



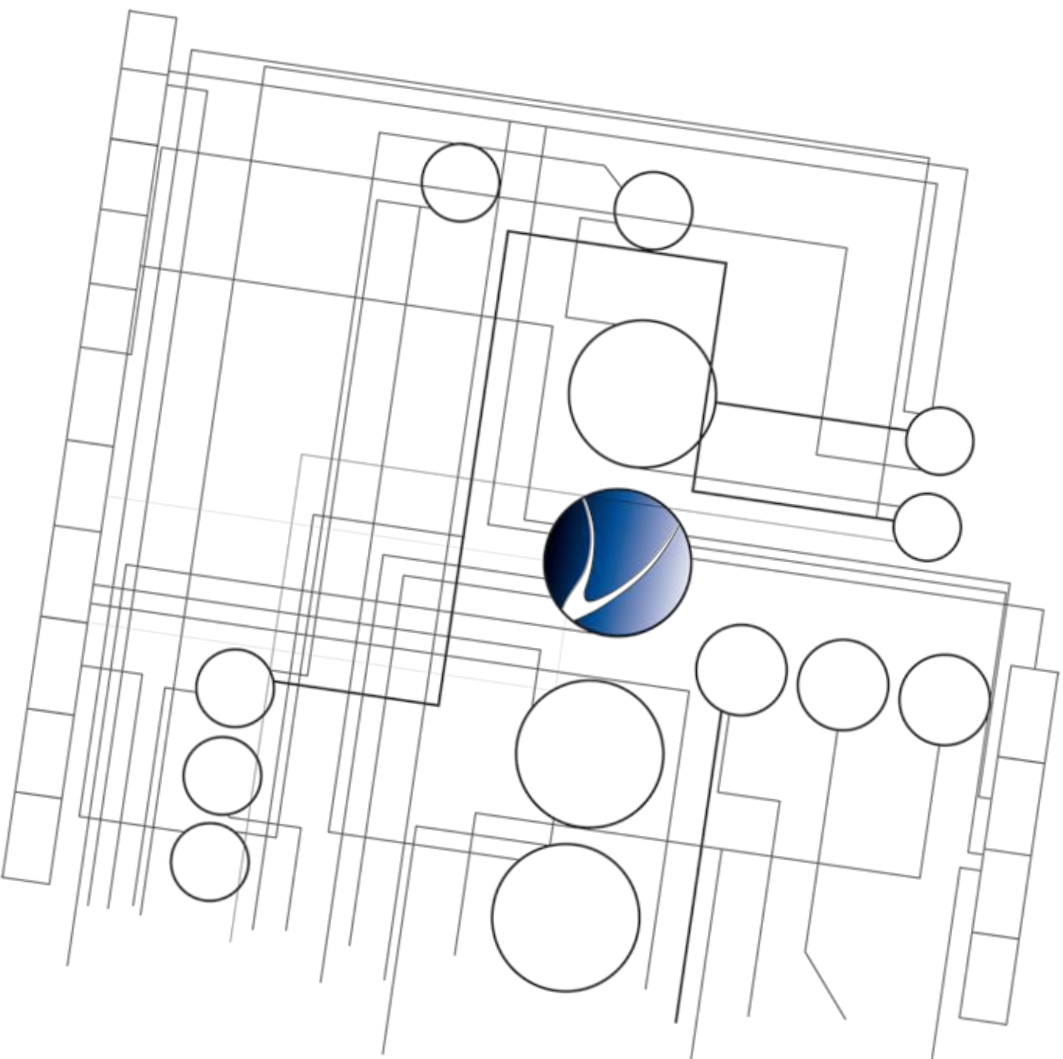
FINFISHER: IT INTRUSION SEMINAR

Uganda – 19th/20th January 2012



FINFISHER
IT INTRUSION

WWW.GAMMAGROUP.COM



Day 1:

1. Introduction: GammaGroup
2. IT Intrusion: "Hacking"
3. Example Cases
4. Intrusion Techniques

Day 2:

1. FinFisher Portfolio
2. Real-Life Operations



Gamma Group - Fields of Operation

3

Gamma TSE

- Technical Surveillance Equipment
- Surveillance Vans



G2Systems

- Intelligence Training
- VIP Protection



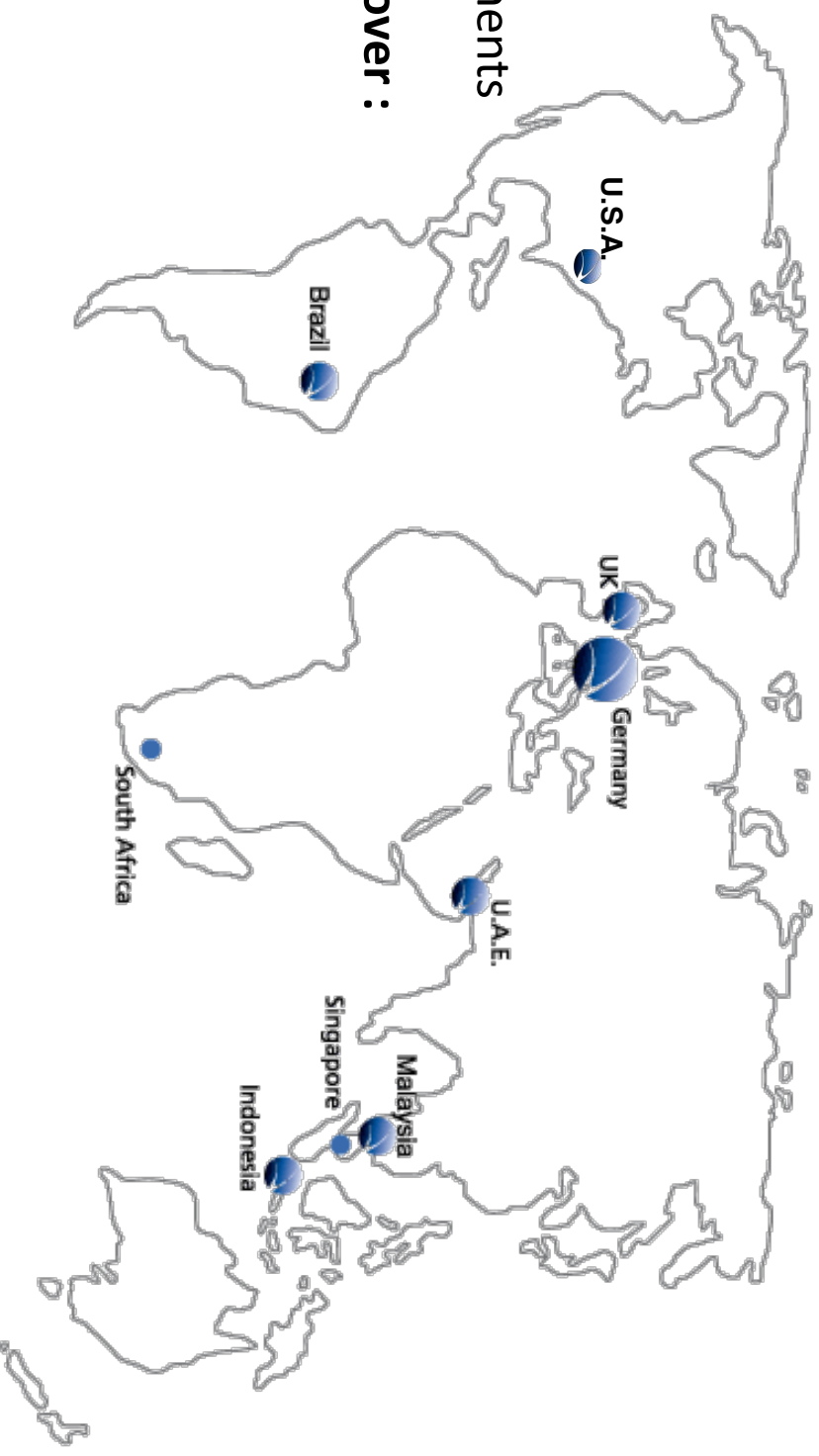
Gamma International

- FinFisher - IT Intrusion
- Communication Monitoring



Facts, Sales & Support Operation

- **Founded:**
1996
- **Office Locations:**
9 offices in 4 continents
- **Gamma Group Turnover :**
EUR 80' (in 2010)
- **Employees :**
78 Globally



Target Clients

5



- **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

Gamma International serves Governmental Customers only



History and Background of FinFisher

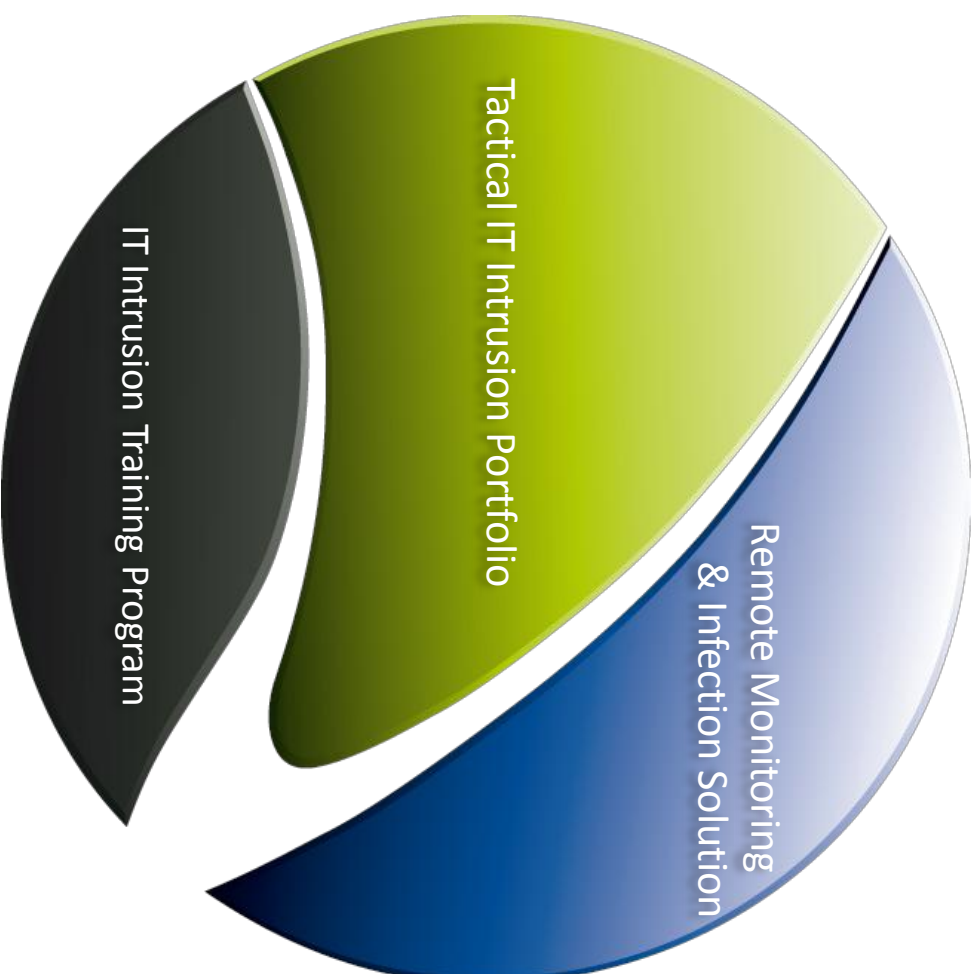
6

- 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

7



Requirement of Governmental IT Intrusion

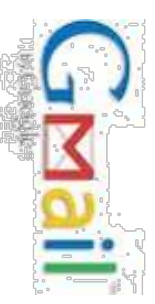
8

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 ...)
 - Data Encryption (PGP, S/MIME, ...)
 - Hard-Disk Encryption (Truecrypt, SafeGuard, ...)
 - VPN Connections
- **Global mobility** of Devices and Targets
- **Anonymity** through Hotspots, Proxies, Webmail, ...



TRUE CRYPT



Governmental IT Intrusion in the News

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

0 Germany Furious Over Chinese Spy Hackers

Georgia President's web site 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 sleuths 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 Salenji/AP

[+ Enlarge](#)

(3 of 3) [Prev](#) | [Next](#)

German Chancellor Angela Merkel and Chinese Premier Wen Jiabao du guard of honor at the Great Hall of the People in Beijing, Monday, Aug. 27, 2007...



Summary

From Russia with (political) love? appears so according to a deeper analysis of command and control servers used by attackers. During the weekend, Georgia's web site was under a distributed denial of service (DDoS) attack from Russian hackers.



Governmental IT Intrusion - Legal Situation

10

New laws are being established all around the world and Trojan-Horse technology is already legally used in many countries.

ZDNet / News / Software

Australian police get go-ahead on spyware

By M...
Leaked Documents Show German Police Attempting to Hack Skype

set 0 Like

FBI uses hacking technology for surveillance

By Staff, CNet, 22 November, 2001 11:50

Topics

Hacking, trojan horse, Surveillance, FBI, Tools, keystrokes, Viruses

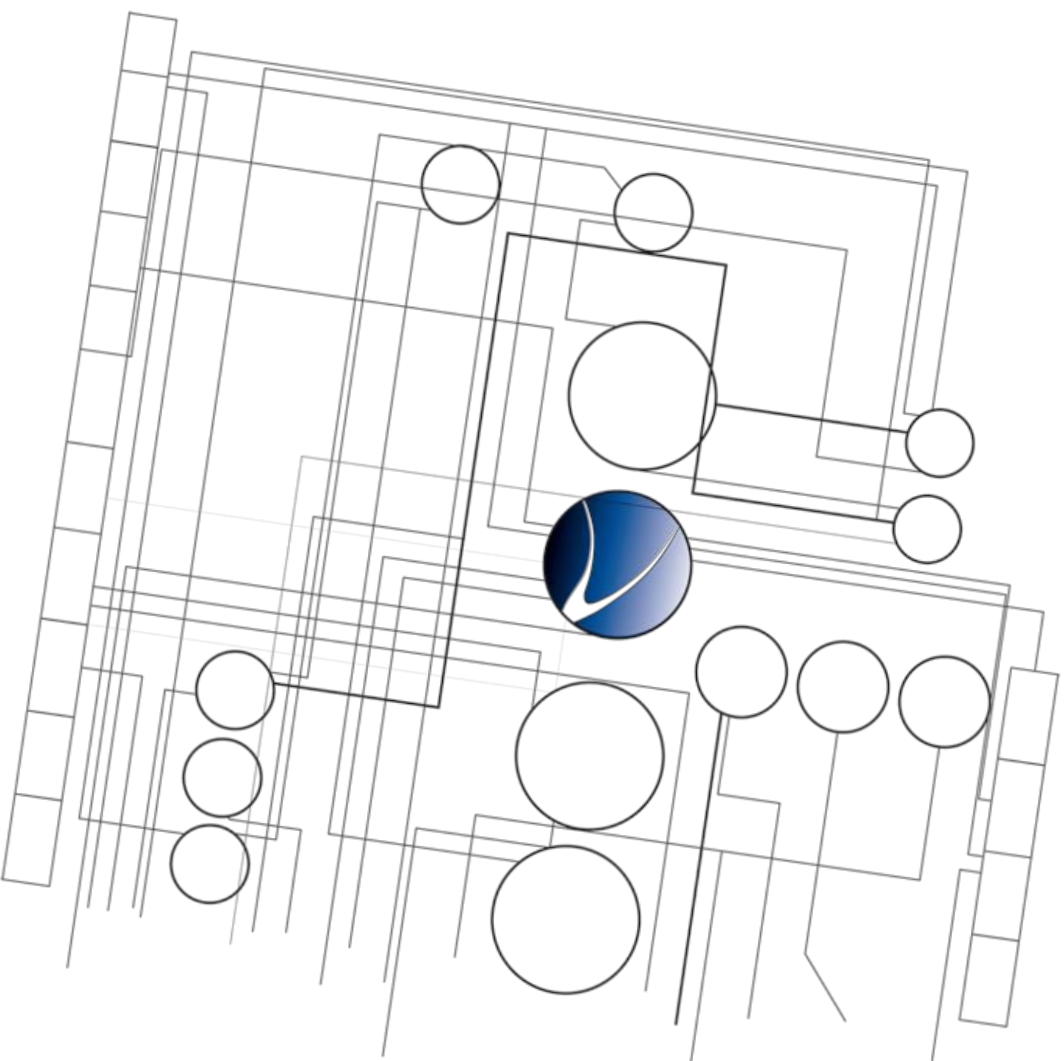
NEWS A new tool reportedly being developed by law enforcement agencies to remotely install surveillance programs on a suspect's computer is little more than three-year-old hacking technology, security experts said on Wednesday.

On Tuesday, MSNBC reported that the FBI was working on a computer "virus" to install key-logging programs and other surveillance software onto a suspect's computer.



Table of Content

11



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



Typical Operations:



Search Engines:

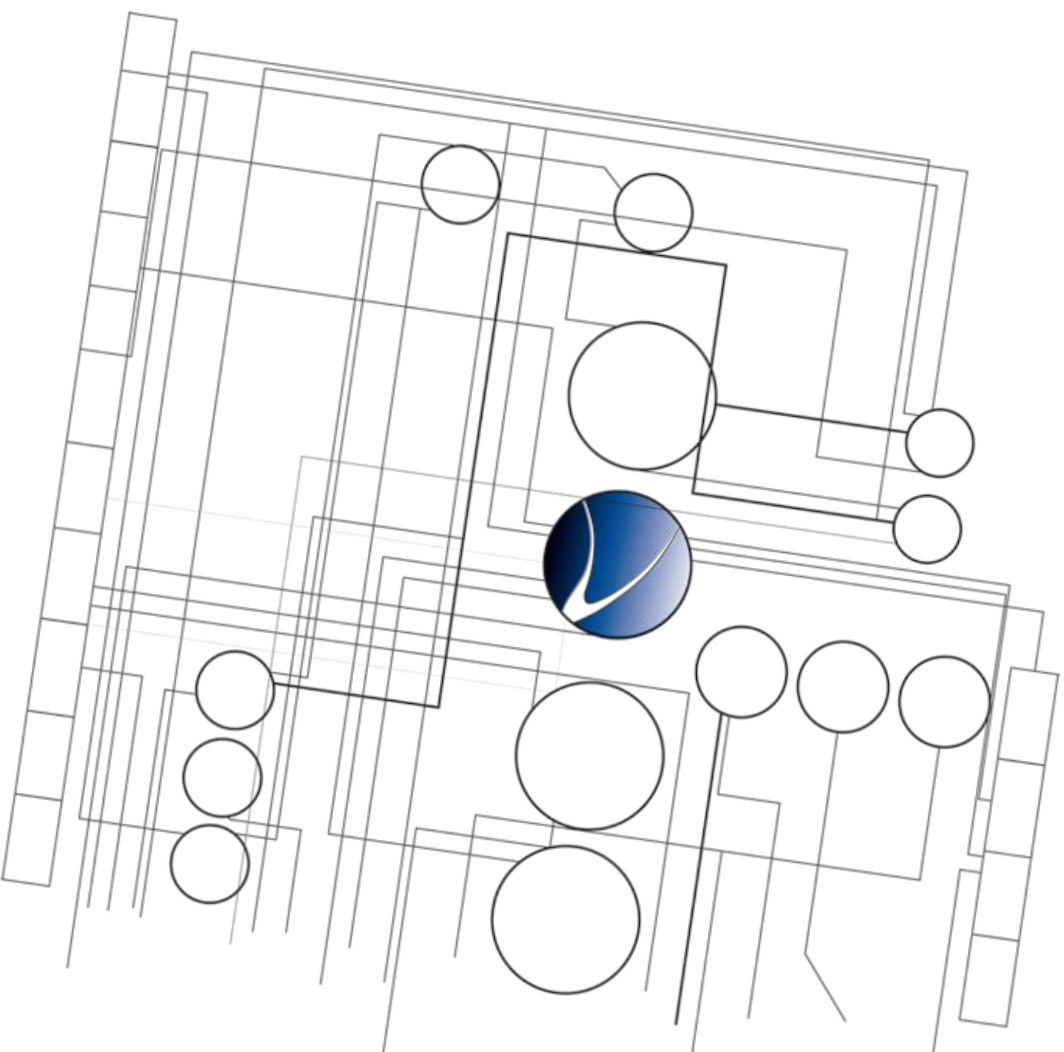
- Crawls public websites and archives
- Provides important intelligence for most operations
- **Demo: Maltego**



Social Networks:

- Link Analysis: See all friends, job history, interests, etc
- See current activities
- Extract GPS Information from Photos
- **Demo: Geotag Photos**





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

Tactical Operations / USB Forensics

14

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



Typical Operations:



Wireless Networks:

- Break Encryption and record all Traffic
- Provide Fake Access-Point
- Demo: WEP/WPA Crack and FakeAP



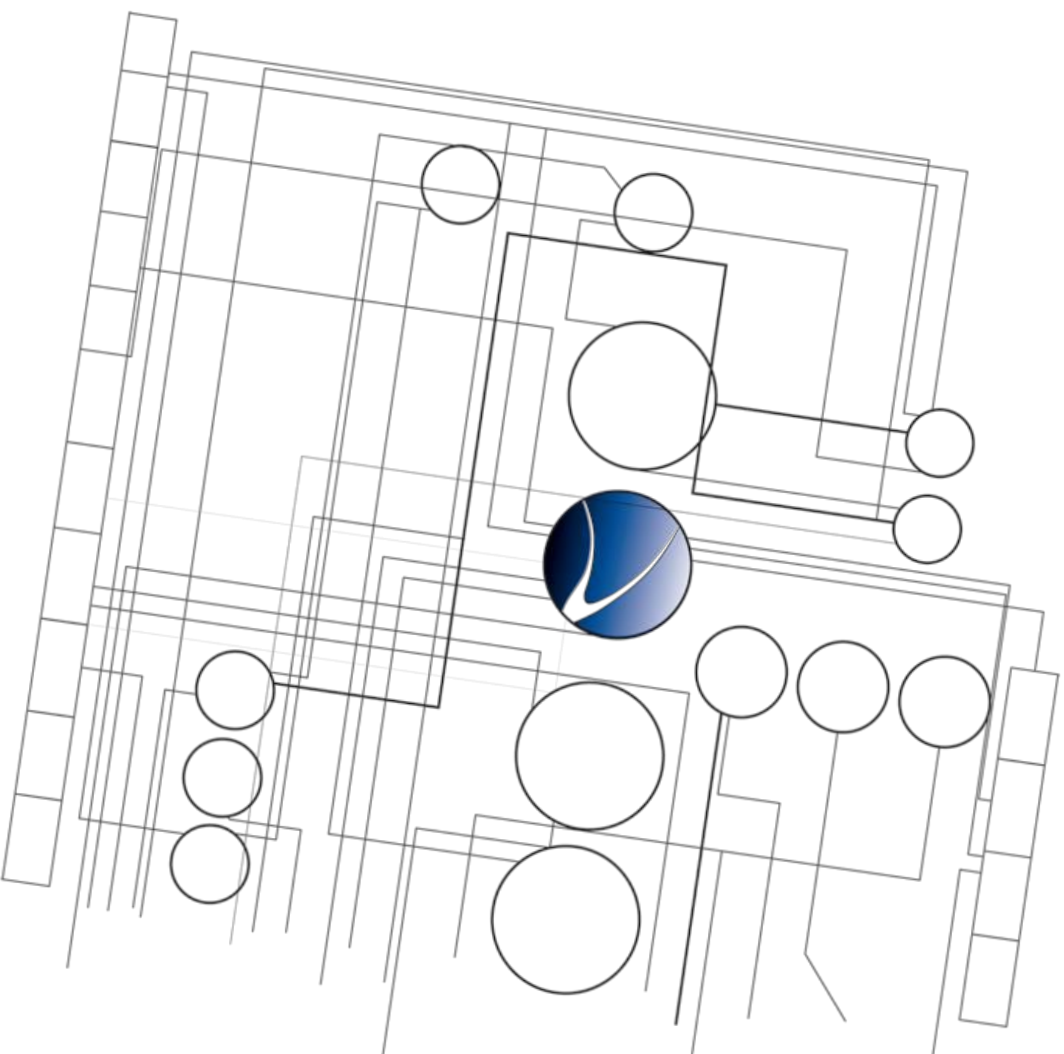
Monitor LAN Systems:

- Record Usernames and Passwords
- Access systems with enabled shares
- Demo: MITM and SMB shares



Table of Content

16



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



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)**



Typical Operations:



Server Profiling:

- Get Information about Servers
- See old versions of websites



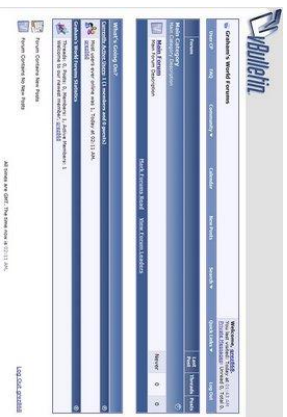
Former Defacements:

- See whether server has been compromised before
- Retrieve name of former attackers
- Demo: Defacement Archive



Server Intrusion / Exploits

Typical Operations:



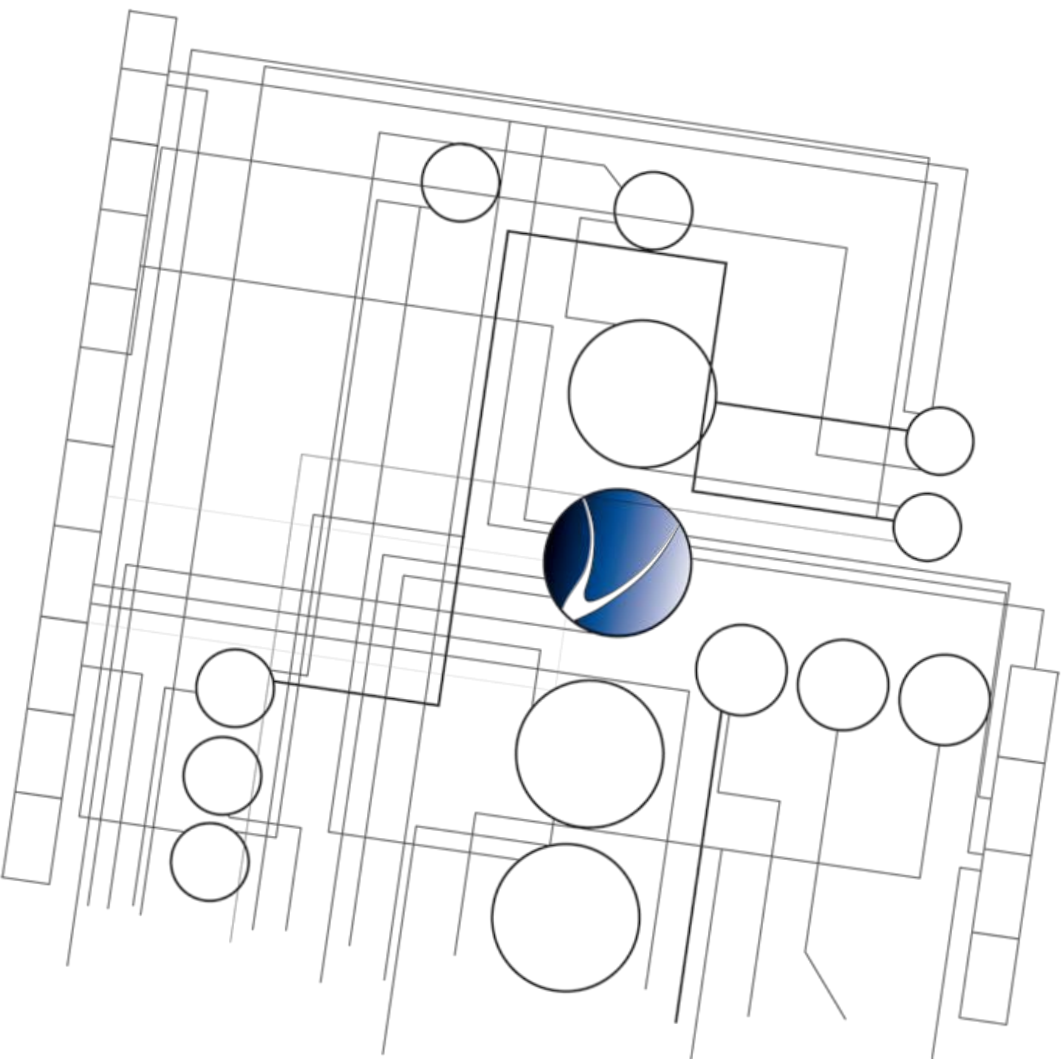
Web Applications:

- Access server through vulnerabilities in web application
- Variety of bugs, e.g. SQL Injection, XSS, File-Inclusion
- **Demo: Web Application Hacking**

Server Software:

- Use vulnerabilities in Server software
- Few bugs but very powerful

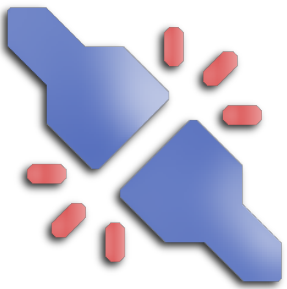




1. Introduction
2. Human Intelligence
3. Tactical Operations
4. Client/Server Intrusion
5. **Denial of Service**
6. Conclusion



Typical Operations:



Client Jammer:

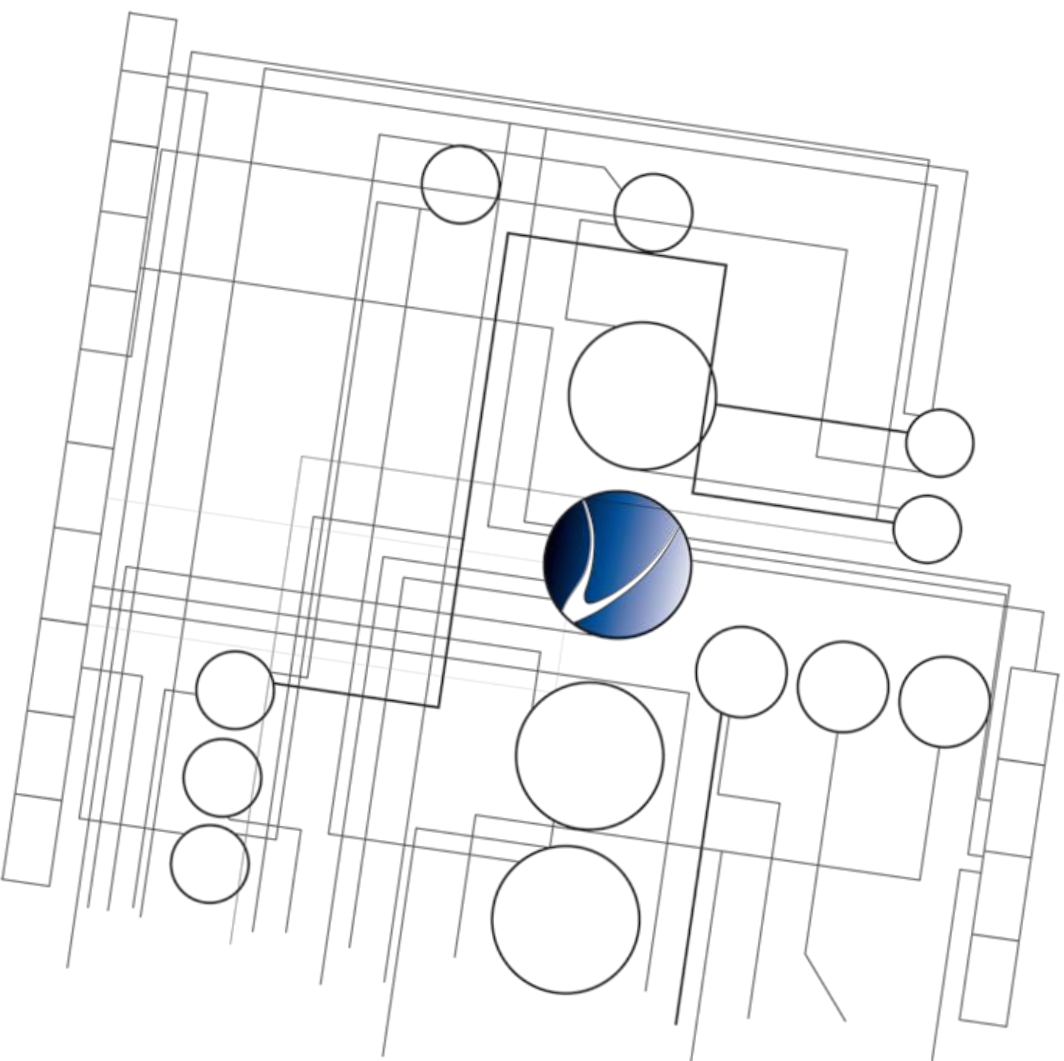
- Jam dedicated computers on Local Area Networks
- Jam dedicated computers on the internet
- **Demo: Jam Client**



Distributed Denial of Service:

- Jam complete infrastructures
- Simple to use software with massive effect





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



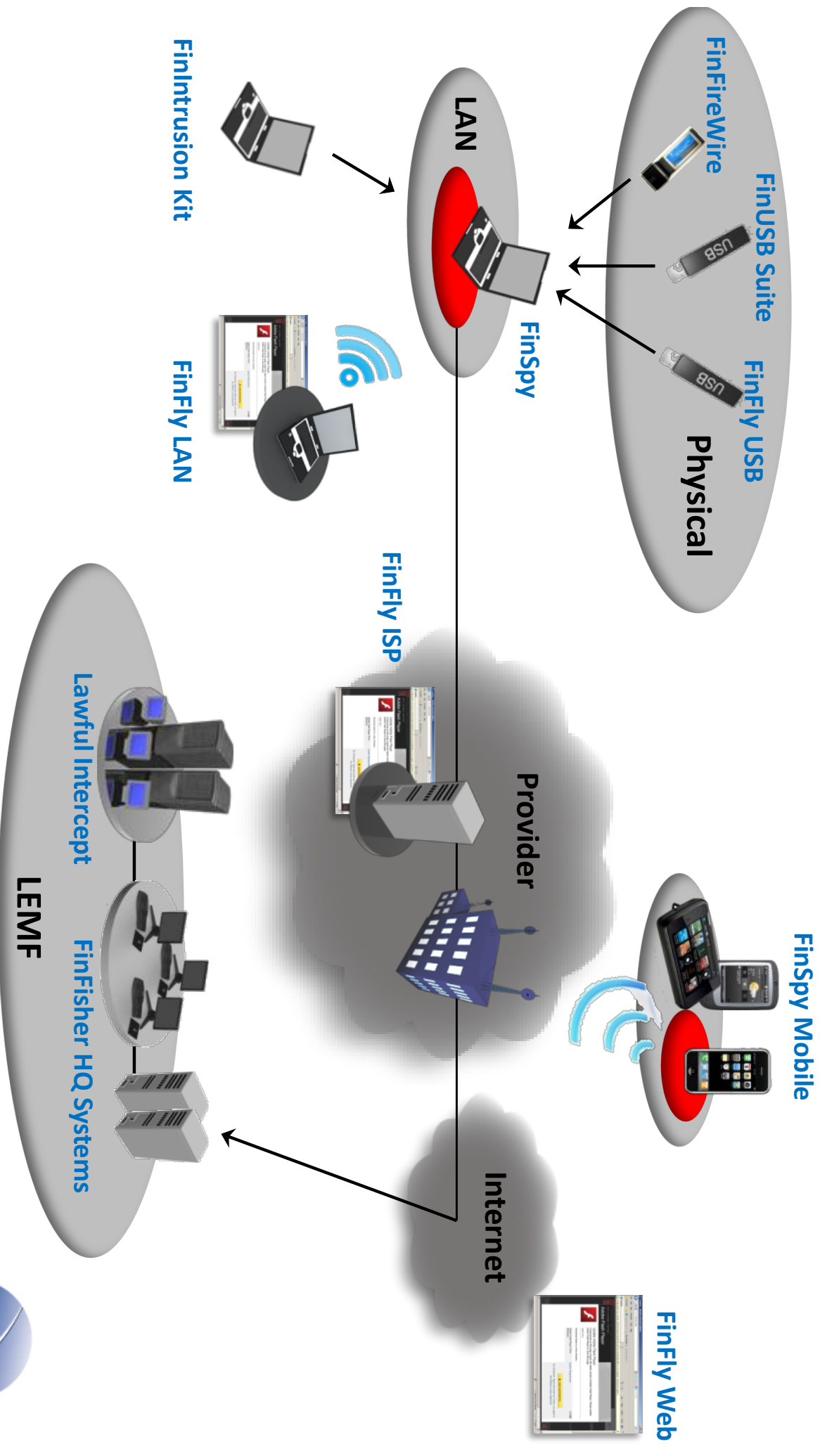
Conclusion

23

- 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



FinFisher – The Complete IT Intrusion Portfolio



Questions?

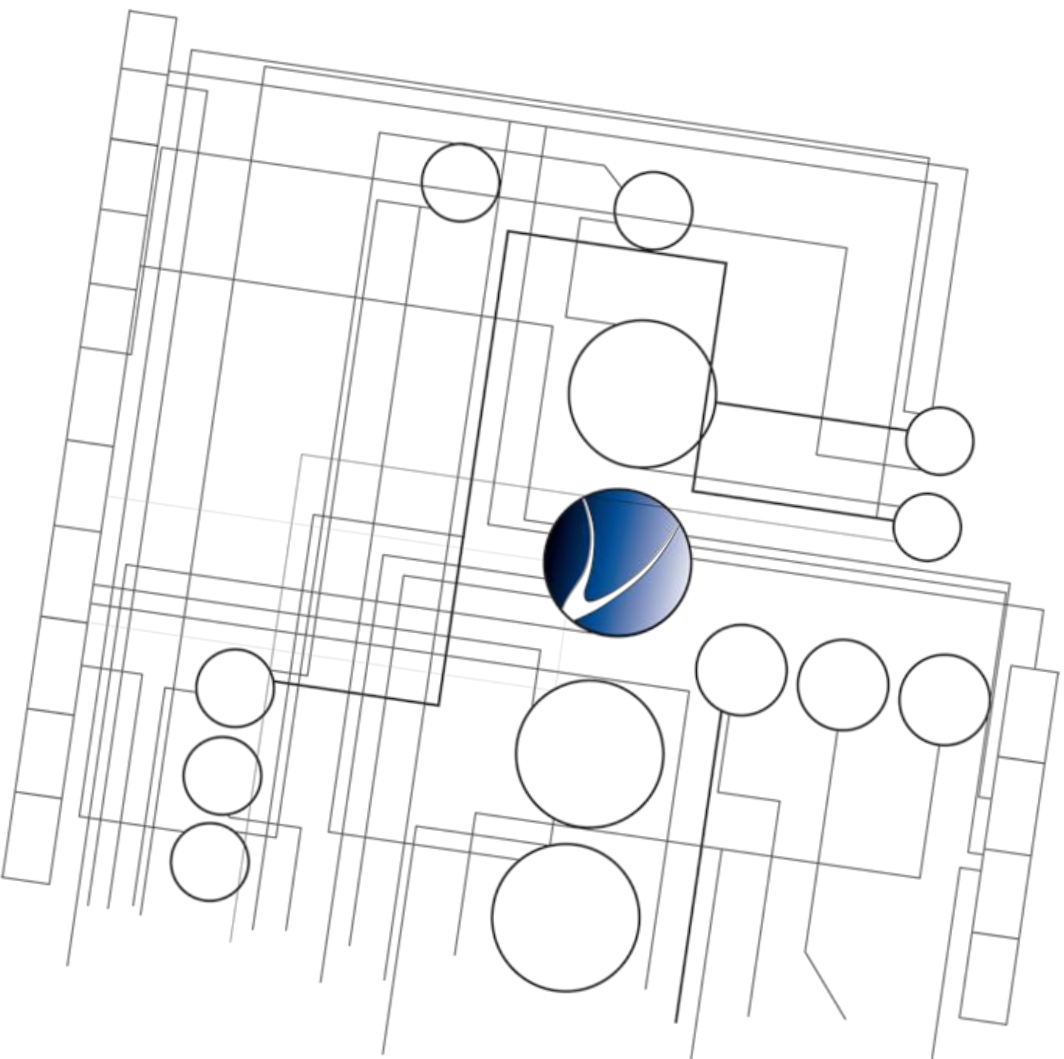
End of Day 1.

Thank you for your attention!



FINFISHER
IT INTRUSION

WWW.GAMMAGROUP.COM



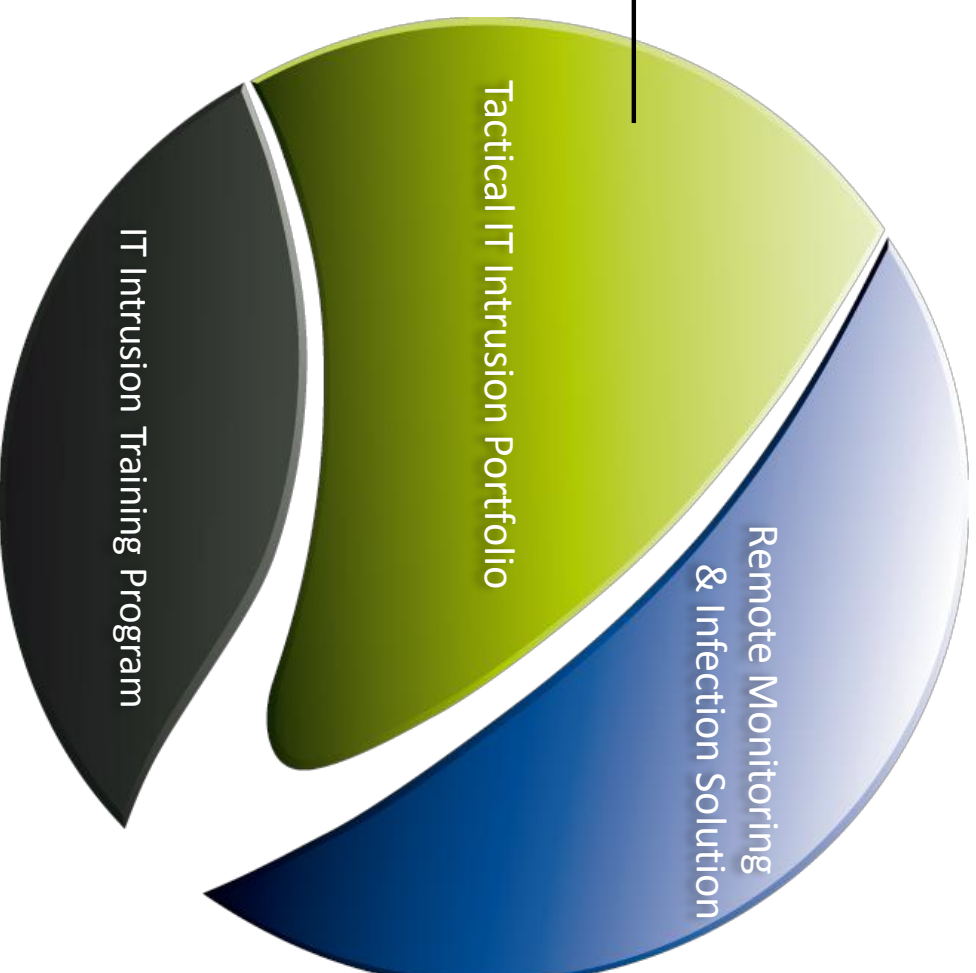
Day 2:

1. FinFisher Portfolio

- **Product Range**
- **Training Courses**
- **Support**

2. Real-Life Operations

Tactical IT Intrusion Portfolio



FinUSB Suite

FinIntrusion Kit

FinFireWire



FinUSB Suite / Operational Usage

28

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



- Extraction of **Username**s and **Password**s for all common software like:
 - E-Mail Clients 
 - Messengers   
 - Browsers    
- **Silent Copying of Files** (Search Disks, Recycle-Bin, Last Opened)  
- Extracting **Network Information** (Chat Logs, Browsing History, WEP/WPA(2) Keys, Cookies, ...) 
- Compilation of **System Information** (Running/Installed Software, Hard-Disk Information, ...) 



FinUSB Suite / Headquarter Software

The FinUSB HQ provides target-specific configurations and professional data analysis.

The screenshot displays the 'FinUSB HQ' interface. At the top, there is a 'Data Analysis' section with a table containing columns for ID, Date, User, and System. Below the table are buttons for 'Import Data', 'View Data', and 'Delete Data'. To the left, there are sections for 'Preferences' (Updates, License, Language), 'Configuration' (Dongle Settings, Update Dongle, Delete Dongle Data, Generate Certificates), and 'Help' (About, Online Help). A 'Welcome to FinUSB Suite' message is visible at the bottom left.

ID	Date	User	System
F602356	Mon, 25 Apr 2011 17:52:16 GMT	Test	TEST-PC
F602132	Mon, 25 Apr 2011 17:50:42 GMT	W7-test-Admin	W7-CLEAN:X64
F602116	Mon, 25 Apr 2011 17:50:42 GMT	W7-test-Admin	W7-CLEAN:X64
F603284	Thu, 21 Apr 2011 02:27:26 GMT	Gamma User	WIN-AJGQMAOQS4
F603284	Thu, 21 Apr 2011 02:27:26 GMT	Gamma User	WIN-AJGQMAOQS4
F603888	Thu, 21 Apr 2011 02:27:26 GMT	Gamma User	WIN-AJGQMAOQS4
F603888	Thu, 21 Apr 2011 02:27:26 GMT	Gamma User	WIN-AJGQMAOQS4
F602796	Thu, 21 Apr 2011 02:27:26 GMT	Gamma User	WIN-AJGQMAOQS4
F602796	Thu, 21 Apr 2011 02:27:26 GMT	Gamma User	WIN-AJGQMAOQS4

This block shows a series of overlapping screenshots of the software's configuration interface. The windows display various settings such as 'System Settings', 'Network Settings', 'Security Settings', and 'Advanced Settings'. Each window has a title bar and standard window controls (minimize, maximize, close). The screenshots illustrate the depth of configuration options available in the software.



FinUSB Suite / Professional Reports

Sample report generated by the *FinUSB HQ* software:



FinUSB Suite: Report

I. Generic

Generic Information

II. Passwords

- Windows Account Hashes
- E-Mail Accounts
- Messenger Accounts
- Google/Chrome Passwords
- Firefox Passwords
- Network Passwords
- Protected Storage
- Internet Explorer Accounts

III. System

- Windows Product Keys
- Windows Updates
- LSA Secrets
- Current Processes

IV. Network

- Network Adapters
- Network Ports
- Internet Explorer History
- Mozilla Firefox History
- Wireless Keys
- Mozilla Firefox Cookies

Generic Information

Generic Information

Date	Computer	Username	Language
Mon Sep 01 21:43:27 2008	XPSP2-F4115D11B	eddqa	English_United States 1252

Windows Account Hashes

Username	LM Hash	MD4 Hash
Administrator	aad3b435b51404eeaad3b435b51404ee	31d6cf4e0d16aa931b73c349f7e0086d
eddqa	012c0a4b0c7bce929aa43b435b51404ee	0d6694e805f797b2a82d07970d9937
Guest	aa83b435b51404eeaad3b435b51404ee	31d6cf4e0d16aa931b73c349f7e0086d
HelpAssistant	25f2930461c0b0b855032e96490728	12f7f0589a87310d879a58a39a306c93
SUPPORT_388945d0	aa83b435b51404eeaad3b435b51404ee	94e609322d28ce411c70b59d4300b4f2a

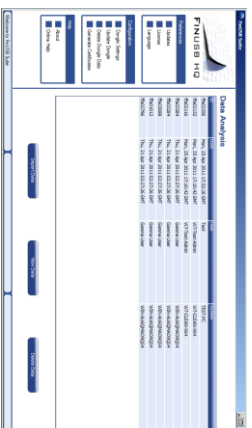
E-Mail Accounts

Name	Application	Email	Server	Type	User	Password	Profile
max merk	MS Outlook	f-q@gmx.de	pop.gmx.net	POP3	f-q@gmx.de	Mo-14.07	
max merk	MS Outlook	f-q@gmx.de	mail.gmx.net	SMTP			
max merk	MS Outlook 2002/2003/2007	f-q@gmx.de	pop.gmx.net	POP3	f-q@gmx.de	Mo-14.07	Microsoft Outlook Internet Settings
max merk	Thunderbird	f-q@gmx.de	pop.gmx.net	POP3	f-q@gmx.de		
f-q@	Hotmail/MSN	f-q@live.de		HTTP	f-q@	Mo-14.07	



FinUSB Suite / Portable Unit

- Notebook (Windows 7, FinUSB HQ)



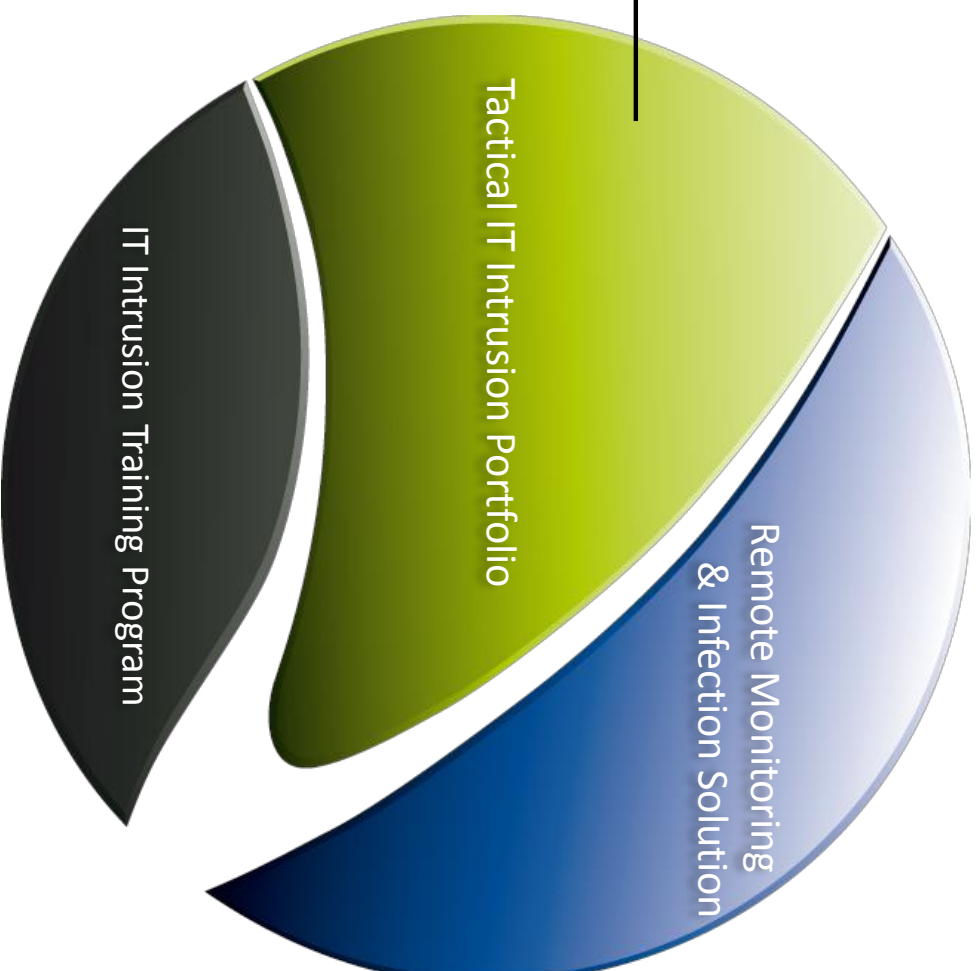
- 10 FinUSB Dongles



- 2 Bootable CD-Roms



Tactical IT Intrusion Portfolio



FinUSB Suite

FinIntrusion Kit

FinFireWire



FinIntrusion Kit / Operational Usage

34

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



FinIntrusion Kit / Core Features

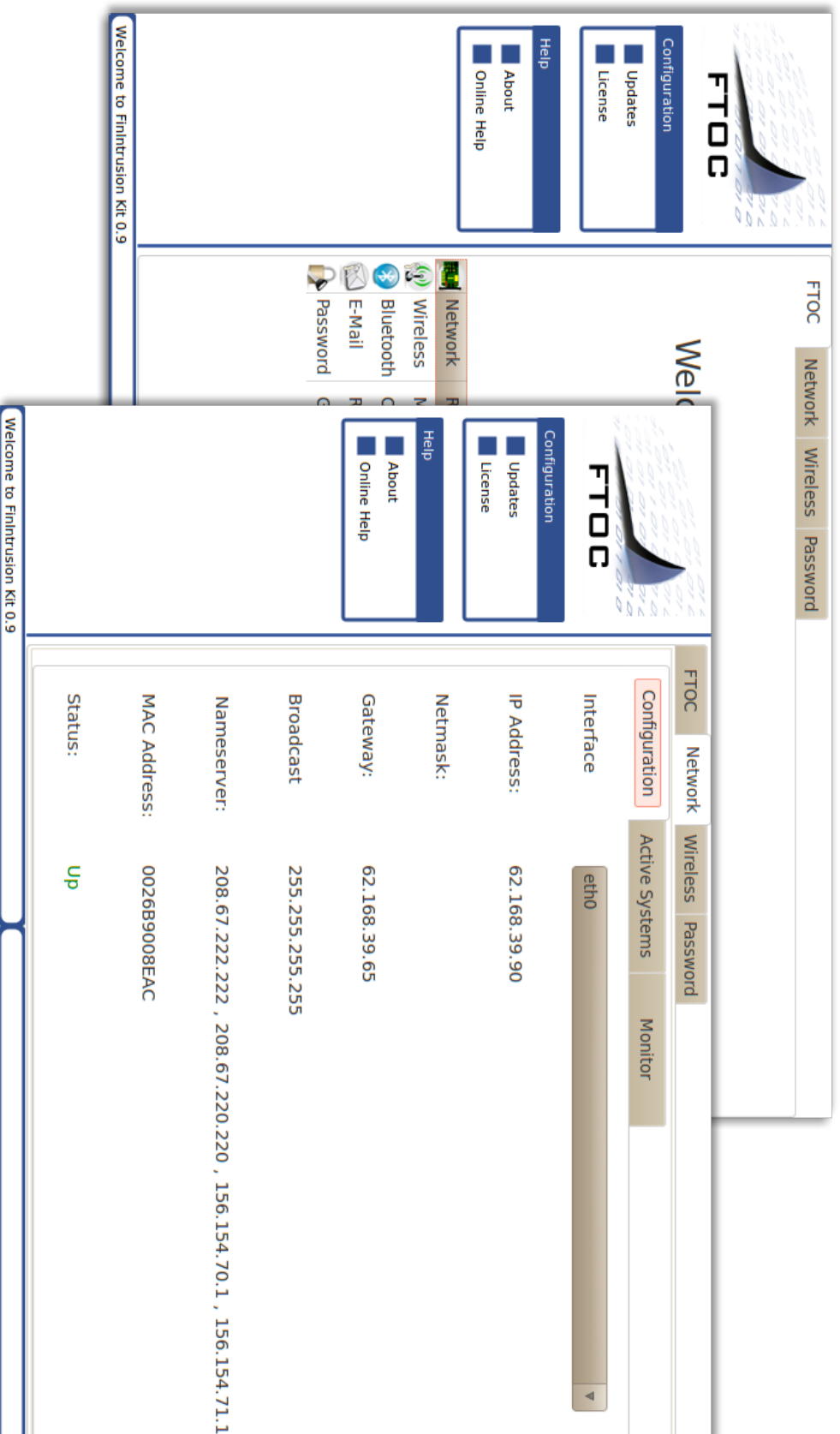
35

- 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



FinIntrusion Kit / Operation Center

The Operation Center provides easy-to-use **point-and-click attacks**.



FinIntrusion Kit / Covert Tactical Unit

- Notebook (FinTrack, FTOC)



- Autorun and bootable USB Device



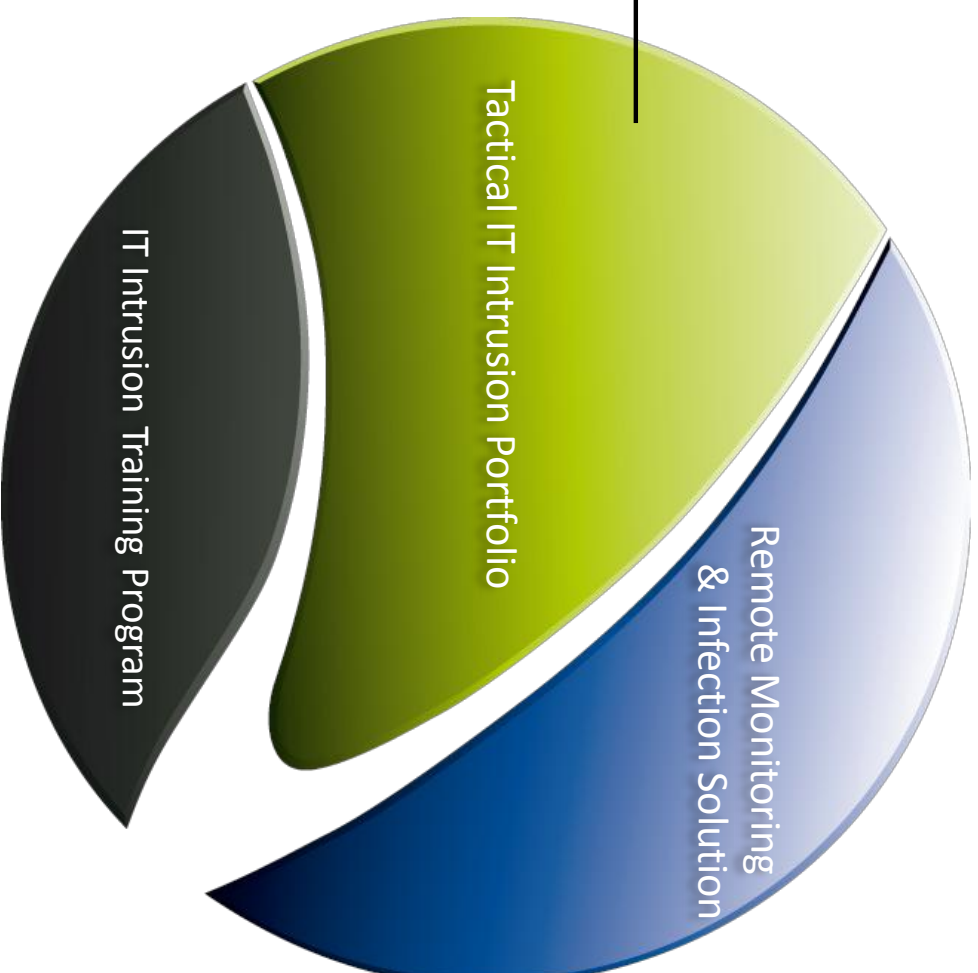
- FinTrack bootable CD-Rom



- Wireless Intrusion Hardware



Tactical IT Intrusion Portfolio



FinUSB Suite

FinIntrusion Kit

FinFireWire



FinFireWire / Operational Usage

39

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



- 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 losing 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**



FinFireWire / User Interface

Once connected to the Target System, the software provides a **easy-to-use point-and-click Interface**.



FinFireWire / Portable Unit

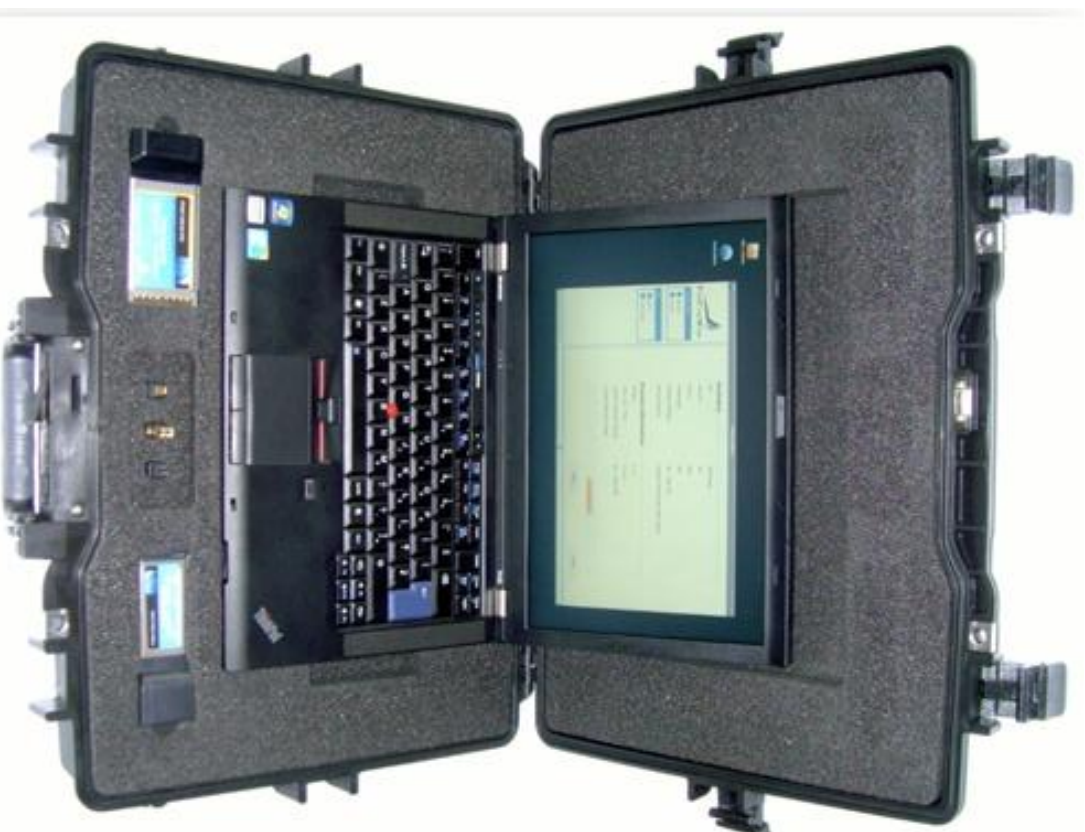
- FinFireWire Software

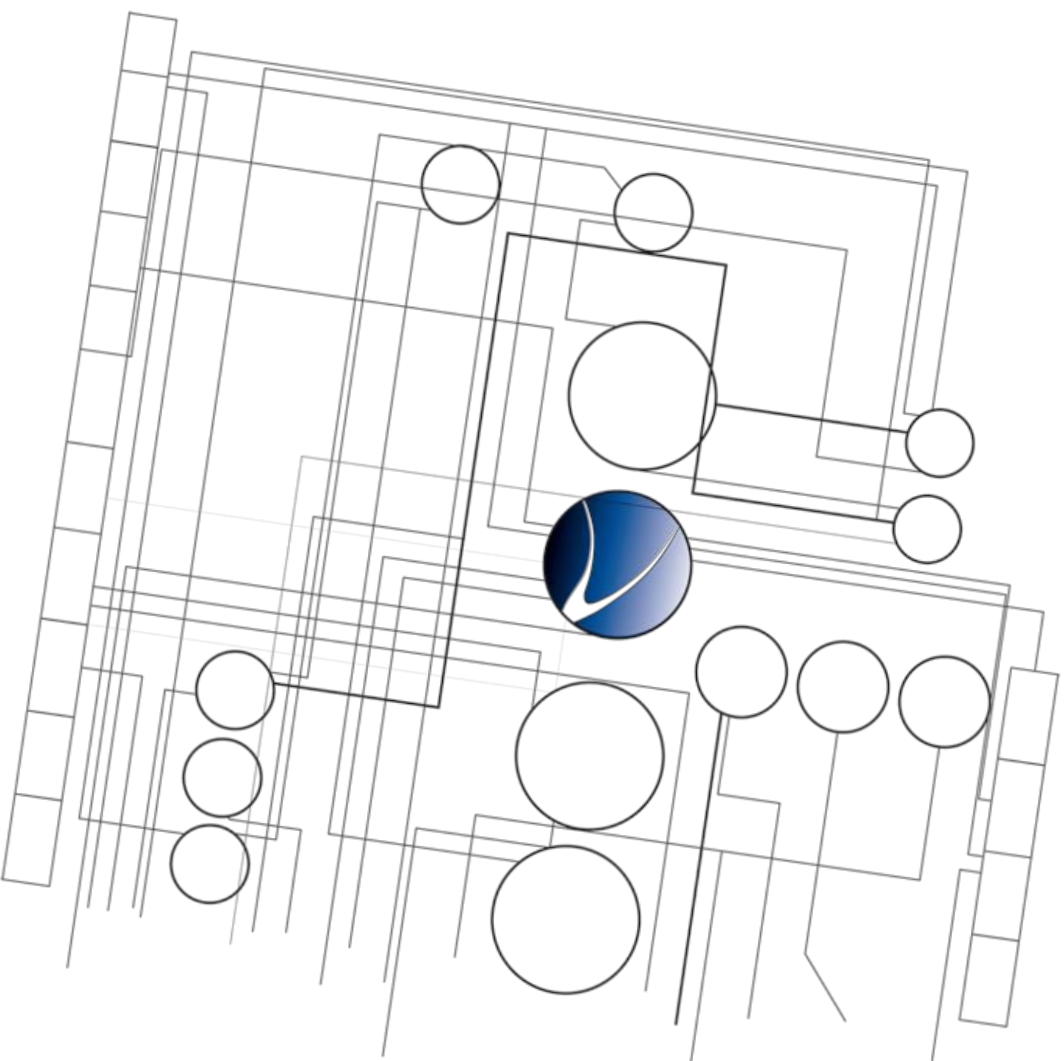


- FireWire Cables for all Ports



- PCMCIA / Express Card Adapters

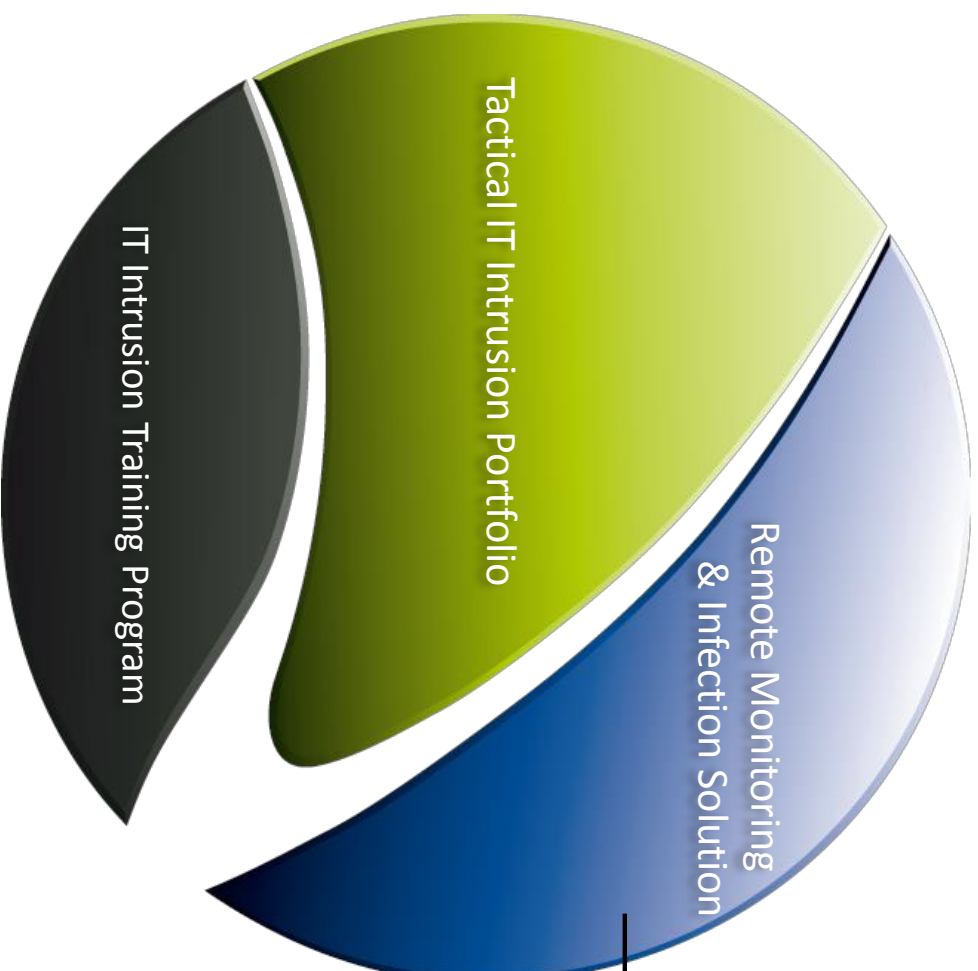




1. Introduction
2. Tactical IT Intrusion Portfolio
3. **Remote Monitoring & Infection Solutions**
4. IT Intrusion Training Programm
5. Summary



Remote Monitoring and Infection Solutions



FinSpy

FinFly

FinSpy Mobile



FinSpy / Operational Usage

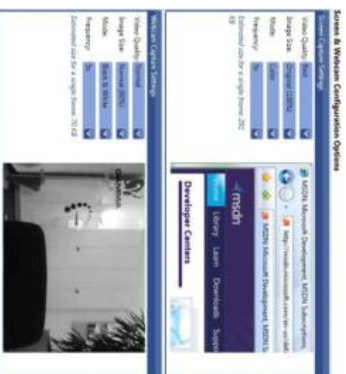
FinSpy is an advanced Intrusion system which once implemented into a Target System guarantees full access to the system with advanced features.

Typical Operations:



Monitor Encrypted Communication:

- 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

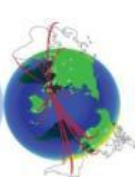
- The product functions on any major Operating System such as **Microsoft Windows (2000 -> 7), Mac OSX and Linux**
- All communication and all temporary files are **fully encrypted**
- Target software is regularly tested to **bypass the world's top 40 Anti-Virus applications and hide deep inside the 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**



FinSpy / Target Features

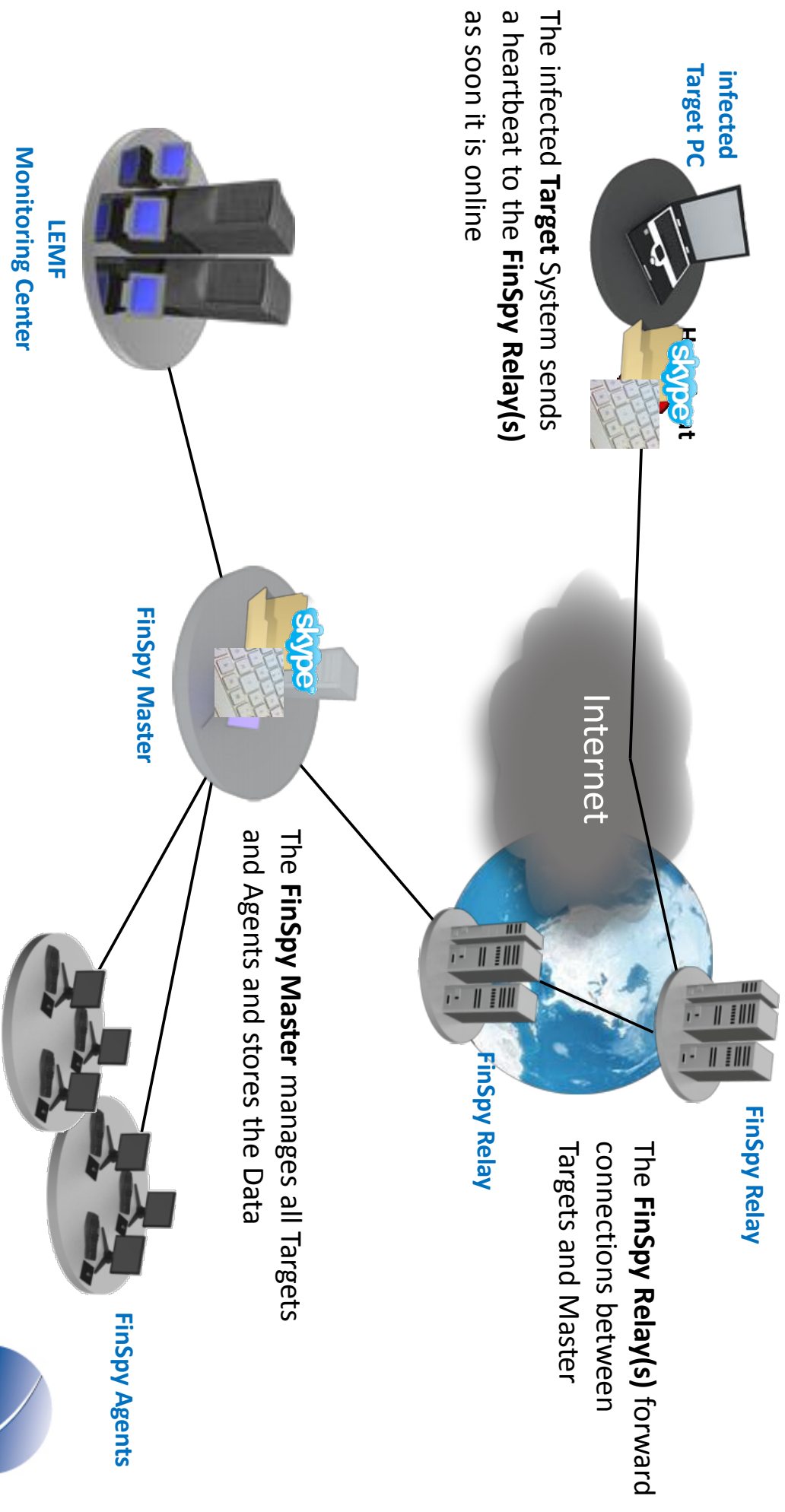
47

- Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)
- Recording of all **VoIP communication**
- **Live Surveillance** through Webcam and Microphone
- **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



FinSpy / Network Layout

With the **FinSpy Master LEMF** Interface the tactical solution can be fully integrated into the Law Enforcement Monitoring Functionality (LEMF)



FinSpy / User Interface

The whole system is controlled through the **easy-to-use Graphical User Interface**.



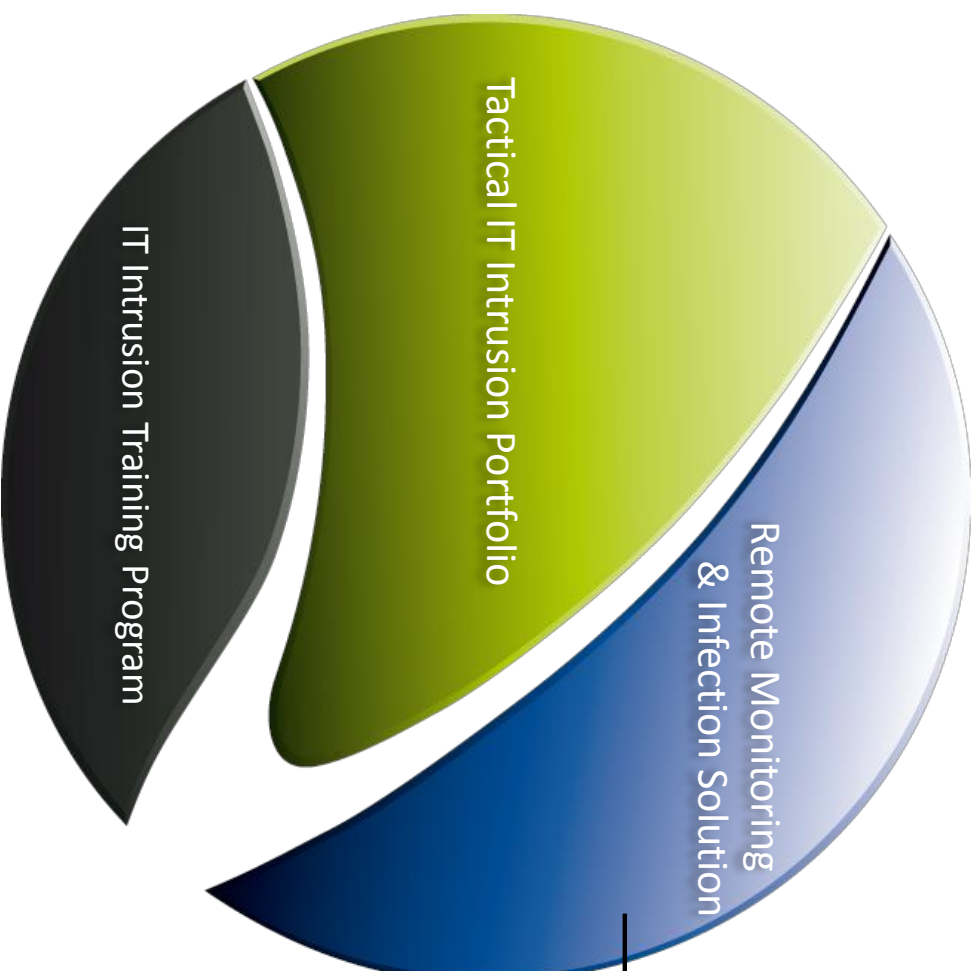
FinSpy / Strategic System

- FinSpy Master and Relay



- FinSpy Agent(s)





FinSpy

FinFly

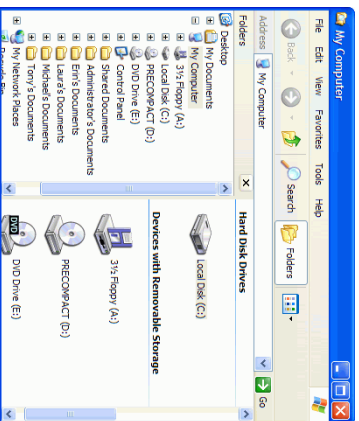
- **USB**
- Web
- LAN
- ISP

FinSpy Mobile



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



- 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

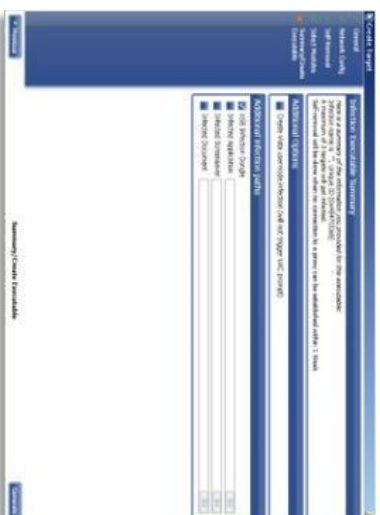


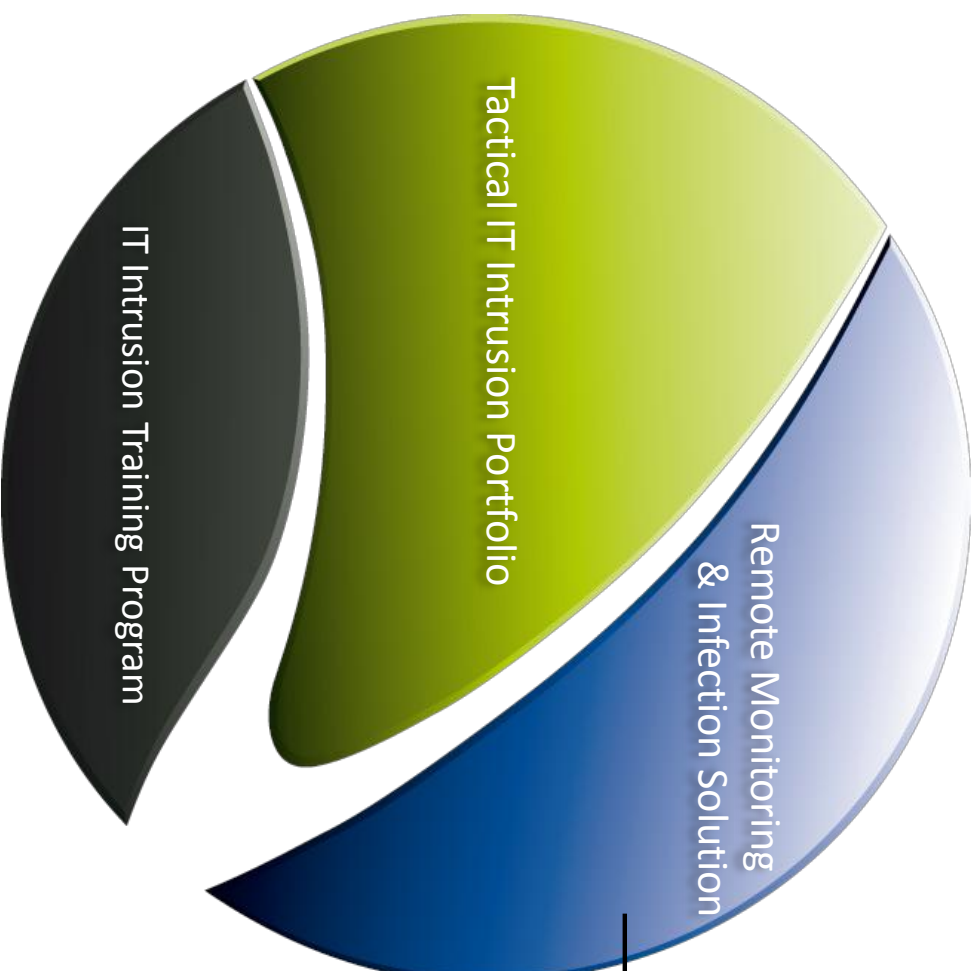
FinFly USB / Hard- and Software

- 5 FinFly USB Dongles



- Full Integration into FinSpy





FinSpy

FinFly

- USB
- **Web**
- LAN
- ISP

FinSpy Mobile

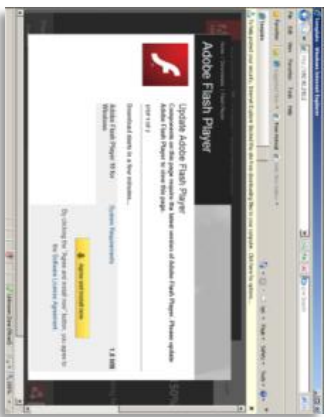


FinFly Web is designed to covertly inject a configurable software into remote Target Systems through integration in Websites.

Typical Operations:

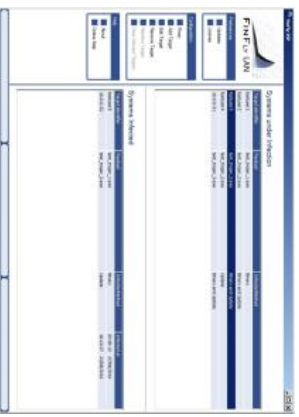
Deploy FinSpy through custom Homepages:

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



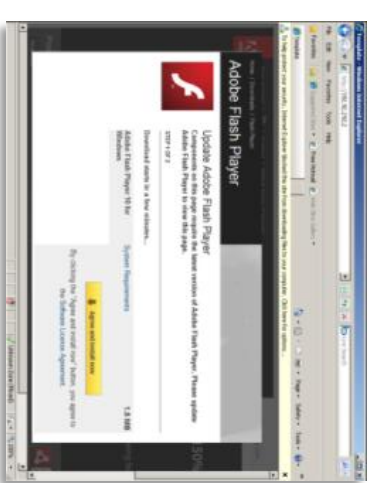
Create FinFly LAN/FinFly ISP Module

- Create Infection Module for Integration into FinFly LAN and FinFly ISP

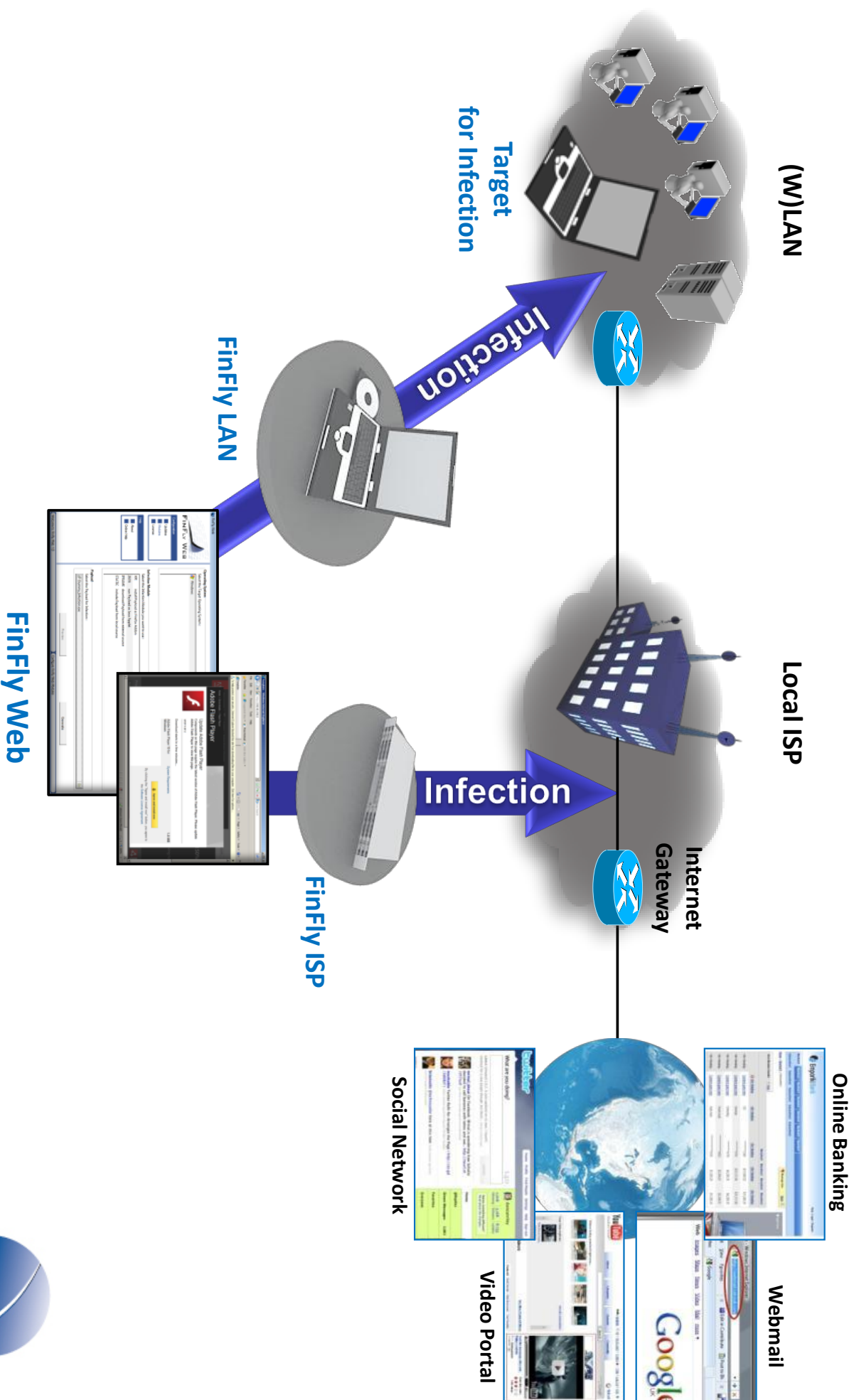


FinFly Web / Core Features

- **All common Browsers** are supported
- **Various Modules** are available for Infection
- 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 even into popular sites** like GMail, YouTube, etc.

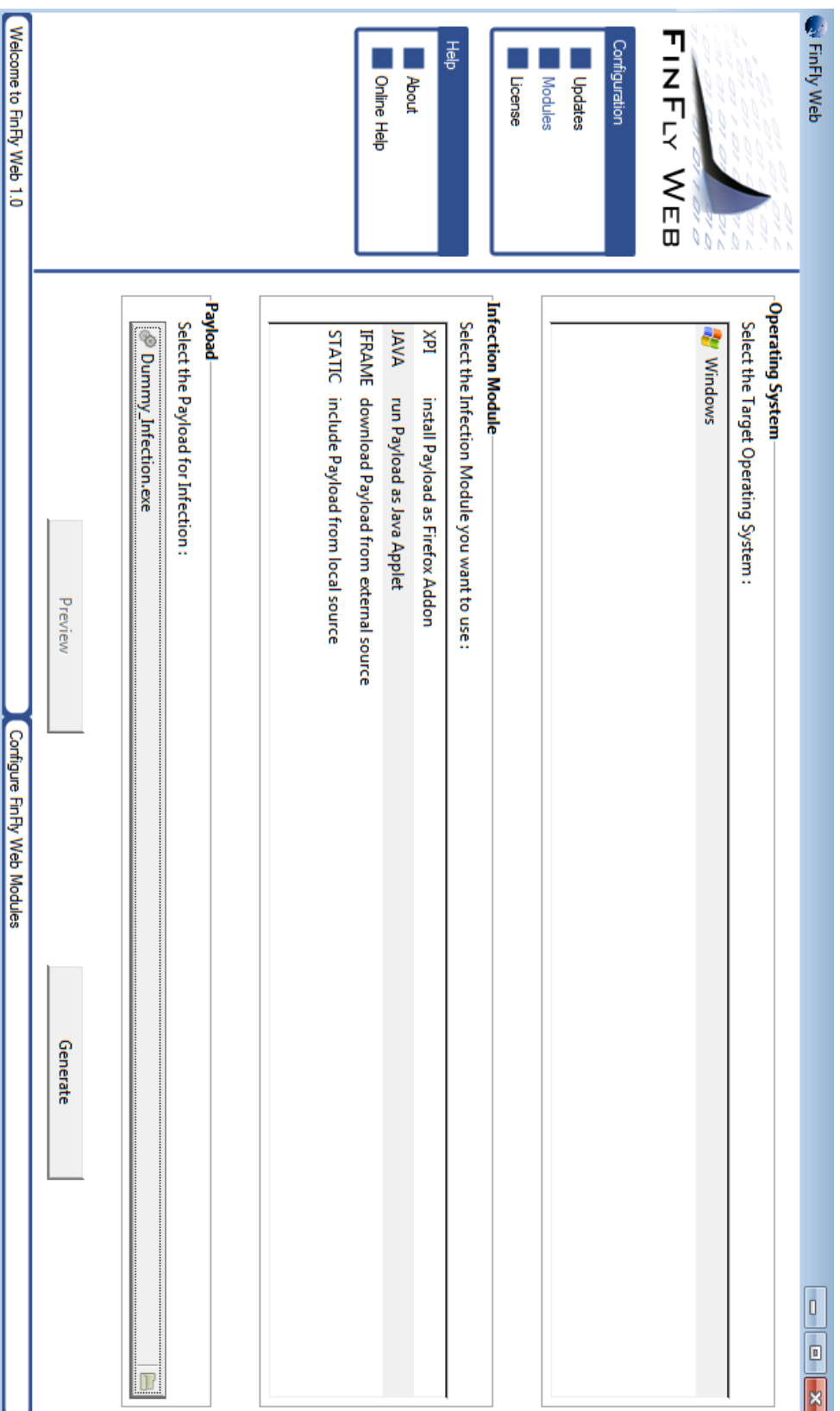


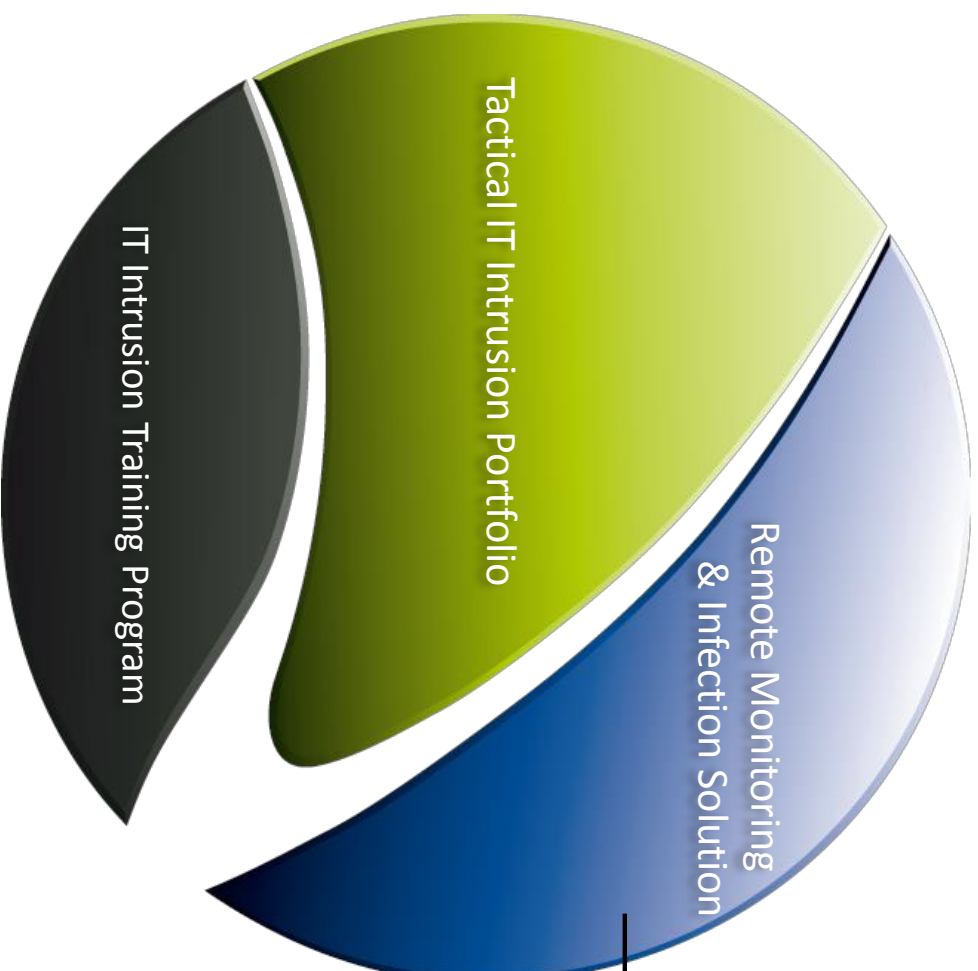
FinFly Web / LAN / ISP Integration



FinFly Web / Hard- and Software

- FinFly Web User Interface





FinSpy

FinFly

- USB
- Web
- **LAN**
- ISP

FinSpy Mobile



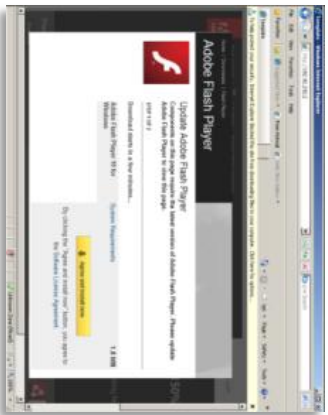
FinFly LAN / Operational Usage

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

Typical Operations:

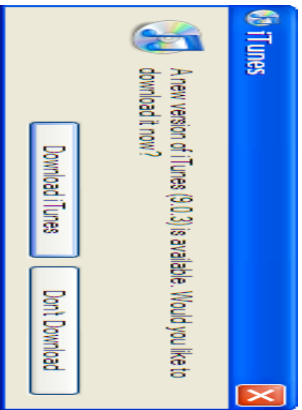
Deploy FinSpy through Hotspots:

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



Deploy FinSpy through LAN:

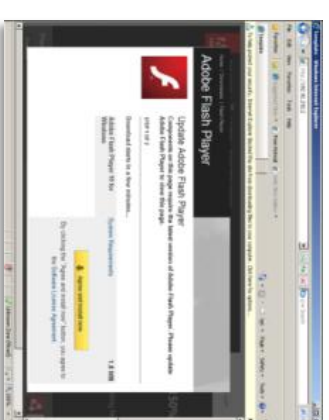
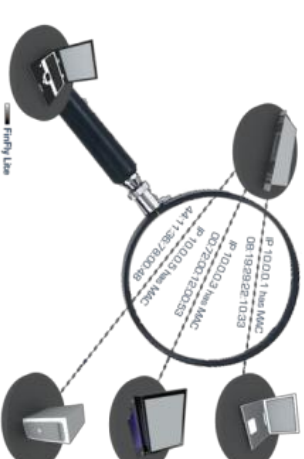
- Install FinSpy on Target System in Local Area Network
- Deploy by injecting fake Software Updates



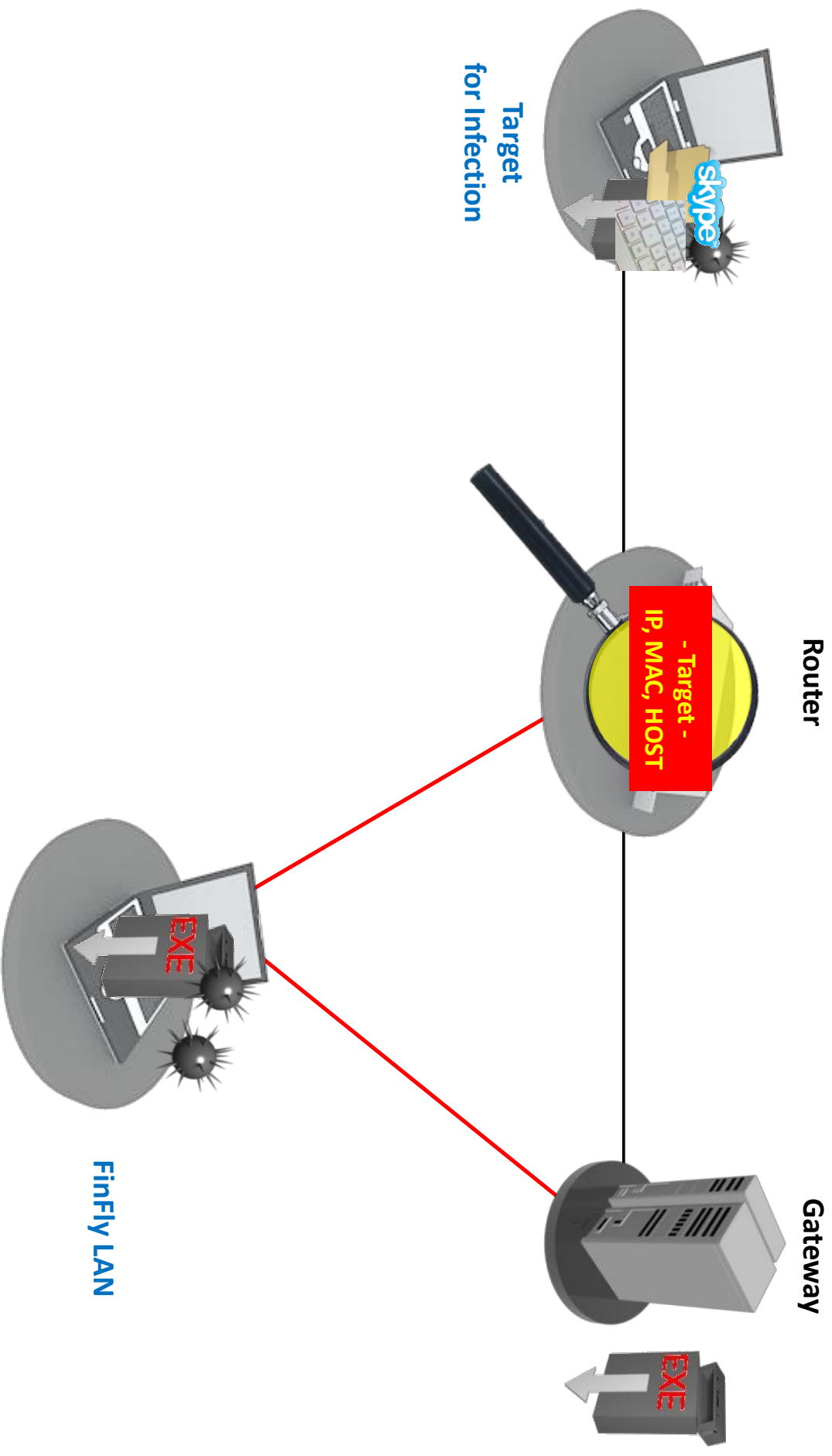
FinFly LAN / Core Features

62

- **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
- 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 LAN / Workflow



FinFly LAN / Hard- and Software

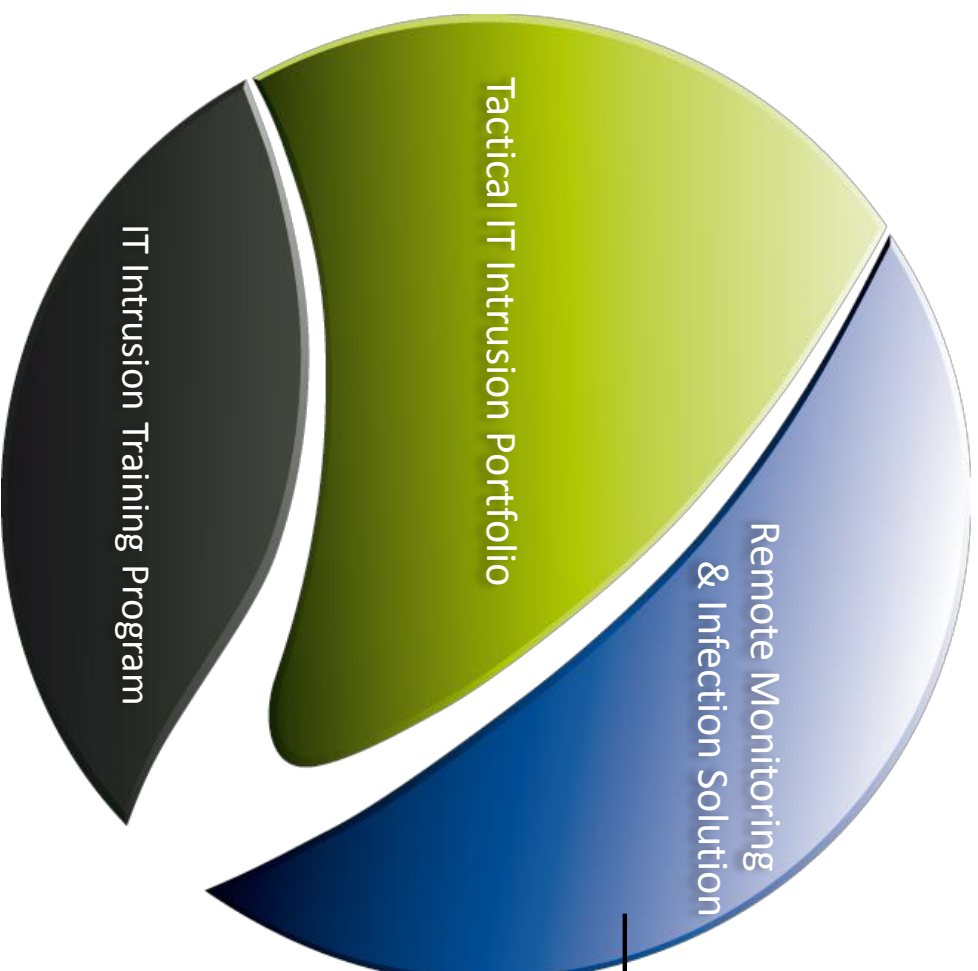
- FinFly LAN User Interface

The screenshot displays the FinFly LAN user interface. At the top, there is a header with the 'FinFly ISP' logo and the application name 'FINFLY LAN'. Below the header, there are three main menu sections: 'Preferences' with 'Updates' and 'License' options; 'Configuration' with 'Proxy', 'Add Target', 'Edit Target', 'Remove Target', 'Reinfect Target', and 'Clear Infected Targets' options; and 'Help' with 'About' and 'Online Help' options. The main content area is divided into two sections: 'Systems under Infection' and 'Systems Infected'. Each section contains a table with columns for 'Target Identifier', 'Payload', and 'InfectionMethod'. The 'Systems under Infection' table lists three test users with various payloads and infection methods. The 'Systems Infected' table lists two test users with different payloads and infection methods, including the date and time of infection.

Target Identifier	Payload	InfectionMethod
testuser 1	test_trojan_1.exe	Binary
testuser 2	test_trojan_2.exe	Binary and Update
testuser 3	test_trojan_2.exe	Binary and Update
testuser 4	test_trojan_2.exe	Update
10.0.0.51	test_trojan_3.exe	Binary and Update

Target Identifier	Payload	InfectionMethod	Infected at
testuser 5	test_trojan_1.exe	Binary	20:30:12 27/08/2010
10.0.0.52	test_trojan_2.exe	Update	16:12:37 23/08/2010





FinSpy

FinFly

- USB
- Web
- LAN
- **ISP**

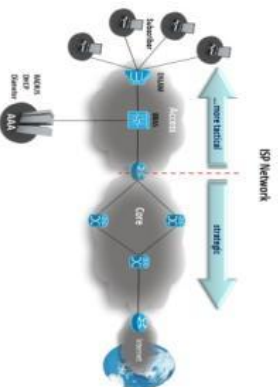
FinSpy Mobile



FinFly ISP/ Operational Usage

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



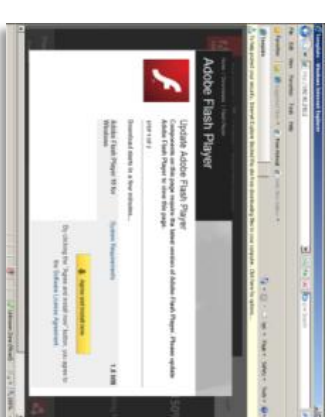
Install in Core of Local Area Networks:

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

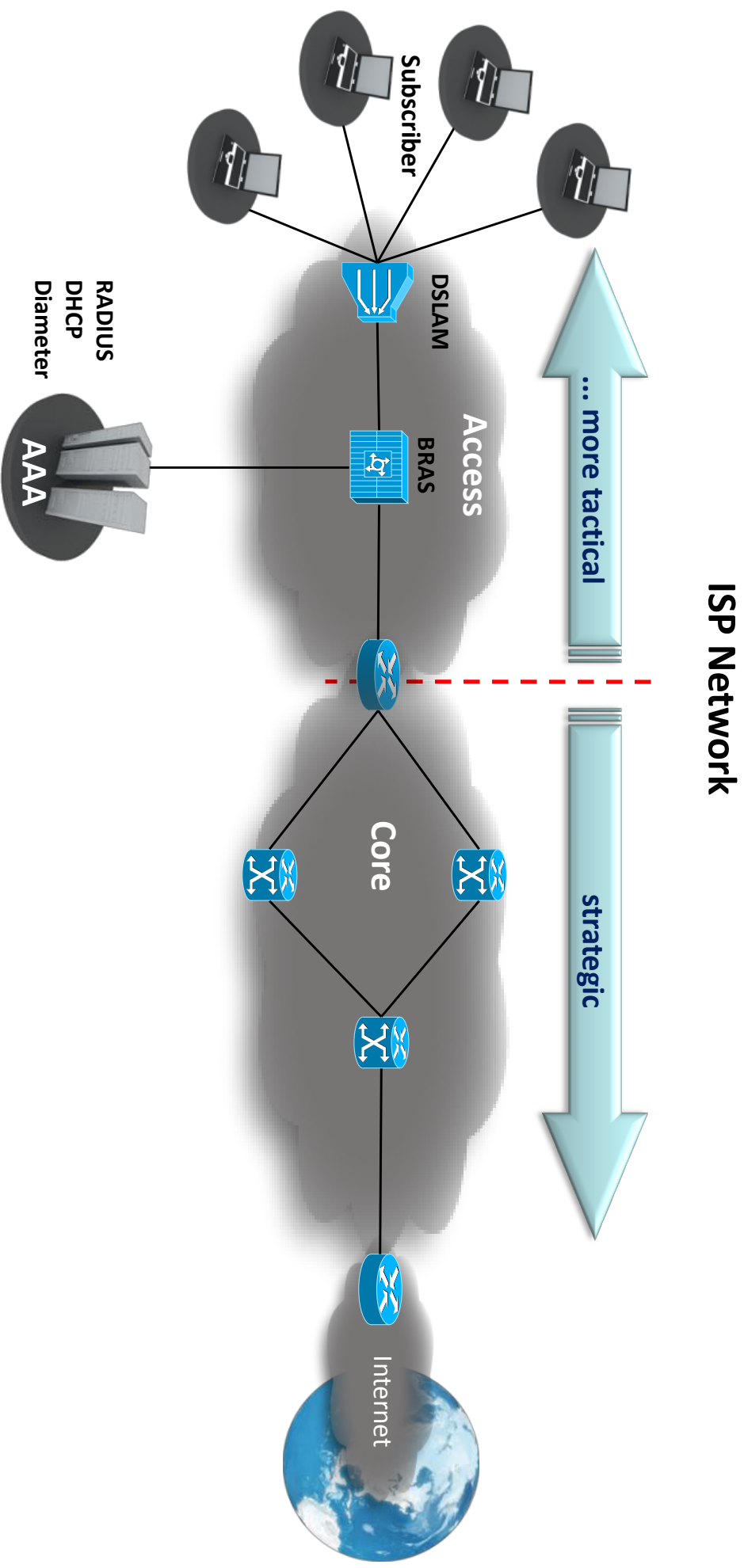


FinFly ISP / Core Features

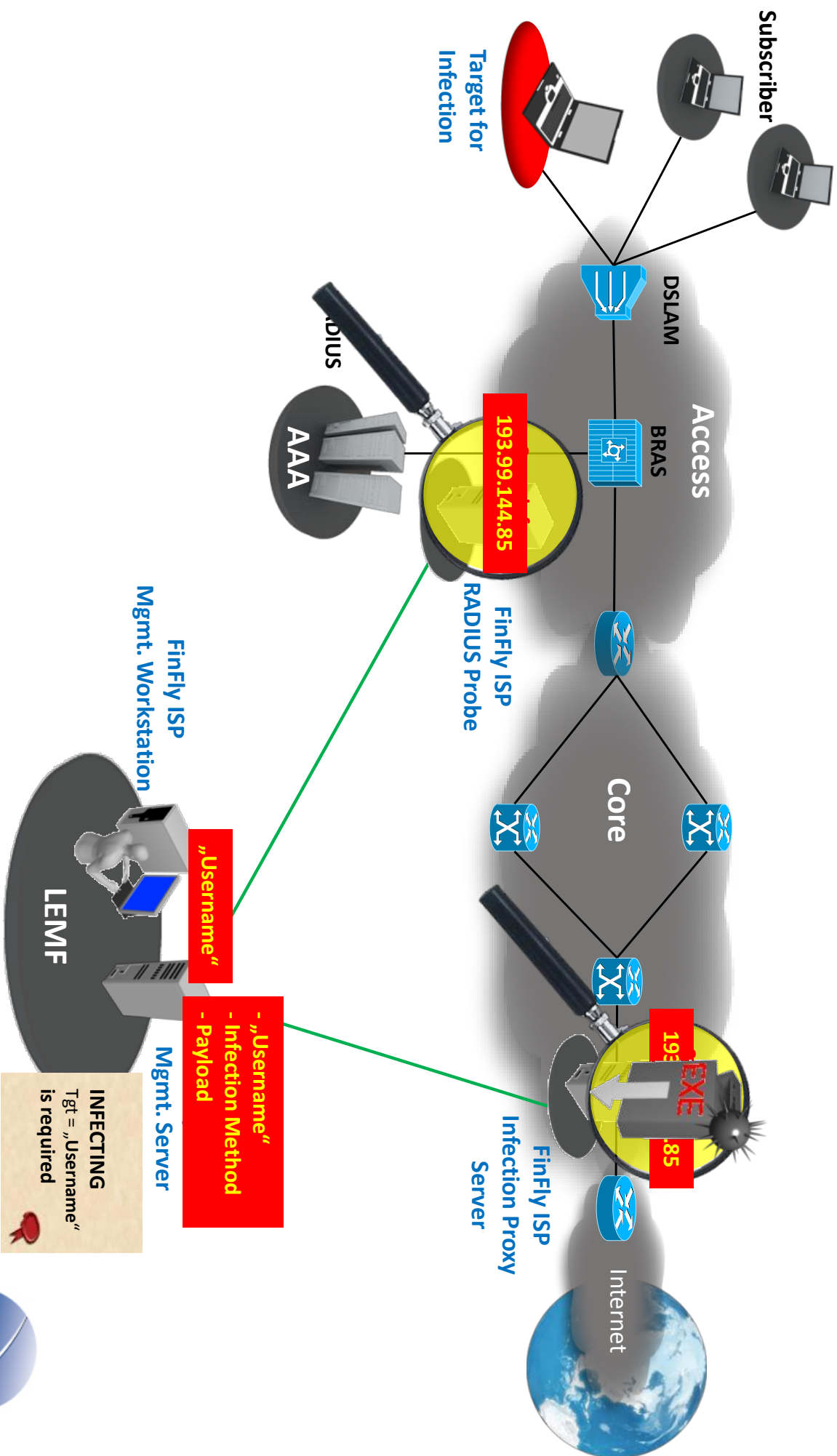
- Identify Targets by:
 - Username, Password (e.g. xDSL)
 - MAC-Addresses (Cable)
 - Dial-in phone number (ISDN, POTS)
 - IMSI, T-IMSI, MSISDN (Internet Access in Mobile Networks)
- Hides Remote Monitoring Solution in **Downloads of Targets**
- Injects Remote Monitoring Solution as **Software Updates**
- **Remotely installs Remote Monitoring Solution** through Websites visited by the Target



FinFly ISP / Deployment Example

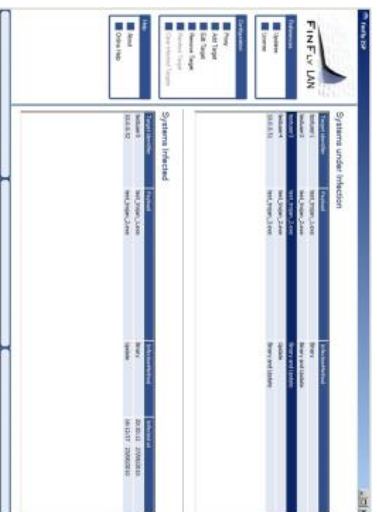


FinFly ISP / Workflow



FinFly ISP / Hard- and Software

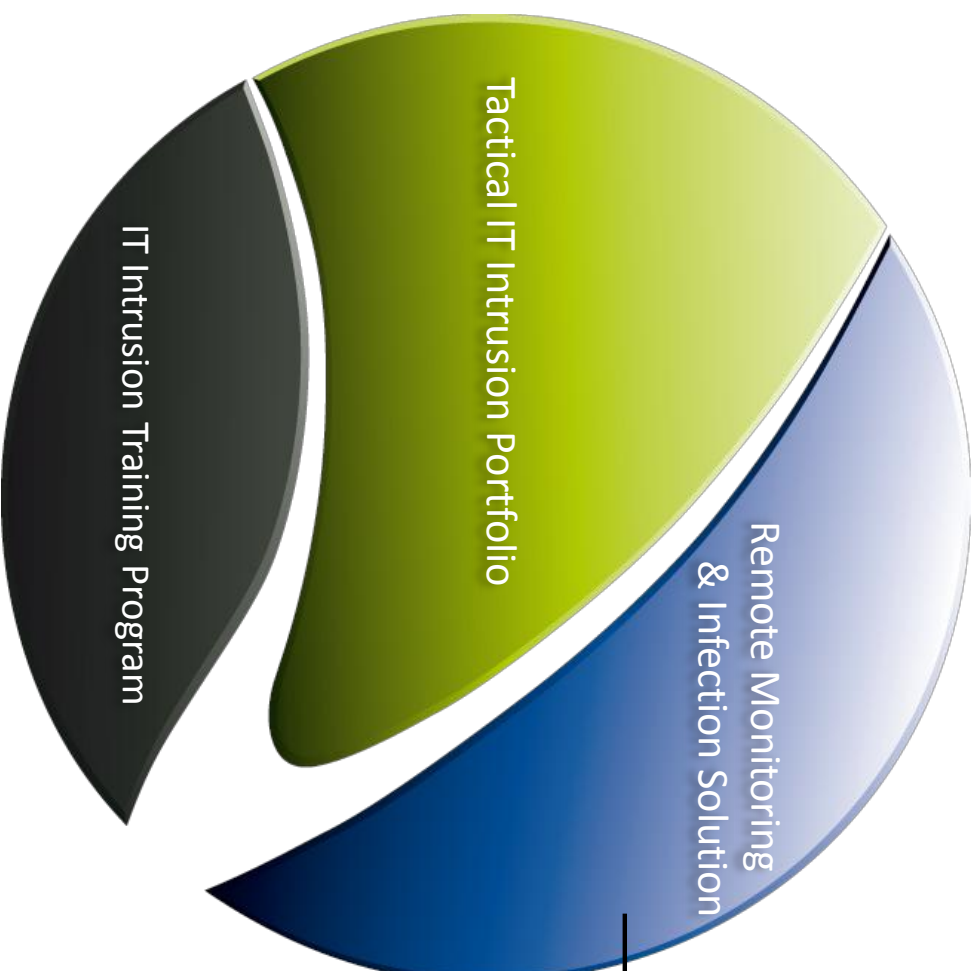
- FinFly ISP User Interface (GUI)



- Hardware – dependent on requires performance



Remote Monitoring and Infection Solutions



FinSpy

FinFly

FinSpy Mobile



FinSpy Mobile / Operational Usage

72

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



FinSpy Mobile / Core Features

- 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

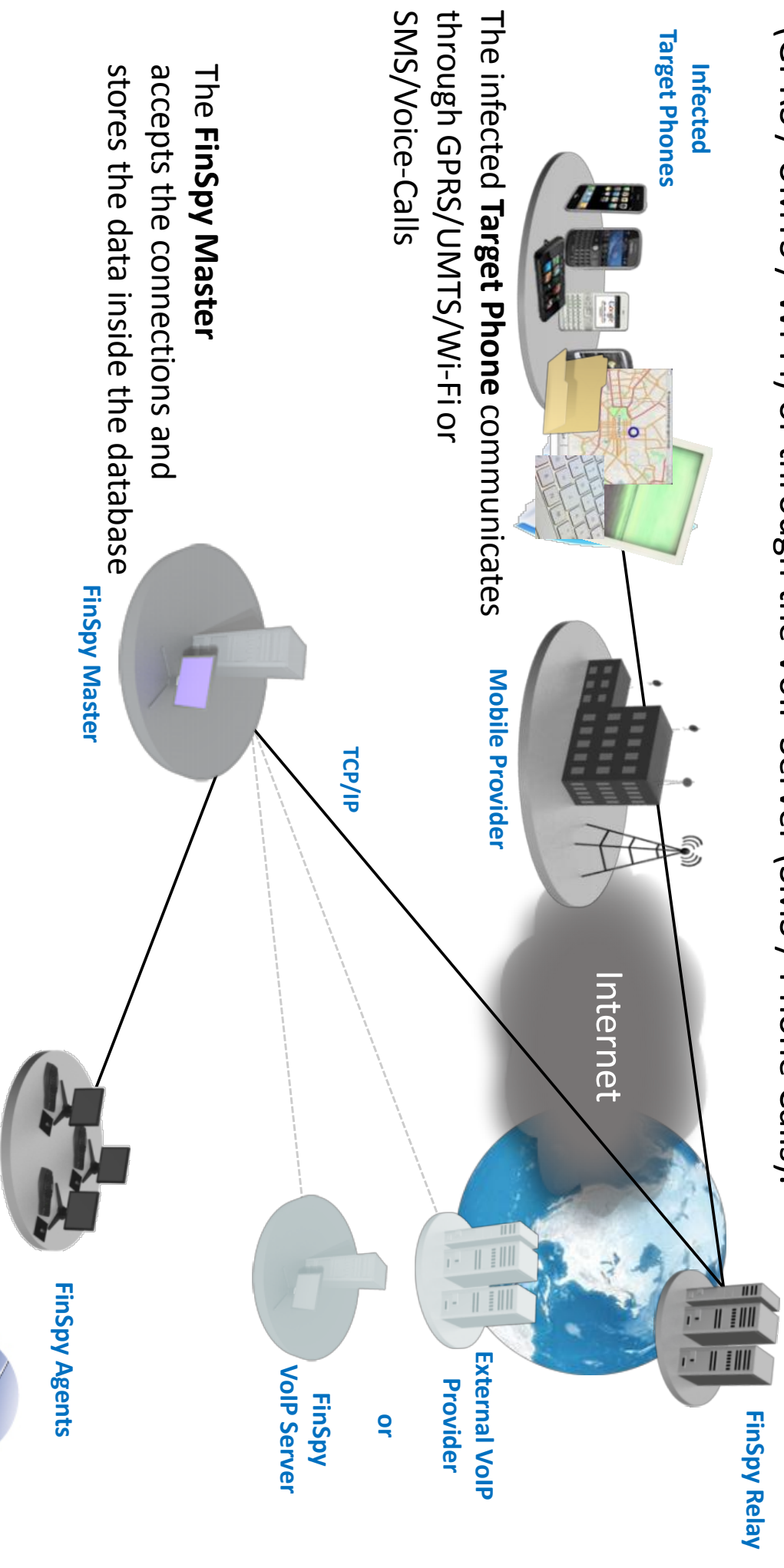


Evidence



FinSpy Mobile / Setup

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).



FinSpy Mobile / User Interface

The whole system is controlled through the **easy-to-use Graphical User Interface**.

The screenshot displays the 'Active' tab of the 'Mobile Targets' section in the FinSpy Mobile User Interface. The interface includes a sidebar with navigation options like 'Target', 'Tools', 'Administration', and 'Help'. The main area shows a table of active targets with the following data:

Name	UID	IMSI	Phone Number	OS	Provider	Country	City	Base Station	Last Heartbeat Time	IMEI	Heartbeat Type
testV30	0x144E298588A55	262022004940992	+491726651421	Android	Vodafone	Germany	--	262/2/951/236728743	2012-01-05 13:44:10	357215036475989	SMS
testV44	0x140747CF82895	262011541103511	+4915115194014	Android	T-Mobile	Germany	--	262/1/16970/27682	2012-01-05 11:53:55	352344033732757	SMS
test3	0x146558BC9EFE4	262021007649901	+491622197618	Android	Vodafone	Germany	--	262/2/951/12711	2012-01-10 09:17:40	358809030225892	TCP
test3	0x1408F671DC62	262021540263045	+491622099391	Android	Vodafone	Germany	--	262/2/951/236728743	2012-01-10 09:58:42	352666046815330	TCP
sony	0x87356870376	262022004940985	+491726606823	Android	Vodafone	Unknown	--	-1/-1/0/0	2012-01-02 21:17:15	012590000833398	SMS
SocketX	0x141D84196255C	262026042589822	+4915226632645	Android	Vodafone	Germany	--	262/2/951/12711	2012-01-09 16:57:46	353872045811036	SMS
SII	0x1460877A39930	262011541103512	+4915115194015	Android	T-Mobile	Germany	Harlaching	262/1/17355/5957742	2011-12-23 14:59:59	358490042505520	SMS
NoMod	0x1433912034A87	262021540263044	+491622095309	Android	Vodafone	Germany	Harlaching	262/2/951/236728743	2012-01-10 05:57:13	355499040262839	SMS
Newus12	0x142D4DFDC038A	262022004940985	+491726606823	Android	Vodafone	Germany	--	262/2/951/236728743	2012-01-09 17:19:20	354957032948666	SMS
MalagaX	0x7048858BC058A	666666553648138		Android	Unknown	Unknown	--	12/666/0/0	2012-01-02 12:39:31	123456783648138	SMS
MalagaX	0x1461D6536FA83	262011541103513	+4915115194016	Android	T-Mobile	Germany	--	262/1/16970/27681	2012-01-03 10:30:14	358567042808499	SMS
Happy	0x1448A21CDFED	262021007649902	+491622197660	Android	Vodafone	Germany	--	262/2/951/12711	2012-01-10 09:11:10	356835040032749	TCP
Galatlab	0x14104259F22C	262022004940985	+491726606823	Android	Vodafone	Germany	Harlaching	262/2/951/236728743	2012-01-10 10:02:41	352961048474156	TCP
Archived											
sdfdf	0x1470A6AE768A0	424021431706947	+971506448151	Android	Etsicat	United Arab Emi	Jumeira	424/2/40611/26622352	2012-01-09 11:54:22	359585045506976	SMS
ITest01	0x0A6014087118	226019451724216	+40724109607	Android	Vodafone	Romania	Desa	226/1/31119/0	2011-12-20 13:35:27	12030002622747	SMS



FinSpy Mobile / Infection Techniques

76

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**



FinSpy Mobile / Strategic System

- FinSpy Master and Relay

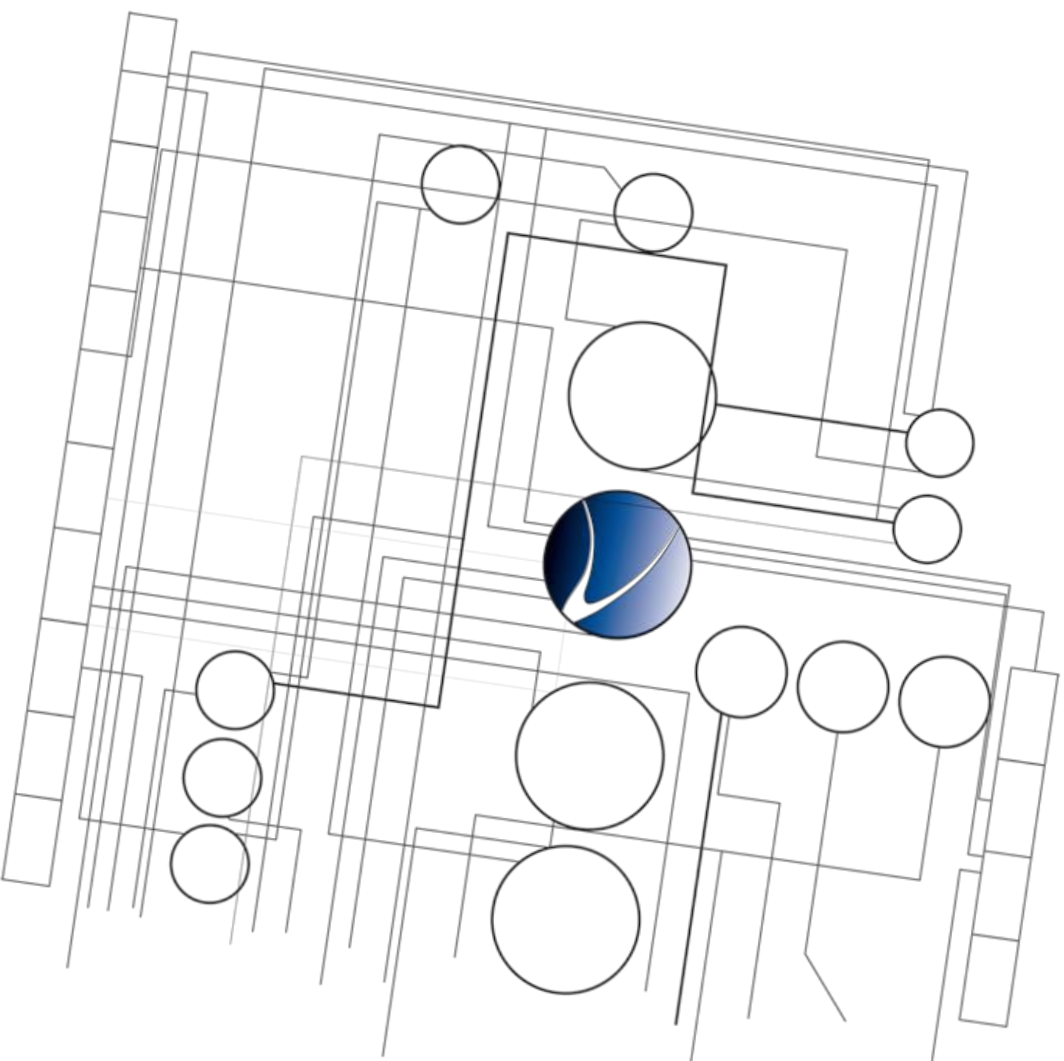


- FinSpy Agent(s)



- FinSpy VoIP Server PRI Cards for up to 30 lines





Day 2:

1. FinFisher Portfolio

- **Product Range**
- **Training Courses**
- **Support**

2. Real-Life Operations



With Gammas Team of **world-leading IT Intrusion experts**, a wide-range of offensive IT Intrusion trainings is available.

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

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



FinTraining / Basic IT Intrusion

80

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.

Duration: 5-10 days

Topics: Profiling, Attacking, Advanced Topics



FinTraining / Wireless IT Intrusion

81

Outline: 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.

Duration: 5 days

Topics: WLAN 802.11, Bluetooth



FinTraining / Practical Software Exploitation

82

Outline: This course is a practical training on using exploits for IT Intrusion purposes, e.g. using the latest Adobe Acrobat exploits to hide FinSpy inside PDF files.

Duration: 5-10 days

Topics: Exploit Introduction, Metasploit, Simple Reverse Engineering



FinTraining / Practical Web Application Exploitation

83

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.

Duration: 5-10 days

Topics: Identifying Software, Exploiting Vulnerabilities



FinTraining / Practical Penetration Testing

84

Outline: This course covers a wide-range of penetration testing examples which is conducted through several practical examples.

Duration: 5-10 days

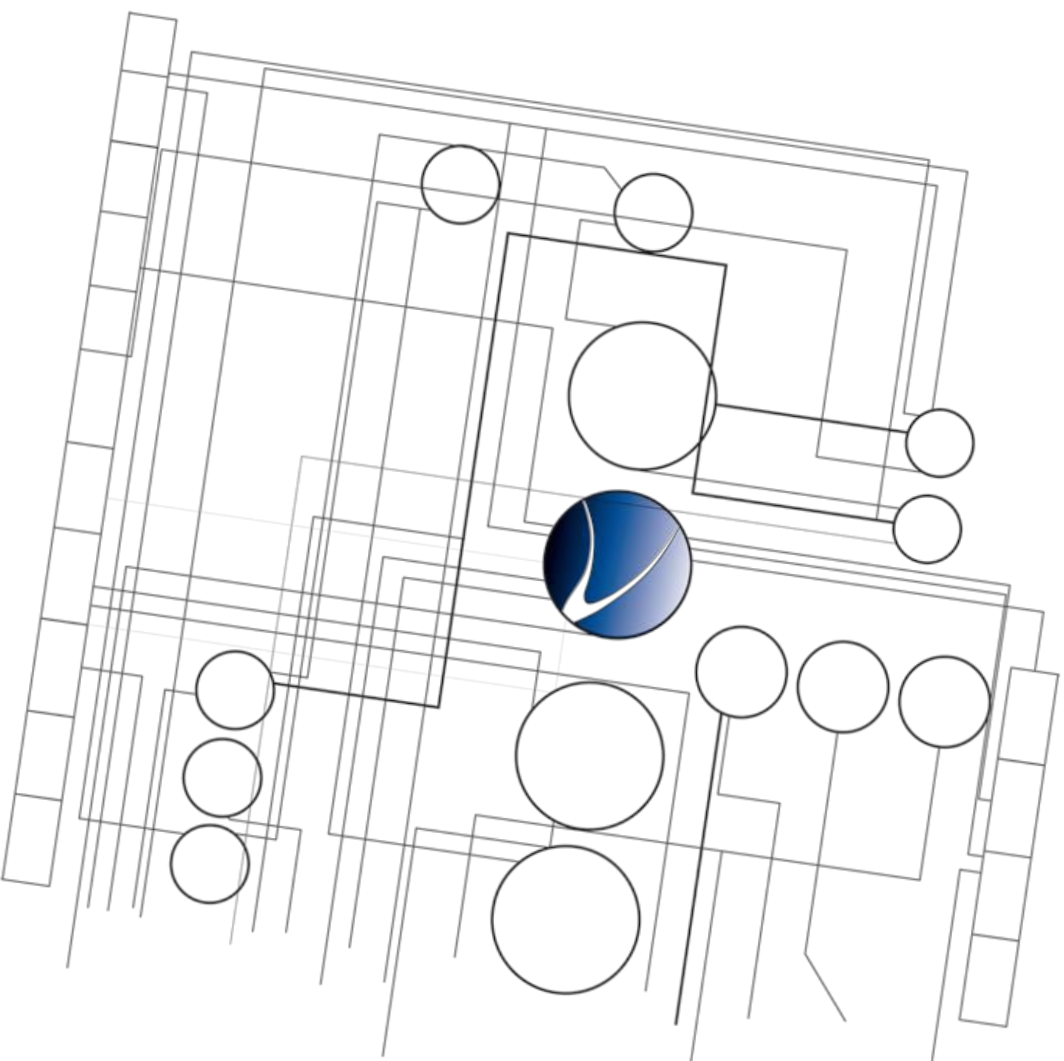
Topics: Network Attacks, Metasploit, Backdoors, Phishing, Wardialing, SSL Attacks



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

All Offensive IT Intrusion related topics can be provided on request.





Day 2:

1. FinFisher Portfolio

- **Product Range**
- **Training Courses**
- **Support**

2. Real-Life Operations

Professional Support

Online Support Website includes:

- User Manuals
- Product Roadmaps
- Product Change-Logs
- Frequently Asked Questions
- Bug Reporting System

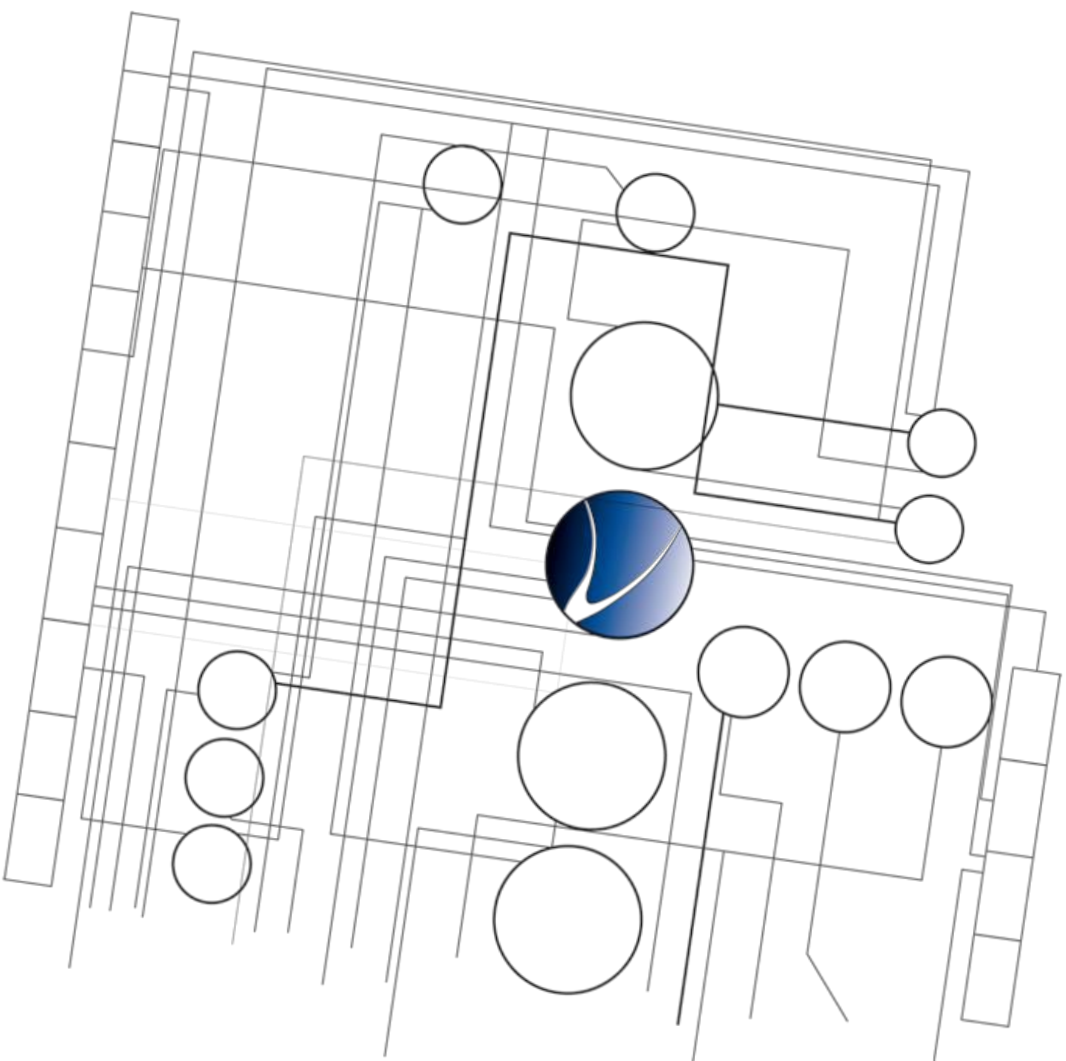
Software updates provided via:

- Download from Web
- Via Online Update System



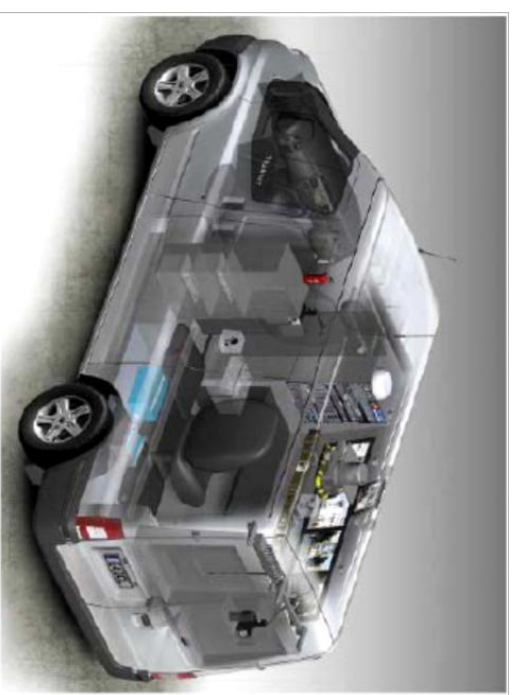
Day 2:

- 1. FinFisher Portfolio**
- 2. Real-Life Operations**



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 targets 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.

Also several customers use it to supply intelligence to TSU's for their operations.



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.



Scenario 4: FinUSB Suite

A target enters an Internet Café and checks his email. FinUSB had been applied after the suspect left the facility in order to extract all previously visited Web pages and passwords entered.



Scenario 5: FinSpy

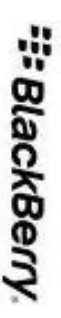
FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. **Using the Webcam**, pictures of the Targets were taken while they were using the system. The build in **Evidence Protection** enabled the LEA to use the information in court (**in accordance to EU standards**).



Evidence

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 and have the capability to identify the current location in case of emergencies. The same procedure was used with undercover operators in several cases.



Scenario 8: FinFly LAN/FinIntrusion Kit

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 in form of **payload within the targets downloads (Trojan Size 150kb)** i.e. .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 government offending websites **by covertly injecting the FinFly Web** code into the targeted websites and generating remote updates.



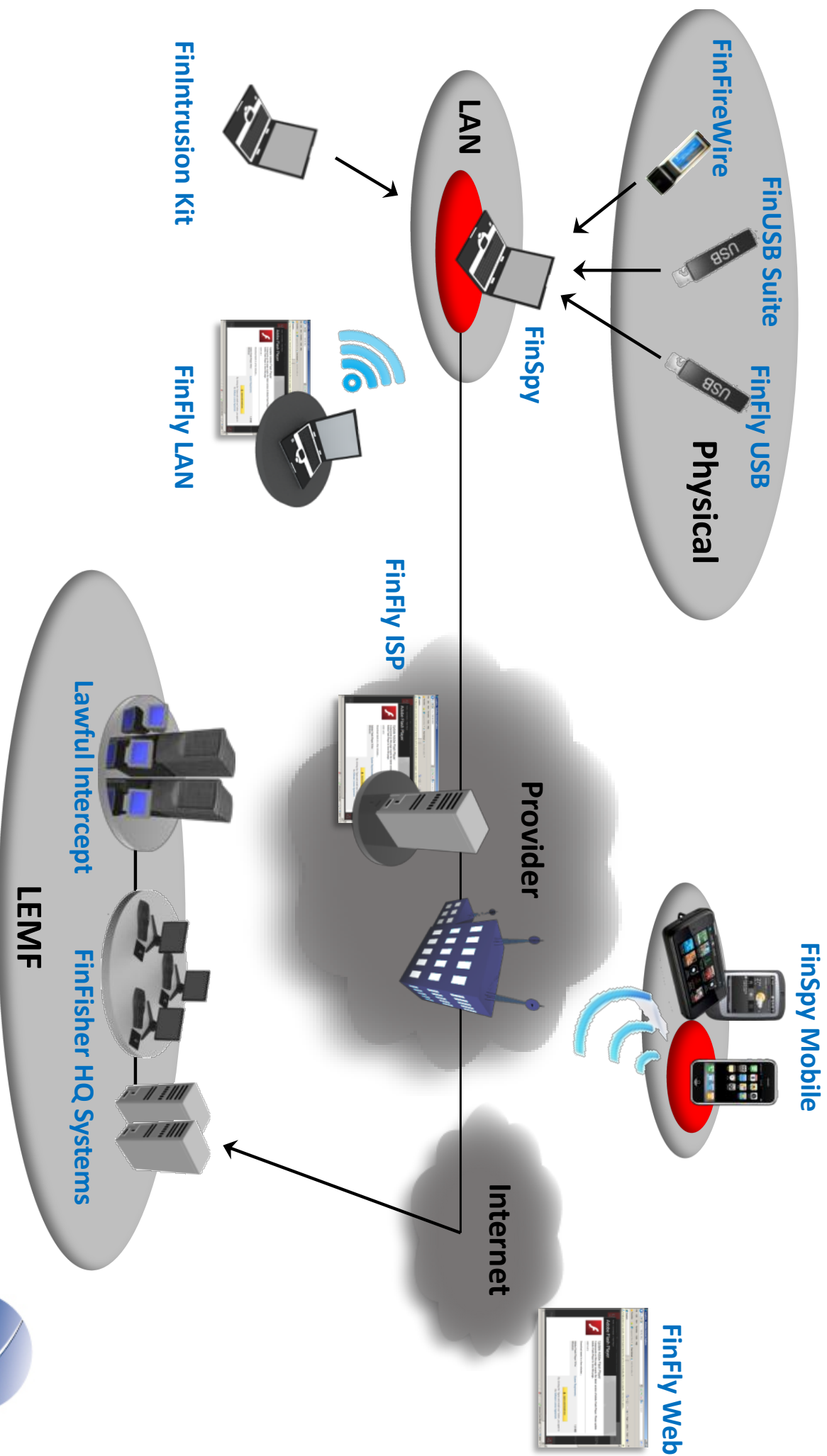
Operational Achievements / Training Examples

94

- **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)
- Attacks on critical Infrastructures
- **Sniffing** Data and User Credentials of Networks
- **Monitoring Hot-Spots**, Internet Cafes and Hotel Networks
- **Intercepts and Records Calls** (VoIP and DECT)
- **Security Assessment** of Web-Servers & Web-Services
- **Cracking** Password Hashes



FinFisher – The Complete IT Intrusion Portfolio



Why Gamma as a Partner?

96

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!



FINFISHER
IT INTRUSION

WWW.GAMMAGROUP.COM