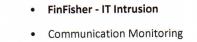


Gamma Group - Fields of Operation Gamma TSE Technical Surveillance Equipment Surveillance Vans G2Systems Intelligence Training





• VIP Protection

• Gamma International



We only serve Governmental Customers

• Law Enforcement Agencies:

Police (Intelligence, Special Branch), Anti -Corruption, VIP Protection, Presidential Guard, Customs, Naval & Boarder Security



• Intelligence Agencies:

Internal and External Security Departments

• Military:

Intelligence, Signal Intelligence, Army, Navy, Air Force

• Special Events:

International Conferences & Events



© GAMMAGROUP

Facts, Sales & Support Operation Founded: 1996 Office Locations: 9 offices in 4 continents Partner Sales & Support: Southern America Gamma Group Turnover: EUR 80' (in 2010) Employees: 78 Globally

History and Background of FinFisher

rem ti

Research starting point was the most government used
 Intrusion tool worldwide: Backtrack (4 Million downloads)



- Winning one of the top Intrusion Specialists and founder of Backtrack to build up required capabilities and to design a comprehensive portfolio
- Generating a team of world class intrusion and research specialists and programmers (well known through public presentations at conventions i.e. Black Hat, DEFCON)



© GAMMAGROUP

Challenges in LI systems

7

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

- Encryption technologies:
 - SSL/TLS Encryption (Web, E-Mail, Messenger, ...)



Instant Messaging (Skype, SimpLite, Blackberry Messenger ...)

≅ BlackBerry

- Data Encryption (PGP, S/MIME, ...)
- Hard-Disk Encryption (Truecrypt, SafeGuard, ...)



VPN Connections

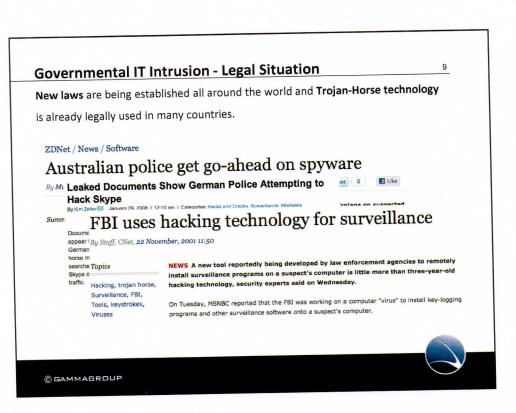


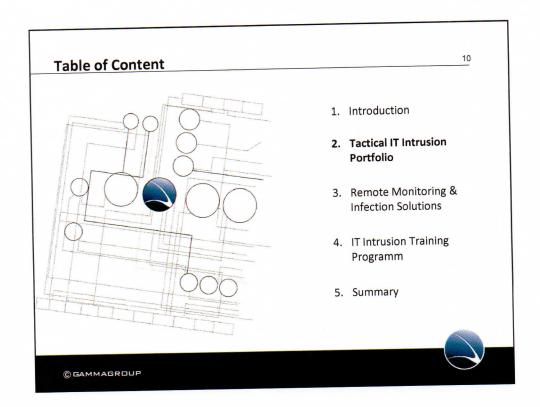
Global mobility of Devices and Targets
 Anonymity through Hotspots, Proxies, Webmail, ...

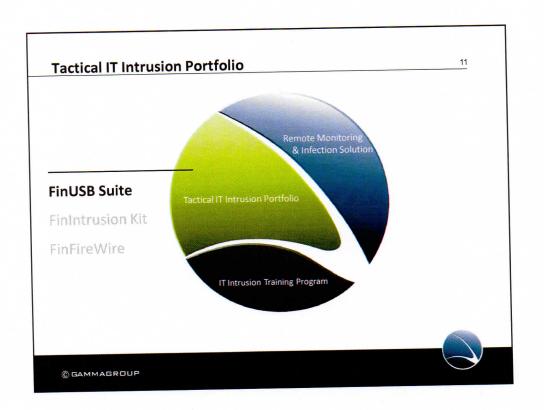












FinUSB Suite / Operational Usage

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



Typical Operations:



Public Systems:

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



Target Systems:

- Using Sources that have physical access to automatically extract Intelligence
- Dongle can be used e.g. by housekeeping staff
- Data is fully encrypted and can only be decrypted in HQ



© GAMMAGROUP

FinUSB Suite / Core Features

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









- Messengers
- Browsers













Extracting Network Information (Chat Logs, Browsing History, WEP/WPA(2) Keys, Cookies, ...)

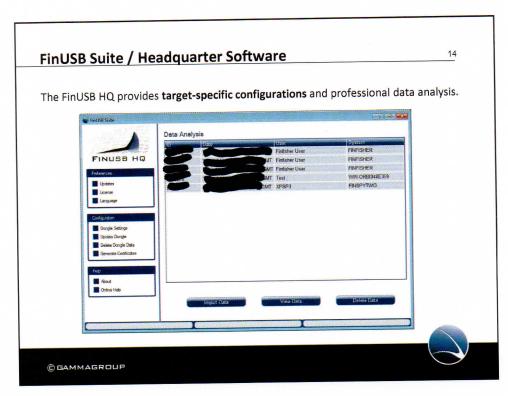


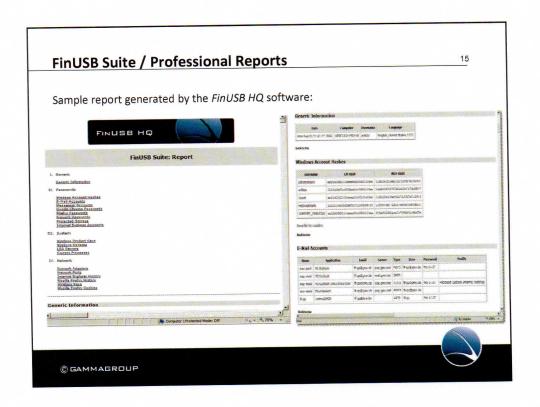
Compilation of System Information (Running/Installed Software, Hard-Disk Information, ...)



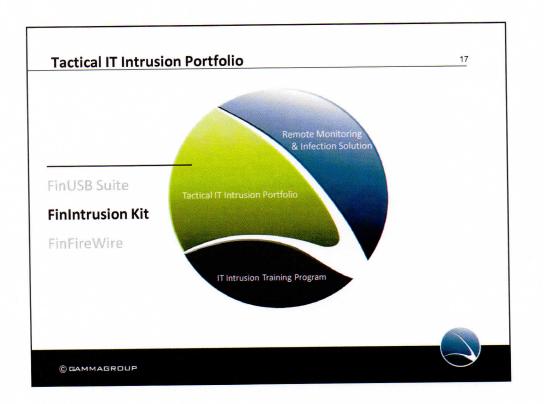












FinIntrusion Kit / Operational Usage

18

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:

- Break Encryption and record all Traffic
- Record Usernames and Passwords even for SSL-encrypted sites (e.g. Facebook, MySpace, Online Banking)



Access remote Systems:

- Gain access to remote Infrastructures and Webservers
- Get access to E-Mail Accounts



© GAMMAGROUP

FinIntrusion Kit / Core Features

19

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



- Emulate Rogue Wireless Access-Point (802.11)
- Actively monitor Local Area Network (Wired and Wireless) and extract
 Usernames and Passwords even for SSL/TLS-encrypted Sessions like
 GMail, Hotmail, Facebook, etc.

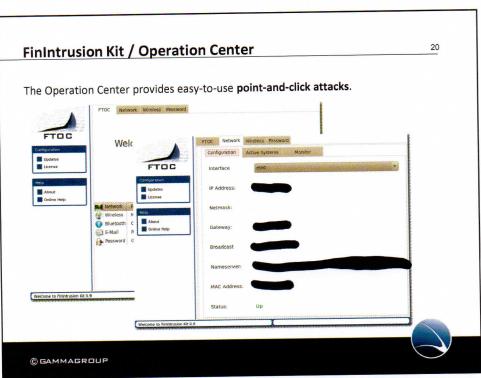


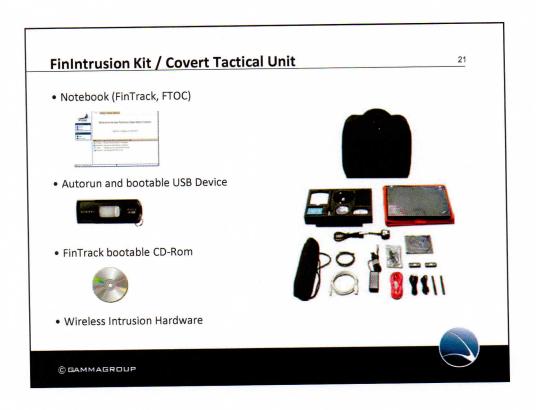
 Remotely break into E-Mail Accounts using Network-, System- and Password-based Intrusion Techniques

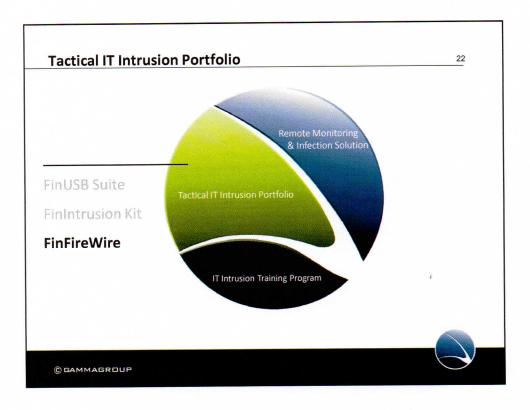












FinFireWire / Operational Usage

23

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

Typical Operations:



Unlock Running Systems:

- Get Live access to running Systems, no more need to reboot and loose essential Evidence
- Modification of system is only temporary and reverted after Operation



Dump RAM Information:

- Extract data from physical RAM for Forensic analysis
- Recover crypto passwords and more



FinFireWire / Core Features

24

 The product functions on any major Operating System such as Microsoft Windows (XP -> 7), Linux and Mac OSX



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



 No reboot is required, quick and covert access is possible without loosing important evidence



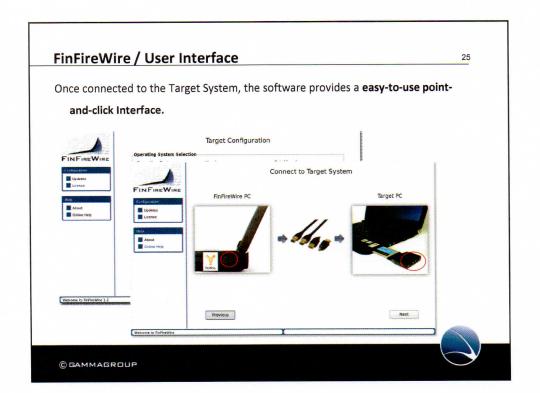
 All configured RAM can be recorded into a file and later analyzed in common Forensic tools like Encase to discover e.g. Hard-Disk
 Encryption Passwords

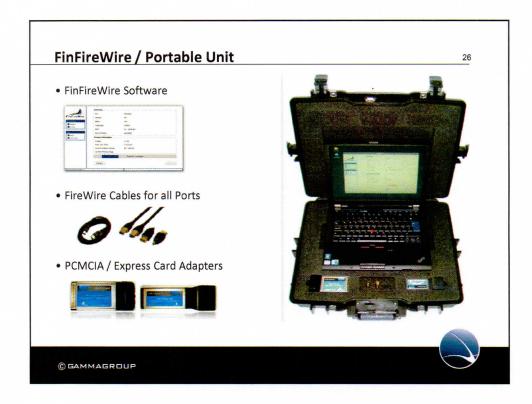


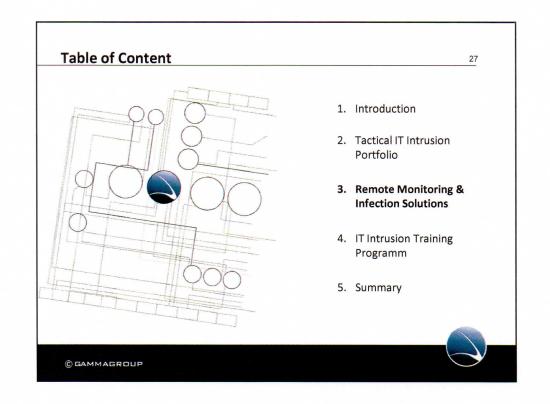
Works with FireWire/1394, PCMCIA and Express Card

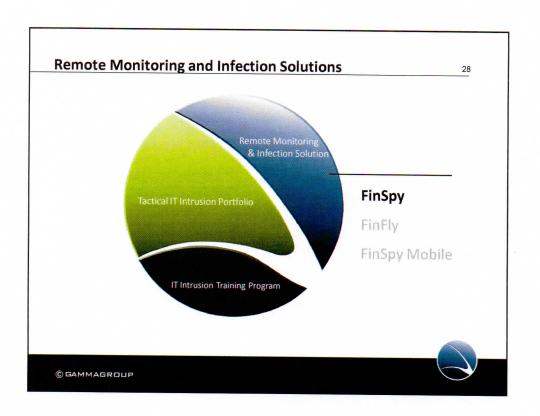












FinSpy / Operational Usage

29

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:

- Full access to all communication including Skype
- Record even SSL-encrypted Communication



Remotely Access Target Systems:

- Full File-System Access
- Surveillance through Webcam and Microphone
- Live Monitoring even if Targets are in foreign Countries



FinSpy / Core Features

30

 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



- True location of the Headquarter is completely hidden through anonymizing Proxies around the world
- The system can be fully integrated with an existing Law Enforcement Monitoring Functionality (LEMF)
- Court-proof Evidence according to European Standards







© GAMMAGROUP

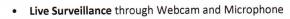
FinSpy / Target Features

21

• Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)



• Recording of all VoIP communication





Country Tracing of Target



 Full File-Access: Live File-Browsing, capturing of deleted/printed/opened Documents



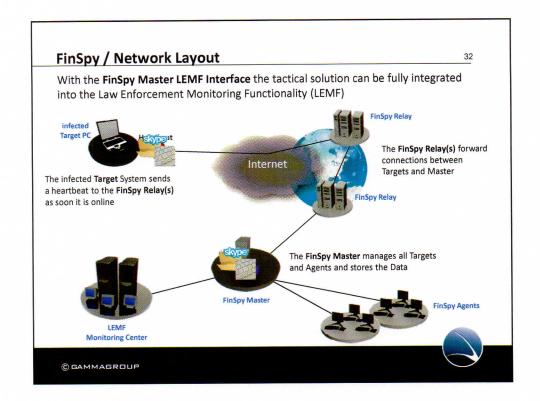
Process-based Keylogger for faster analysis
 Forensic Tools for Live Remote Forensic

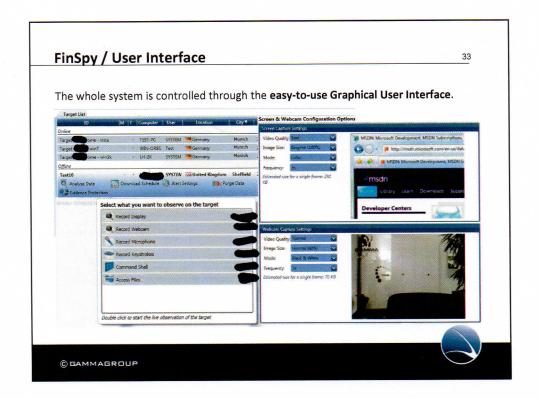


Enhanced Filtering of data and recorded Information

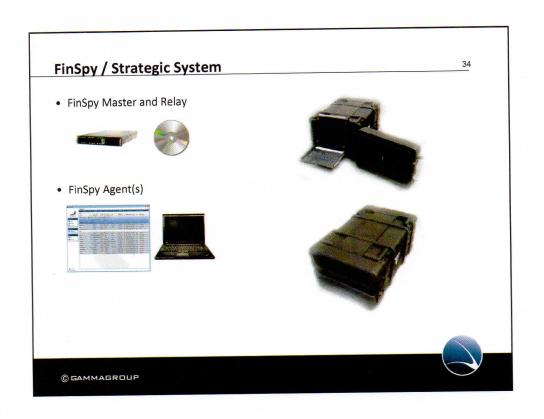


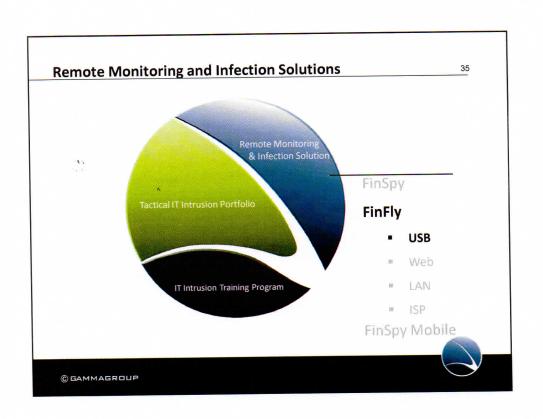










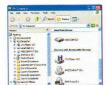


FinFly USB / Operational Usage

36

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



© GAMMAGROUP

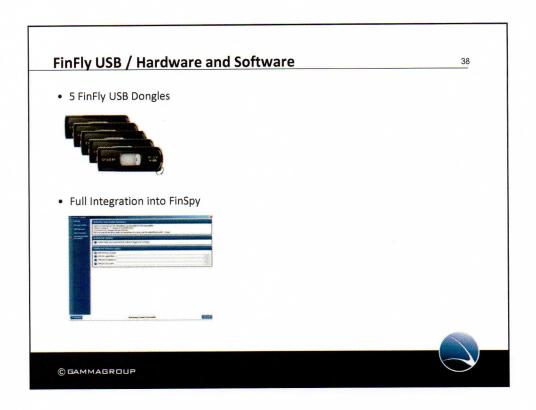
FinFly USB / Core Features

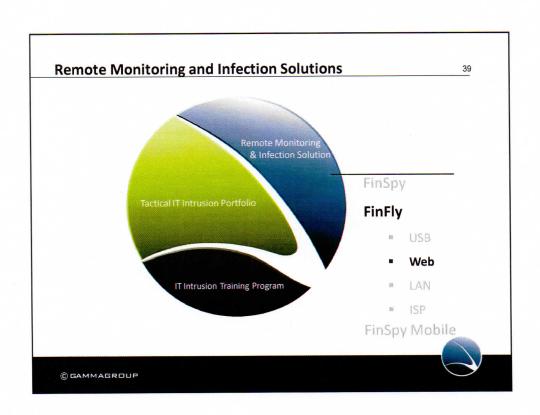
37

- Common USB Device with hidden functionality
- crise See
- 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











FinFly Web / Operational Usage

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 Website of Target Interest Field
- Infect Target with FinSpy when it vists the Website



Create FinFly LAN/FinFly ISP Module

Create Infection Module for Integration into FinFly LAN and



© GAMMAGROUP

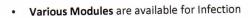
FinFly Web / Core Features













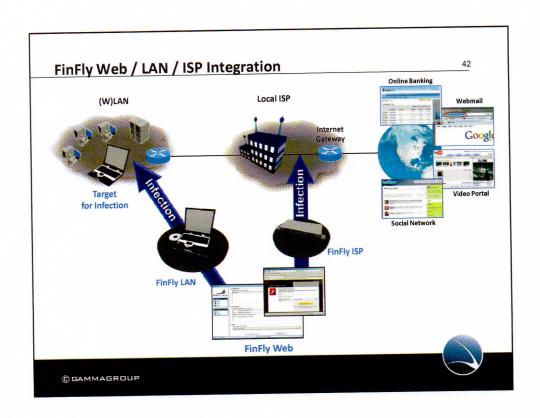


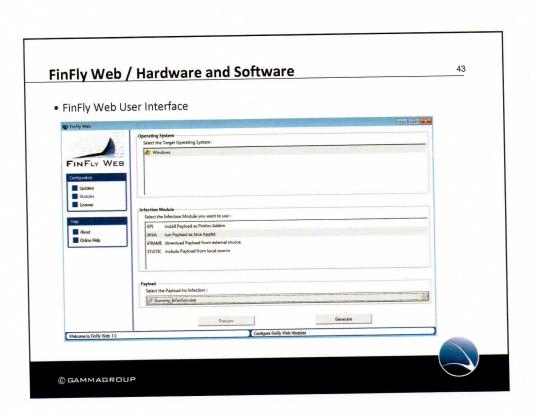


- Supports generation of **Stand-Alone Websites** to infect Targets where only E-Mail Address or Username inside a Discussion Board is known
- Creates FinFly LAN/FinFly ISP Packages to inject the Modules $\textbf{even into popular sites} \ \mathsf{like} \ \mathsf{GMail}, \ \mathsf{YouTube}, \ \mathsf{etc}.$

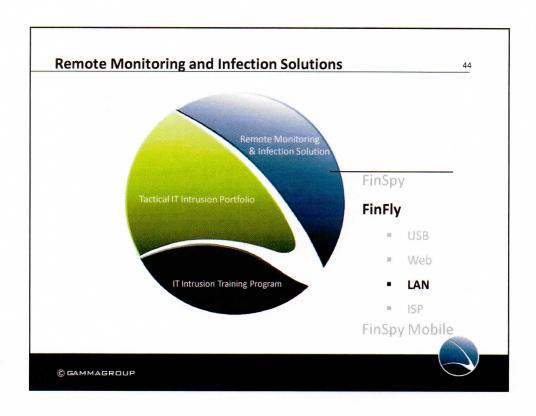














45

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

Typical Operations:



Deploy FinSpy through Hotspots:

- Install FinSpy on Target System through Hotspot Wireless Network
- Deploy by infecting common Websites (e.g. YouTube)



Deploy FinSpy through LAN:

- Install FinSpy on Target System in Local Area Network
- Deploy by injecting fake Software Updates





FinFly LAN / Core Features

46

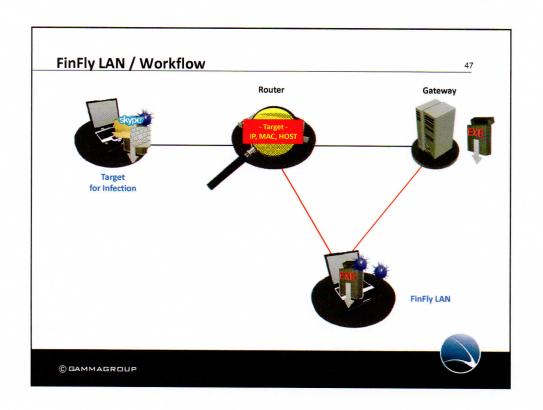
 Discovers all computer systems connected to the Local Area Network via IP-Address, MAC-Address, Host-Name and Operating System



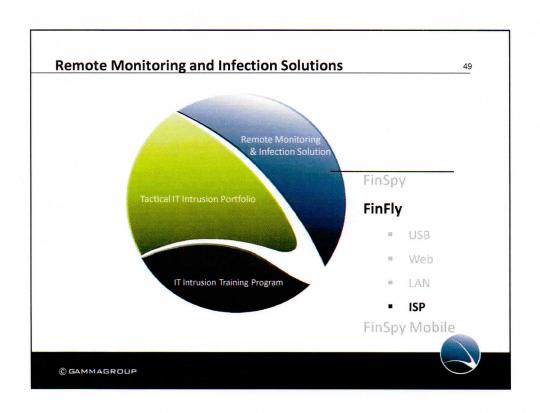
- Works in Wired and Wireless (802.11) networks
- Can be combined with FinIntrusion Kit for covert network access
- Hides Remote Monitoring Solution in **Downloads of Targets**
- Injects Remote Monitoring Solution as Software Updates
- Remotely installs Remote Monitoring Solution through
 Websites visited by the Target













FinFly ISP/ Operational Usage

50

FinFly ISP is designed to covertly inject a configurable software into remote Target Systems through ISP networks.

Typical Operations:



Deploy in Backbone of ISP:

 Install FinSpy on Target Systems by selecting their Username/RADIUS name for Infection



Install in Core of Local Area Networks:

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



© GAMMAGROUP

FinFly ISP / Core Features

51

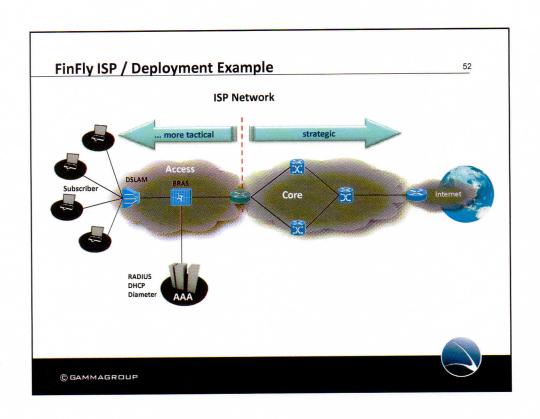
- Identify Targets by:
 - Username, Password (e.g. xDSL)
 - MAC-Addresses (Cable)
 - Dial-in phone number (ISDN, POTS)
 - IMSI, T-IMSI, MSISDN (Internet Access in Mobile Networks)

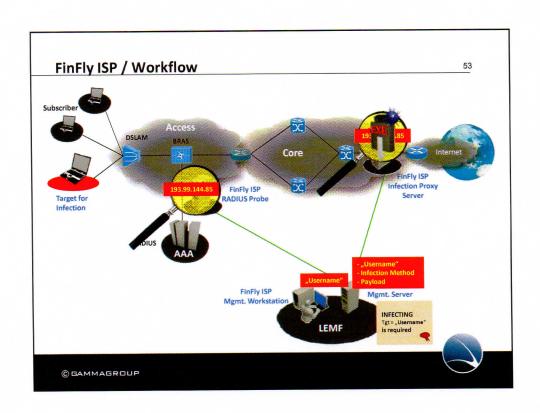


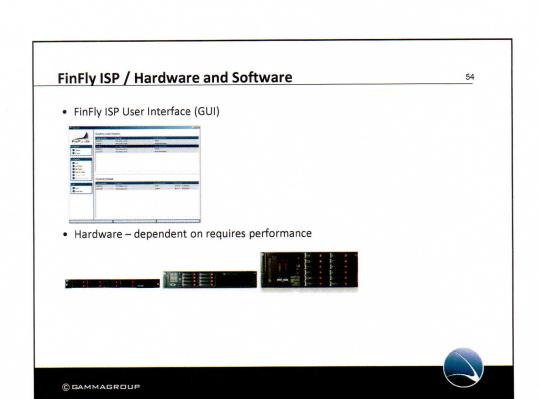
- Hides Remote Monitoring Solution in Downloads of Targets
- Injects Remote Monitoring Solution as Software Updates
- Remotely installs Remote Monitoring Solution through Websites visited by the Target

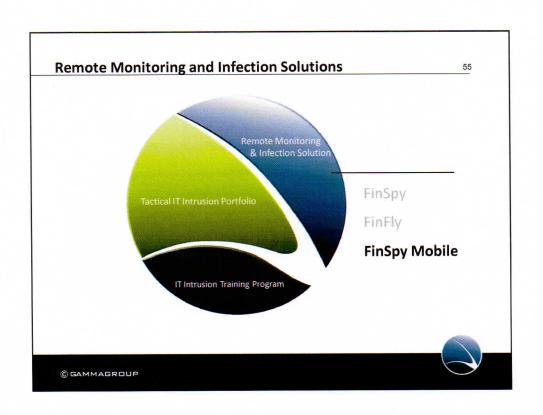












FinSpy Mobile / Operational Usage

56

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:



Monitor all Communication:

- Full access to all basic Communication like SMS/MMS, Calls, etc
- Record even encrypted Communication like BlackBerry Messenger



Live Surveillance:

- GPS Tracking of Target Phones
- Spycalls to listen Live to Phone



© GAMMAGROUP

FinSpy Mobile / Core Features

57

 The product functions on any major Operating System such as BlackBerry, iOS (iPhone), Android and Windows Mobile / Windows Phone



All communication and all temporary files are fully encrypted



• BlackBerry Messenger surveillance



• Recording of incoming and outgoing E-Mails



• Location Tracking (Cell IDs and GPS Data)

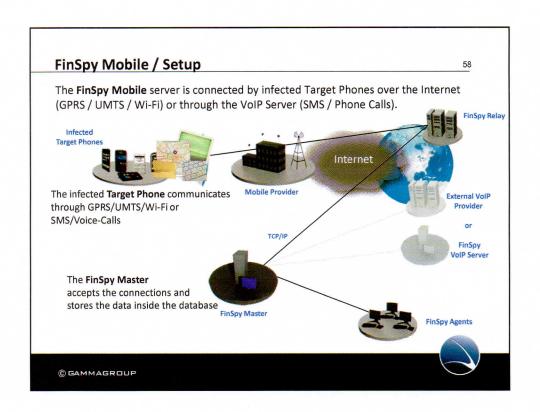
• Live Surveillance through Silent Calls

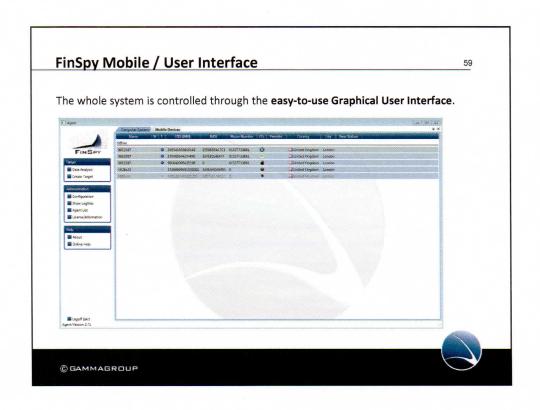


• Basic Communication Interception like Calls, SMS/MMS, Call Logs

Cuidonco







FinSpy Mobile / Infection Techniques

60

Various infection techniques exists like:

Remote Infection via Bookmark SMS to Target Phone



Provider-Supported Infection via WAP Push



• Tactical Infection via Cable or Bluetooth



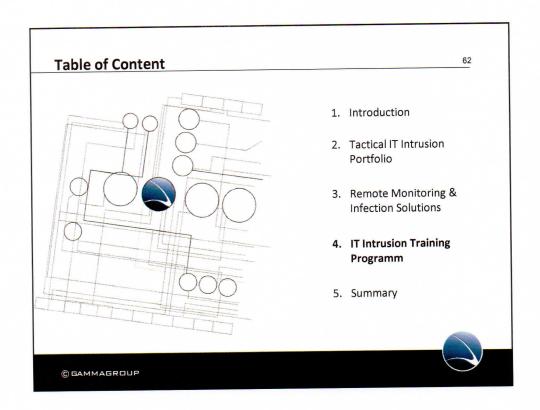
• Infection when synchronizing with infected PC (Q4 2011)



© GAMMAGROUP

• FinSpy Mobile / Strategic System • FinSpy Master and Relay • FinSpy Agent(s) • FinSpy VolP Server PRI Cards for up to 30 lines









FinTraining / Operational Usage

64

With Gamma's Team of world-leading IT Intrusion experts, a wide-range of practical IT Intrusion trainings is available.

Typical Operations:



Gain Access to Webserver:

- Remotely get access to Target Servers
- Actively Monitor foreign Targets



Perform Security Assessment:

- Evaluate Security of critical Infrastructures
- Increase Security through regular Penetration Tests



© GAMMAGROUP

FinTraining / Core Facts

6

Training Facts:

- Trainings conducted in Europe or In-Country
- Limited to 2-4 participants
- Fully practical trainings
- Techniques can immediately be used for real-life operations



Contents:

- Basic IT Intrusion Training courses for all Topics
- Most Trainings are fully customized to fulfill customer needs and requirements



FinTraining / Examples

66

Example Courses:

- Basic and Advanced IT Intrusion
- Basic and Advanced Software Exploitation
- Basic and Advanced Web Application Intrusion
- Wireless IT Intrusion (WLAN, Bluetooth, RF)

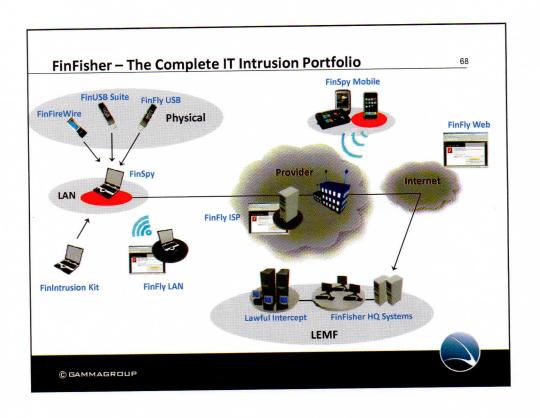
Example Topics:

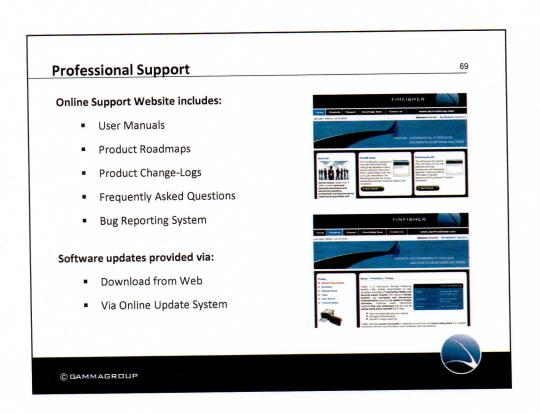
- Profiling of Target Websites, Networks and Persons
- Tracing of anonymous E-Mails
- Remote access to Webmail Accounts
- Security Assessment of Web-Servers & Web-Services
- Monitoring Hot-Spots, Internet Café's and Hotel Networks
- Intercept and Record Calls (VoIP and DECT)





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







Why Gamma as a Partner?

70

Commercial:

- Long-term, stable & strong partner
- Entirely self-financed, independent and privately-owned company
- All solutions are made in accordance to end-users requirements

Technical:

- Many years of experience on the field of Governmental IT Intrusion
- Most advanced solutions and portfolio in the market
- Existing global support infrastructure



Questions?

Thank you for your attention!



FIN FISHER

WWW.GAMMAGROUP.COM