabilities in Client software
  - New bugs found on daily basis
  - Demo: Client-Side Exploit (Browser)

Social Engineering:

Typical Operations:
Typical Operations:

Server Profiling:
- Get Information about Servers
- See old versions of websites
- Retrieve name of former attackers
- See whether server has been compromised before

Former Defacements:
- Demo: Defacement Archive
Typical Operations:

Server Intrusion / Exploits

Server Software:
- Use vulnerabilities in Server software
- Few bugs but very powerful
- Demo: Web Application Hacking

Web Applications:
- Variety of bugs, e.g. SQL Injection, XSS, File-Inclusion
- Access server through vulnerabilities in web application
- Demo: Web Application Hacking
1. Introduction
2. Human Intelligence
3. Tactical Operations
4. Client/Server Intrusion
5. Denial of Service
6. Conclusion

Table of Contents
Denial of Service / Networks

Typical Operations:

- Client Jammer:
  - Jam dedicated computers on Local Area Networks
  - Jam dedicated computers on the Internet

- Distributed Denial of Service:
  - Jam complete infrastructures
  - Demo: Jam Client
  - Simple to use software with massive effect
  - Jam dedicated computers on Local Area Networks

Client Jammer:

Demo: Jam Client

© GAMMA GROUP
1. Introduction
2. Human Intelligence
3. Tactical Operations
4. Client/Server Intrusion
5. Denial of Service
6. Conclusion
Most Government Agencies use IT Intrusion techniques since several years. Due to the rapid change of the Internet and communication techniques, IT Intrusion is an absolute requirement in addition to traditional lawful monitoring solutions. There’s a wide range of possible techniques and the Operators need to be highly trained in order to use the right techniques in the right places.
Thank you for your attention!

End of Day 1.

Questions?
2. Real-Life Operations

Support

Training Courses

Product Range

1. FinFisher Portfolio

Day 2:
The FinUSB Suite is designed to covertly extract data from Target Systems.

Typical Operations:
- Dongle can be used e.g. by housekeeping staff
- Extract Intelligence
- Using Sources that have physical access to automatically

Target Systems:
- Essential tool for Technical Surveillance Units
- Quick Forensic Analysis (20-30 seconds)

Public Systems:
- From Target Systems.

Data is fully encrypted and can only be decrypted in HQ.

Typical Operations:
- Quick Forensic Analysis (20-30 seconds)
- Essential tool for Technical Surveillance Units

The FinUSB Suite is designed to covertly extract data.
FinUSB Suite / Core Features

- Extraction of Usernames and Passwords for all common software like:
  - E-Mail Clients
  - Messengers
  - Browsers
  - E-Mail Clients

- Silent Copying of Files (Search Disks, Recycle-Bin, Last Opened)

- Compilation of System Information (Running/Installed Software, Hard-Disk Information, ...) NetworK Information (Chat Logs, Browsing History, WEP/WPA(2) Keys, Cookies, ...)

- Extraction of Usernames and Passwords for all common software
The FinUSB HQ provides target-specific configurations and professional data analysis.
Sample report generated by the FinUSB HQ software.
- 2 Bootable CD-Roms
- 10 FinUSB Dongles
- Notebook (Windows 7, FinUSB HQ)

FinUSB Suite / Portable Unit
Tactical IT Intrusion Portfolio

Remote Monitoring & Infection Solution

IT Intrusion Training Program

FinUSB Suite

FinFireWire

FinIntrusion Kit
FinIntrusion Kit / Operational Usage

The FinIntrusion Kit is a portable IT Intrusion kit which can be used for various
strategic and tactical attacks by red-teams inside or outside the Headquarters.

Typical Operations:

Wireless Networks:
- Get access to E-Mail Accounts
- Gain access to remote Infrastructures and Web servers
- Break Encryption and record all Traffic

Access Remote Systems:
- Record Usernames and Passwords even for SSL-encrypted sites (e.g. Facebook, MySpace, Online Banking)

Operational Usage

- Gain access to remote Infrastructures and Web servers
- Break Encryption and record all Traffic
- Record Usernames and Passwords even for SSL-encrypted sites (e.g. Facebook, MySpace, Online Banking)
FinIntrusion Kit / Core Features

- Discover Wireless LANs (802.11) and Bluetooth® devices
- Recover WEP (64 and 128 bit) Passphrase within 2-5 minutes
- Break WPA1 and WPA2 Passphrase using Dictionary Attacks
- Recover WEP (64 and 128 bit), WPA2 Passphrase
- Emulate Rogue Wireless Access Point (802.11)
- Actively monitor local Area Network (Wired and Wireless) and extract Usernames and Passwords and SSL/TLS-encrypted Sessions like GMail, Hotmail, Facebook, etc.
- Remotely break into E-Mail Accounts using Network, System- and Password-based Intrusion Techniques
The Operation Center provides easy-to-use point-and-click attacks.
• Wireless Intrusion Hardware
• FinTrack bootable CD-Rom
• Autorun and bootable USB Device
• Notebook (FinTrack, FTOC)

FinIntrusion Kit / Covert Tactical Unit
FinFireWire / Operational Usage

The FinFireWire product enables quick and covert access to locked Target Systems without losing critical evidence due to requiring to reboot the system.

**Unlock Running Systems:**
- Get live access to running systems, no more need to reboot

**Operation:**
- Modification of system is only temporary and reverted after
- Get live access to running systems, no more need to reboot

**Dump RAM Information:**
- Extract data from physical RAM for forensic analysis

**Typical Operations:**
- Recover crypto passwords and more

**Features:**
- Extract data from physical RAM for forensic analysis
- Unlock running systems
- Dump RAM information
- Recover crypto passwords and more
FinFireWire / Core Features

• Works with FireWire/1394, PCMCIA and Express Card

Encryption Passwords

Common Forensic tools like EnCase to discover e.g. Hard-Disk encryption information.

All configured RAM can be recorded into a file and later analyzed in common Forensic tools like Encase to discover e.g. Hard-Disk Encryption Passwords.

• No reboot is required, quick and covert access is possible without providing any password.

The product enables the agent to access the Target System without providing any password.

Works with Microsoft Windows (XP -> 7), Linux and Mac OS X

The product functions on any major Operating System such as Microsoft Windows (XP -> 7), Linux and Mac OS X.
Once connected to the Target System, the software provides an easy-to-use point-and-click Interface.
• FinFireWire Software
• FinFireWire Portable Unit
• FireWire Cables for all Ports
• PCMCIA / Express Card Adapters
Table of Content

1. Introduction
2. Tactical IT Intrusion Portfolio
3. Remote Monitoring & Infection Solutions
4. IT Intrusion Training Program
5. Summary
Remote Monitoring and Infection Solutions

Remote Monitoring

IT Intrusion Training Program

Tactical IT Intrusion Portfolio

FinSpy

FinSpy Mobile

FinFly
FinSpy / Operational Usage

FinSpy is an advanced Intrusion system which once implemented into a Target System guarantees full access to the system with advanced features.

Typical Operations:

- Monitor Encrypted Communication:
  - Record even SSL-encrypted Communication
- Full File-System Access
- Surveillance through Webcam and Microphone
- Remotely Access Target Systems:
  - Full access to all communication including Skype
  - Live Monitoring even if Targets are in Foreign Countries

Monitor Encrypted Communication:

System guarantees full access to the system with advanced features.
• The product functions on any major Operating System such as Microsoft Windows (2000 - 7), Mac OSX and Linux
• All communication and all temporary files are fully encrypted
• Target software is regularly tested to bypass the world’s top 40 Anti-Virus applications and hide deep inside the Target System
• Target location of the Headquarters is completely hidden through anonymizing Proxies around the world
• Court-proof Evidence according to European Standards
• The system can be fully integrated with an existing Law Enforcement Monitoring Functionality (LEMF)

FinSpy / Core Features
FinSpy / Target Features

- Full Skype Monitoring (Calls, Chats, File Transfers, Video, Contact List)
- Recording of all VoIP communication
- Live Surveillance through Webcam and Microphone
- Full File Access: Live File-Browsing, capturing of deleted/printed/opened Documents
- Process-based Keylogger for faster analysis
- Country Tracing of Target
- Forensic Tools for Live Remote Forensic
- Enhanced Filtering of data and recorded information
With the FinSpy Master LEMF Interface, the tactical solution can be fully integrated into the Law Enforcement Monitoring Functionality (LEMF). The infected Target System sends a heartbeat to the FinSpy Relay(s) as soon as it is online. The infected Target System sends a heartbeat to the FinSpy Relay(s). The FinSpy Relay(s) forward connections between Targets and Master and Agents and stores the data.
The whole system is controlled through the easy-to-use graphical user interface.
- FinSpy Master and Relay
- FinSpy Agent(s)
FinFly USB / Operational Usage

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

Typical Operations:

- Deploy FinSpy on running System:
  - Plug-in USB in Running Target System to install FinSpy

- Deploy FinSpy on turned off System:
  - Boot USB to automatically deploy FinSpy
FinFly USB / Core Features

- Common USB Device with hidden functionality
- Automatic execution on Windows 2000/XP based Systems
- One-click execution on Windows Vista/7 based Systems
- Automatic installation through bootable System
- Can even infect switched off Target Systems when the Hard-Disk is fully encrypted with TrueCrypt
- Can even infect switched off Target Systems when the Hard-Disk is fully encrypted with TrueCrypt
- Common USB Device with hidden functionality
• FinFly USB Dongles

• Full Integration into Finspy

• 5 FinFly USB Dongles
Remote Monitoring and Infection Solutions

- FinSpy Mobile
- IP
- LAN
- Web
- USB

IT Intrusion Training Program
Tactical IT Intrusion Portfolio
Financial IT Intrusion Solution
FinFly Web is designed to covertly inject a configurable software into remote Target Systems through integration in Websites.

**Typical Operations:**
- Deploy FinSpy through custom Homepages:
  - Create Infection Module for Integration into FinFly LAN and FinFly ISP Module
  - Create FinFly LAN/FinFly ISP Module
  - Infect Target with FinSpy when it visits the Website
  - Create Website of Target Interest Field

**Operations:**
- Target Systems through integration in Websites.
FinFly Web / Core Features

- All common Browsers are supported
- Various Modules are available for Infection
- All common Browsers are supported
- Supports Generation of Stand-Alone Websites to Infect Targets
- Creates FinFly LAN/FinFly ISP Packages to Inject the Modules
- Even into popular sites like Gmail, YouTube, etc.
- Various Modules are available for Infection
- Board is known
  where only E-Mail Address or Username inside a Discussion Board is known

FinFly Web / Core Features
FinFly Web / LAN / ISP Integration

- Online Banking
- Webmail
- Video Portal
- Social Network

Target for Infection (W)LAN

FinFly ISP

FinFly LAN

FinFly Web

Internet Gateway

Local ISP

(W)LAN
FinFly Web User Interface
Remote Monitoring and Infection Solutions

- IT Intrusion Training Program
- Tactical IT Intrusion Portfolio
- & Infection Solution
- FinSpy Mobile
- 1SIP
- LAN
- Web
- USB

FinSpy

FinSpy Mobile

FinSpy Mobile
FinFly LAN / Operational Usage

FinFly LAN is designed to covertly inject software updates into Target Systems in Local Area Networks.

**Typical Operations:**

- **Deploy by infecting fake software updates:**
  - Install FinSpy on Target System in Local Area Network
  - Deploy FinSpy through LAN:
    - Deploy by infecting common Websites (e.g. YouTube)
    - Deploy by infecting common Networks through Hotspot Wireless
  - Install FinSpy on Target System through Hotspot Wireless
  - Deploy FinSpy through Hotspots:

FinFly LAN is designed to covertly inject a configurable software into remote Target Systems in Local Area Networks.
FinFly LAN / Core Features

- Discovers all computer systems connected to the Local Area Network via IP Address, MAC Address, Host-Name.
- Works in Wired and Wireless (802.11) networks.
- Networks via IP-Address, MAC-Address, Host-Name.
- 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.
- Can be combined with FinIntrusion Kit for covert network access.

FinFly LAN / Core Features
FinFly LAN

- IP, MAC, HOST
- Target

FinFly LAN / Workflow
FinFly LAN User Interface
Remote Monitoring and Infection Solutions

Remote Monitoring & Infection Solutions

Tactical IT Intrusion Portfolio

FinSpy Mobile
- ISP
- LAN
- Web
- USB

FinSpy

FinSpy Mobile

IT Intrusion Training Program

Tactical IT Intrusion Portfolio

FinSpy Mobile

IX Infection Solution
Remote Monitoring
FinFly ISP/Operational Usage

FinFly ISP is designed to covertly inject a configurable software into remote target systems through ISP networks.

Typical Operations:

- Install in backbone of ISP:
  - Deploy in Backbone of ISP:
  - Install FINSpy on Target Systems by selecting their Username/RADIUS name for Infection

- Install in small ISP/LAN Environments to install FINSpy on local clients (e.g., in Hotels or Corporate Networks)

Install in Core of Local Area Networks:
FinFly ISP / Core Features

- Identify Targets by:
  - Username, Password (e.g. xDSL)
  - MAC-Addresses (Cable)
  - IMSI, T-MeSI, MlSISDN (Internet Access in Mobile Networks)
  - Dial-in phone number (ISDN, POTS)
  - Username, Password (e.g. xDSL)

- Hides Remote Monitoring Solution in Downloads of Targets
- Remotely Installs Remote Monitoring Solution through Websites visited by the Target
- Injects Remote Monitoring Solution as Software Updates
FinFly ISP / Deployment Example
FinFly ISP / Workflow

LEMF

Infection Method

Username

Payload

Infection Proxy

FinFly ISP

Target for Infection

FinFly ISP

Mgmt. Server

FinFly ISP

Mgmt. Workstation

INFECTING

Tgt = "Username"

is required

193.99.144.85

Search for

192.99.144.85

Search for

193.99.144.85
• FinFly ISP / Hard- and Software

• Hardware – dependent on required performance

• FinFly ISP User Interface (GUI)
Remote Monitoring and Infection Solutions

- IT Intrusion Training Program
- Tactical IT Intrusion Portfolio
- FinSpy
- FinFly
- FinSpy Mobile
FinSpy Mobile / Operational Usage

FinSpy Mobile is an advanced intrusion system which once implemented into a Target Phone guarantees full access to the communication and built-in features.

Typical Operations:

- Spy calls to listen Live to Phone
- GPS Tracking of Target Phones
- Live Surveillance:
  - Messenger
  - Record even encrypted communication like BlackBerry
  - Full access to all basic communication like SM/EMS, Calls, etc.

Monitor all Communication:
• The product functions on any major Operating System such as BlackBerry, iOS (iPhone), Android and Windows Mobile / Windows Phone.

• Basic Communication Interception like Calls, SMS/MMS, Call Logs

• Live Surveillance through Silent Calls

• Location Tracking (Cell IDs and GPS Data)

• Recording of Incoming and Outgoing E-Mails

• BlackBerry Messenger Surveillance

• All communication and all temporary files are fully encrypted

FinSpy Mobile / Core Features
The FinSpy Mobile server is connected by infected Target Phones over the Internet (GPRS / UMTS / Wi-Fi) or through the VoIP Server (SMS / Phone Calls). The FinSpy Master accepts the connections and stores the data inside the database.

Infected Target Phone

TCP/IP

FinSpy Agents

FinSpy Master

Mobile Provider

FinSpy Relay

External VoIP Provider

FinSpy VoIP Server

Internet

SMS/Voice-Calls

Target Phone comunicates through GPRS/UMTS/Wi-Fi!
The whole system is controlled through the easy-to-use Graphical User Interface.
Various infection techniques exist like:

• Remote Injection via SNS to Target Phone
• Tactial Infection via Cable or Bluetooth
• Provider-Supported Injection via WAP Push
• Infection via Bookmark SMS to Target Phone
- FinSpy Master and Relay
- FinSpy VoIP Server PRI Cards for up to 30 lines
- FinSpy Mobile / Strategic System
- FinSpy Agent(s)
- FinSpy Master and Relay
<table>
<thead>
<tr>
<th>Table of Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Day 2:</strong></td>
</tr>
<tr>
<td>1. FinFisher Portfolio</td>
</tr>
<tr>
<td>2. Real-Life Operations</td>
</tr>
<tr>
<td>- Support</td>
</tr>
<tr>
<td>- Training Courses</td>
</tr>
<tr>
<td>- Product Range</td>
</tr>
</tbody>
</table>
FinFisher Training Program.

Custom training courses and long-term training programs are part of the

- Fully practical trainings
- Real-life usable techniques
- Limited to 2-4 participants
- Trainings conducted in Germany or In-Country

offensive IT Intrusion trainings is available.

With Gammas Team of world-leading IT Intrusion experts, a wide-range of
Outline: This course gives a practical introduction to the IT Intrusion field covering a wide-range of basic IT Intrusion techniques which are demonstrated and trained in real-life scenarios.

Topics: Profiling, Attacking, Advanced Topics

Duration: 5-10 days
This course covers all topics related to Wireless IT Intrusion including the monitoring of Wireless networks, breaking the existing encryption protocols, attacking Wireless clients and more.

Outline: This course covers all topics related to Wireless IT Intrusion including the

Topics: WLAN 802.11, Bluetooth

Duration: 5 days
Outline: This course is a practical training on using exploits for IT Intrusion purposes. It covers the latest Adobe Acrobat exploits to hide FinSpy inside PDF files, among other topics.

Topics: Exploit Introduction, Metasploit, Simple Reverse Engineering, Duration: 5-10 days.
Outline: This course focuses on Web Application security and shows many different ways on analyzing them for security issues and using them to get remote access to web-servers.

Topics: Identifying Software, Exploiting Vulnerabilities

Duration: 5-10 days

This course focuses on Web Application security and shows many different ways on analyzing them for security issues and using them to get remote access to web-servers.

Outline: This course focuses on Web Application security and shows many different ways on analyzing them for security issues and using them to get remote access to web-servers.

Outline: This course focuses on Web Application security and shows many different ways on analyzing them for security issues and using them to get remote access to web-servers.

Outline: This course focuses on Web Application security and shows many different ways on analyzing them for security issues and using them to get remote access to web-servers.

Outline: This course focuses on Web Application security and shows many different ways on analyzing them for security issues and using them to get remote access to web-servers.
Outline: This course covers a wide-range of penetration testing examples which is conducted through several practical examples.

Topics: Network Attacks, Metasploit, Backdoors, Phishing, Wardialing, SSL Attacks

Duration: 5-10 days

This course covers a wide-range of penetration testing examples which is conducted through several practical examples.
All Offensive IT Intrusion related topics can be provided on request.

- Profiling of Target Websites, Networks and Persons
- Tracing of anonymous E-Mails
- Remote access to Webmail Accounts
- Intercept and Record Calls (VoIP and DECT)
- Monitoring Hot-Spots, Internet Cafes and Hotel Networks
- Security Assessment of Web-Servers & Web-Services
- Attacks on critical Infrastructures
- Attacks on critical Infrastructures
- Cracking Passwords
- Tracking of anonymous E-Mails
- Profiling of Target Websites, Networks and Persons

Fintaining / Other Example Topics
# Table of Content

1. FinFisher Portfolio
   - Product Range
   - Training Courses
   - Support

2. Real-Life Operations

Day 2:
Professional Support

Online Support Website includes:
- User Manuals
- Product Roadmaps
- Product Change-logs
- Frequently Asked Questions
- Bug Reporting System
- Download from Web
- Via Online Update System

Software updates provided via:
- Download from Web
- Via Online Update System

Online Support Website includes:
Day 2:

1. FinFisher Portfolio

2. Real-Life Operations
Operational Achievements / Tactical IT Intrusion Portfolio

Scenario 1: FinIntrusion Kit I
An Intrusion Unit parks with a Surveillance vehicle in front of a target company and breaking with a directional antenna connected to the FinIntrusion Kit into the target’s network and extracting confidential information, passwords, and user accounts.

Scenario 2: FinIntrusion Kit II
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.

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.

Scenario 2: FinIntrusion Kit II

Information, passwords, and user accounts are entered into the target’s network and extracted confidential information. A directional antenna connected to the FinIntrusion Kit is used to remotely break into the target’s network.

An Intrusion Unit parks with a Surveillance Vehicle in front of a target company and breaking with a directional antenna connected to the FinIntrusion Kit.

Scenario 1: FinIntrusion Kit I
Operational Achievements / Tactical IT Intrusion Portfolio

Scenario 3: FinFireWire

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.

The unit would have lost all data by switching off the system as the hard-disk was fully encrypted. The unit used FinFireWire to unlock the running Target system enabling the agent to copy all files before switching the computer off.
Operational Achievements / Remote Monitoring

Scenario 5: FinSpy
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. The build-in Evidence Protection enabled the LEA to use the information in court (in accordance to EU standards). The evidence was presented in foreign individual’s trials, especially Skype communication to Internet Cafes in critical areas in order to monitor them for suspicious activity.

Scenario 6: FinSpy Mobile
FinSpy Mobile was installed on a BlackBerry where the BlackBerry Mail and Messaging are encrypted via the RIM server. In such a case, FinSpy Mobile will guarantee full access to Phone & Spy Calls, SMS, GPS location, BB Messaging etc.
Scenario 7: FinSpy / VIP Protection

FinSpy was deployed on the Notebook and Mobile Phone of a VIP in order to be able to monitor the surroundings of a VIP in case of emergencies. The same procedure was used and have the capability to identify the current location of a VIP in order to be able to monitor the surroundings with undercover operators in several cases.

Operational Achievements / Remote Monitoring
Operational Achievements / Remote Infection

Scenario 8: FinFly LAN/FinIntrusion Kit
A Technical Surveillance Unit was following a Target for weeks without being able to physically access the target. They used FinFly LAN to install the Remote Monitoring Solution in form of payload within the target’s downloads (.exe, .scr, .doc, .xls etc.) when he was using a public Hotspot at a coffee shop.

Scenario 9: FinFly ISP/FinFly Web
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 offending websites. The code was covertly injected into the targeted websites by covertly injecting the FinFly Web payload into government websites. 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 offending websites. 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 offending websites. 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 offending websites.
Operational Achievements / Training Examples

- Profiling of Target Websites and Persons
- Tracing anonymous Emails
- Remote access to Webmail Accounts
- Practical Software Exploitation
- Wireless IT Intrusion (WLAN/802.11 and Bluetooth)
- Monitoring Hot-Spots, Internet Cafes and Hotel Networks
- Sniffing Data and User Credentials of Networks
- Intercepts and Records Calls (VoIP and DECT)
- Attacks on critical Infrastructures
- Security Assessment of Web-Servers & Web-Services
- Cracking Password Hashes
- Monitoring of Target Websites and Persons
- Tracking of Target Websites and Persons
- Tracking anonymous Emails
- Remotely accessing Webmail Accounts
- Practical Software Exploitation
FinFisher – The Complete IT Intrusion Portfolio
Why Gamma as a Partner?

Commercial:
- Long-term, stable & strong partner
- Entirely self-financed, independent and privately-owned company
- All solutions are made in accordance to end-users requirements
- Existing global support infrastructure
- Most advanced solutions and portfolio in the market
- Many years of experience on the field of Governmental IT Intrusion

Technical:
- Many years of experience on the field of Governmental IT Intrusion
- Most advanced solutions and portfolio in the market
- Existing global support infrastructure
Thank you for your attention!

Questions?