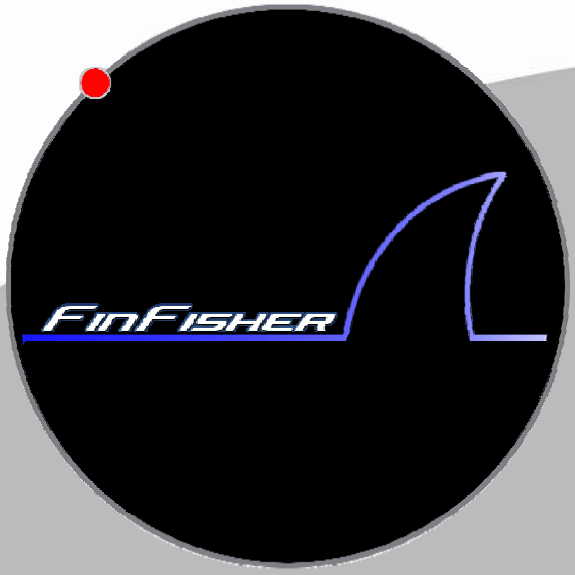
elaman
GERMAN SECURITY SOLUTIONS

GOVERNMENTAL SECURITY SOLUTIONS

FinFisher IT Intrusion Products



Finfisher Introduction

Introduction to Finfisher

Elaman is proud to present its new FinFisher product suite to aid government agencies in gathering critical IT information from target computers. This suite contains an array of IT solutions to help intelligence agencies gain access to information that cannot be procured using traditional methods.

Operational Features

- Information gathering
- Sniffing
- Exploitation
- Monitoring

FinFisher USB Suite

The FinFisher USB Suite is a set of two USB Dongles, two bootable CDs and the FinFisher HQ – a Graphical User Interface (GUI) – for analysis of retrieved data. The FinFisher USB Suite has been engineered for use by any agent, informant, or basically anyone who is able to gain access to a target computer, with minimal computer knowledge. All that needs to be done is to insert the USB into the target computer for a short period of time. It can extract information like usernames and passwords, e-mails, files and other critical system and network information from Windows systems.

FinFisher Remote Hacking Kit

When physical access to a target computer cannot be achieved, the FinFisher Remote Hacking Kit provides agents with all the necessary tools used by professional hackers to remotely gain access to target computers. It consists of a notebook running our specially engineered FinTrack operating system, various wireless equipment, a 500 GB USB hard-disk containing default password lists and rainbow tables, and much more. The FinFisher Remote Hacking Kit can be used for internal security assessment as well as IT intelligence gathering operations targeting public servers or personal computers.

FinSpy

FinSpy is a cutting-edge, professional Trojan horse for Windows systems, which enables you to remotely access and monitor target computers. The basic functionality includes features like Skype Monitoring, Chat Logging, Keystroke Recording, accessing printed and deleted files, and many more features. The Trojan horse is completely hidden and all its communications are entirely covert.

FinFly

FinFly is a transparent HTTP proxy that can modify files while they are being downloaded. Elaman has created two versions of this software; the FinFly-Lite and the FinFly-ISP. The FinFly-Lite can be used by the agency within a local network to append FinSpy or a custom Trojan horse to executables that are downloaded by a target computer. The FinFly-ISP can be integrated into an Internet Provider's network to infect en masse or targeted computers.

FinAudit

Network and system security are top priorities in today's changing world. For this reason, Elaman provides FinAudit – a security assessment of the customer's network and computers carried out by a high specialized Tiger Team to ensure the customer is protected as much as possible from local and remote attacks.

FinTraining

Elaman offers highly specialized FinTraining courses to educate agents in various offensive and defensive security topics. Apart from the Basic Hacking courses, several advanced courses can be given, including topics such as Hacking Voice-over-IP, Hacking Wireless Systems, Basic Cryptography and many more. The level of training is highly dependent on customer knowledge and special training courses can be customized to meet specific customer needs.

DEVELOPMENTS IN 2008

FinFly-ISP

FinFly is a transparent HTTP proxy that can modify files while they are being downloaded. The FinFly-ISP can be integrated into an Internet Provider's network to infect en masse or targeted computers.

FinCrack

Elaman has developed FinCrack – a high-speed super cluster for cracking passwords and hashes. It currently supports password recovery for Microsoft Office documents, NTLM /LM (Windows user hashes), WPA wireless networks, UNIX DES (Unix password hashes), WinZip protected files, and PDF password-protected files.

FinWifiKeySpy

FinWiFiKeySpy is a device for remotely sniffing keystrokes of commercial wireless keyboards (e.g. Microsoft, Logitech) that are within the Wi-Fi device range (20-50 m). The device also enables the customer to remotely control the wireless keyboard and thus control the target computer.

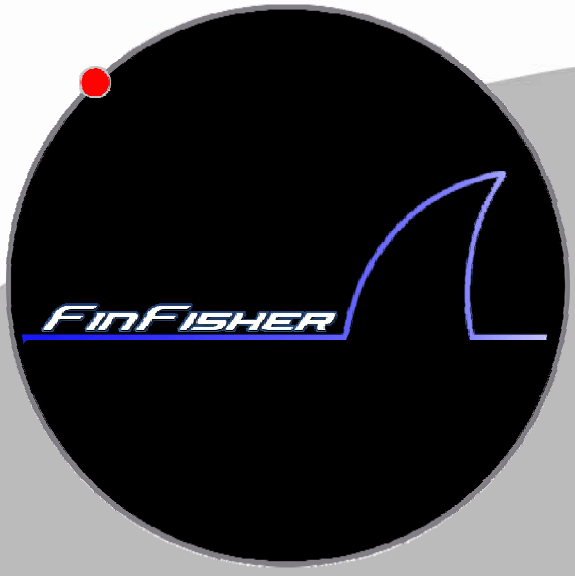
FinBluez

Elaman is developing the FinBluez – a product that enables agencies to do various advanced attacks against Bluetooth devices like mobile phones, headsets and computers. For example, FinBluez is able to record the audio stream between a headset and a mobile phone or utilize common Bluetooth headsets as audio bugs.

elaman
GERMAN SECURITY SOLUTIONS

GOVERNMENTAL SECURITY SOLUTIONS

FinFisher IT Intrusion Products

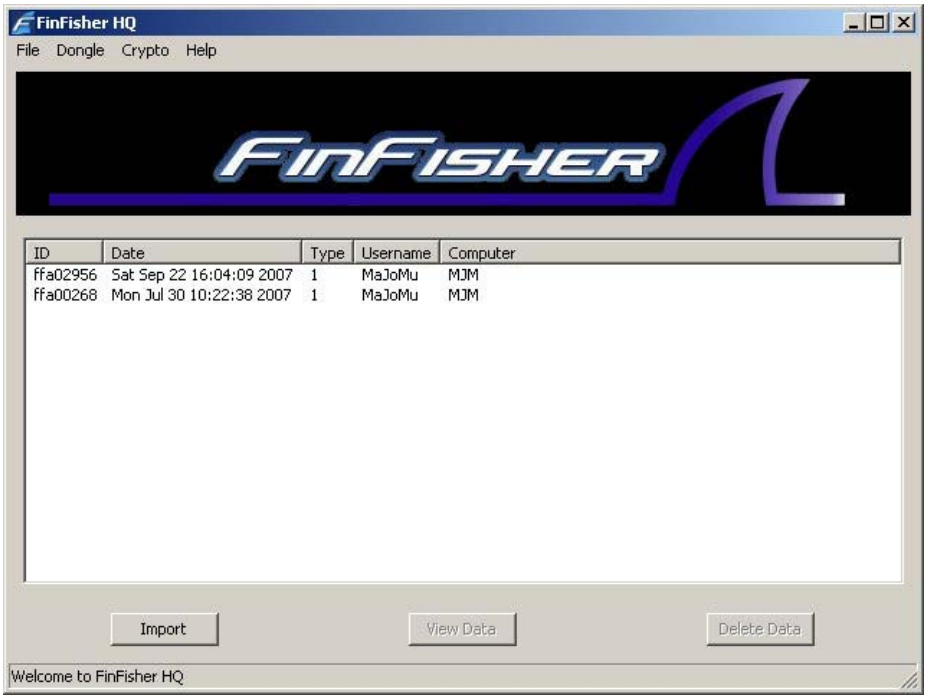


Finfisher Products

Finfisher HQ

The FinFisher HQ software is the main software for FinFisher 1 and 2. It is used to configure the operational options of the two devices and to import/decipher the gathered data and generate reports according to the FinFisher type.
It can also be used to update and repair FinFisher 1 and 2 device systems.
The FinFisher HQ Software shows all gathered and imported data in a sorted list.

Screenshot:

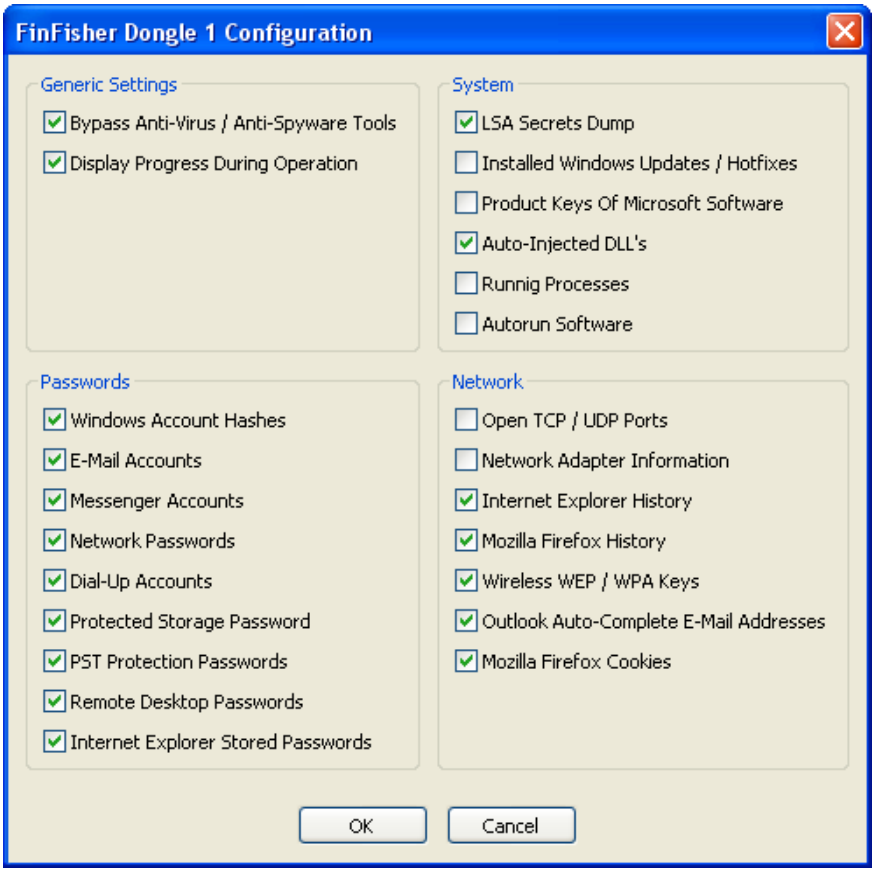


FinFisher HQ supports Windows systems equal to and newer than Windows 2000 and is pre-installed on the FinFisher Hacking PC.

FinFisher 1

FinFisher 1 is a U3-enabled USB device that is activated when inserted into the target's system with no or little user intervention.

The functionality is configured using the FinFisher HQ software. The gathered data is also deciphered, imported and analyzed by the FinFisher HQ software.
The data collected by the device is stored in encrypted form and can only be decrypted and accessed at Headquarters where the HQ software is running. It uses a private-/public-key cryptography mechanism by utilizing various known algorithms.
This prevents data from being disclosed or the device being misused should it be lost or stolen. Furthermore, the operational agent cannot be forced to decipher the data as he would need the private key, which remains on the HQ system.



The device indicates when the data gathering process is finished so that the agent knows when to remove it from the system.
If removed prematurely, due to operational necessity, the device will not be damaged, or compromise the security of the gathered data or the software contained on the device.
The device contains a component that deactivates and then reactivates all known installed Anti-Virus/Anti-Spyware software.
The device contains the following data gathering capability (subject to the information being available on the target's PC and accessible by the FinFisher device):

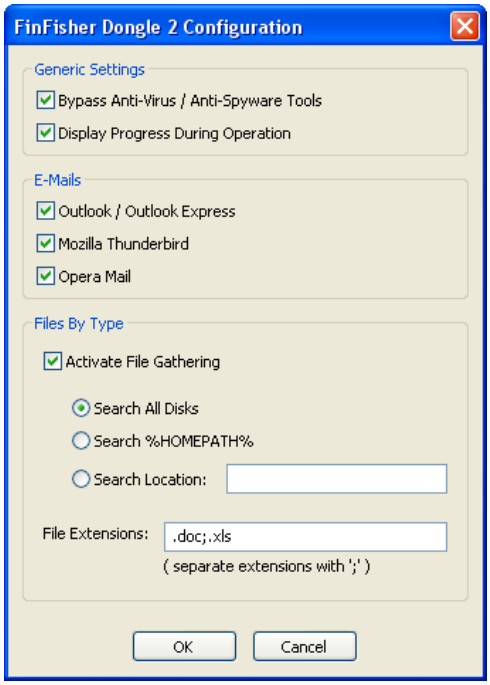
- Displays Windows user accounts and password hashes
- Displays details of passwords and other email account information on the following email applications: Outlook Express, Microsoft Outlook 2000 (POP3/SMTP Accounts only), Microsoft Outlook 2002, IncrediMail, Eudora, Netscape Mail, Mozilla Thunderbird, Group Mail Free, and Web-based email accounts.
- Displays username and password details of MSN Messenger, Windows Messenger (Windows XP), Yahoo Messenger (Version 5.x/6.x), ICQ Lite 4.x/2003, AOL Instant Messenger, AOL Instant Messenger/Netscape 7, Trillian, Miranda, and Gaim / Pidgin
- Displays stored passwords for network shares
- Displays details of all Dial-Up accounts, including the user name, password, and the domain
- Displays the details of the lost password of Outlook .PST (Personal Folders) file
- Displays stored remote desktop passwords

- Displays passwords stored by the Internet Explorer
- Displays the list of all LSA secrets stored in the registry. The LSA secrets may contain RAS/ VPN, Auto-logon and other system passwords / keys
- Displays the content of the protected storage which might contain various passwords
- Displays the list of all installed Windows updates (Service Packs and Hotfixes)
- Displays the product ID and the CD-Key of MS-Office, Windows, and SQL Server
- Displays the list of DLLs that are automatically injected into every new process
- Displays the list of all processes currently running. For each process, it lists all modules (DLL files) that the process loads into memory. For all processes and modules, additional useful information displayed is: product name, version, company name, description of the file, and the size of the file
- Displays the list of all applications that are loaded automatically when Windows boots. For each application, additional information is also displayed (product name, file version, description, and company name)
- Displays the list of all currently opened TCP and UDP ports. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it
- Displays information about the target network adapters: IP addresses, hardware address, WINS servers, DNS servers, MTU value, number of bytes received and sent, the current transfer speed, and more. In addition display general TCP/UDP/ICMP statistics for the target computer.
- Displays all information from the history file on the target computer, and display the list of all URLs that the target has visited with the Internet Explorer browser in the last few days.
- Displays the details of all wireless network keys (WEP/WPA) stored by the 'Wireless Zero Configuration' service of Windows XP
- Displays all auto-complete e-mail addresses stored by Microsoft Outlook
- Displays all cookies stored by Mozilla Firefox

FinFisher 1 supports Windows systems equal to and newer than Windows 2000.

Finfisher 2

FinFisher 2 is a U3-enabled USB device that is activated when inserted into the target's system with little or no user intervention.
The functionality is configured using the FinFisher HQ software. Furthermore, the gathered data is deciphered, imported and analyzed by the FinFisher HQ software.



The data collected by the device is stored in encrypted form and can only be decrypted and accessed at Headquarters where the HQ software is running. It uses a private-/public-key cryptography mechanism by utilizing various known algorithms.
This prevents data from being disclosed or the device being misused should it be lost or stolen. Furthermore, the operational agent cannot be forced to decipher the data as he would need the private key, which remains on the HQ system.
The device indicates when the data gathering process is done so the agent knows when to remove it from the system.
If removed prematurely, due to operational necessity, the device will not be damaged, or compromise the security of the gathered data or the software contained on the device.
The device contains a component that deactivates and then reactivates all known installed Anti-Virus/Anti-Spyware software.
The device contains the following data gathering capability (subject to the information being available on the target's PC and accessible by the FinFisher device):

- Copies any locally stored emails (Microsoft Outlook, Outlook Express, Mozilla Thunderbird, and Opera Mail).
- Copies files with a specific file extension after making a search through all local drives.

FinFisher 2 supports Windows systems equal to and newer than Windows 2000.

FinFisher 3

FinFisher 3 consists of two bootable CD-ROMs.
The devices have to be inserted and the target system has to be rebooted. Little user-interaction is required during the whole process.

The devices contain the following functionality:

- Clears the windows administrator password
- Securely wipe the local hard-disks

FinSpy

FinSpy is a professional Trojan horse that can be used by law enforcement agencies to monitor the computer system of targetted persons that run a Microsoft Windows operating system (Windows 98 to Windows Vista).
The package offers the capability to monitor one or multiple systems using a centralized server and dedicated clients.
The FinSpy package can be used even by agents without advanced IT technology knowledge as it provides a simple point-and-click user interface.
The FinSpy Trojan horse executable itself is fully customizable and will look different on every target system. It also utilizes all up-to-date techniques to hide itself and all its activities from the system and, therefore, is hard to detect.

FinSpy Components:

- *FinSpy Client:* The user interface that is used by the agents to get access to the target's system and gather information or control (e.g. reconfigure or remotely delete) the FinSpy Target
- *FinSpy Server:* Central server where all infected clients connect and publish their availability and basic system information. The server is also contacted by the FinSpy Client to get the infected target list
- *FinSpy Target:* This is the package that is used for the infection and is installed on the target system
- *FinSpy U3-USB Dongle:* A U3 USB dongle that contains software to deactivate all running Anti-Virus/Anti-Spyware software and installs the FinSpy Target component with little or no user interaction
- *FinSpy Antidote:* Software to detect and remove FinSpy Target that can also prevent the installation
- *FinSpy Proxy:* (Optional) A proxy that forwards connections between FinSpy Target and FinSpy Server that can be used to have multiple active public IP addresses and limit the possibility of detection by researchers

FinSpy Features:

Certificate based encryption

All communication and data is enciphered using RSA certificates.

Custom Executables

For each client, a customized executable will be created which prevents detection by Anti-Virus and Anti-Spyware utilities.

File Access

The remote file system can be accessed and all files can be viewed, edited and downloaded. Custom files can also be uploaded to the target system.

Key-logging

All keystrokes can be recorded to a file which enables FinSpy to even view text that is sent through SSL or Skype sessions.

Password Sniffing

A password sniffer can be started in the background that collects all passwords for plain-text protocols like POP3, IMAP, Samba Shares, FTP and many more.

Webcam Recording

The webcam of the target system can be utilized to monitor the target person or environment.

Microphone Recording

The microphone of the target system can be utilized to monitor the target person or environment.

Timing based operations

All operations and functionality of FinSpy can be scheduled by days and hours.

Local Passwords

FinSpy can provide a list of local passwords for applications like Windows, E-Mail clients, Messengers and many more.

E-Mail Dumping

E-Mails can be dumped to a file before they are sent in order to be able to analyze even SSL enciphered mail traffic.

Chat Logging

Various instant messenger and chat protocols can be monitored. This includes MSN, ICQ, IRC and Skype.

Auto-removal

FinSpy can remove itself automatically from a target's system without leaving traces if selected by an agent or scheduled by the configuration.

Live Configure

All options of FinSpy can also be configured at run-time and additional modules can be loaded.

Live Update

The *FinSpy Target* itself can be updated to the newest version even at runtime using the client's software.

IP notification

When the IP address of the target system is changed, it will send the new address to the centralized server.

Country Tracing

Using the IP address, the target's location is traced and traveling is detected by displaying the actual country, plus the previous countries where the target was located.

Generic system information

Generic system information can be retrieved which includes installed software, auto-run programs, etc.

Remote Command Shell

A remote command shell on the target's system can be accessed to manually execute custom commands.

Connect-back

FinSpy is able to create a reverse connection on arrival of a specially crafted packet. This helps bypassing Firewalls and especially NAT-enabled environments where the client does not have a public reachable IP address. **FinSpy supports Windows systems equal to and newer than Windows 98.**

FinFly

FinFly is a transparent HTTP proxy that can modify content while it is being downloaded.
It can be used to infect executables that are downloaded from a web server with FinSpy or custom Trojan horses.
Using the configuration file, IP addresses can be selected which means that only a certain range or a single address is going to be infected or a certain range should be ignored by the proxy.
FinFly comes with a special loader that merges the Trojan horse with the original executable. On execution, the Trojan gets installed, is removed from the original and then the original executable gets executed. Using this technique, most common malware detection mechanism of common Anti-Virus/Anti-Spyware utilities can be bypassed.
Optionally, the proxy can be extended to modify any other file types and also totally replace files while they are being downloaded.
FinFly supports Linux systems equal to and newer than 2.6. Windows and BSD support can be added upon request.

FinFisher Hacking PC

The FinFisher Hacking PC consists of a robust notebook plus various hacking equipment.
It can be used to locally (Wireless LAN, Bluetooth) or remotely attack single systems or networks. The kit is equipped with all generic components that are used by professional hackers.

The equipment includes:

Notebook	1 Steatite M230 Ruggedized Notebook
Wireless	1 PCMCIA Wireless Adapter 1 Bluetooth Adapter (modified to support antennas) 1 Directional antenna 1 Omni-directional antenna
Ethernet	1 USB-to-Ethernet adapter 1 Cross-over Ethernet cable 1 Ethernet cable
Storage	1x 500 GB hard disk (including rainbow tables, default password lists, etc)
Case	1 Case
Misc	1 Power Surge Adapter 1 CD-Holder Windows Driver CD's

The software includes:
FinTrack – An operating system based on BackTrack/Linux that includes patched wireless drivers, all common and up-to-date hacker tools and lots of additional scripts for easier and faster usage.

Windows XP – Including the FinFisher HQ software and all common up-to-date hacker tools that are available for the Windows platform.

FinAudit

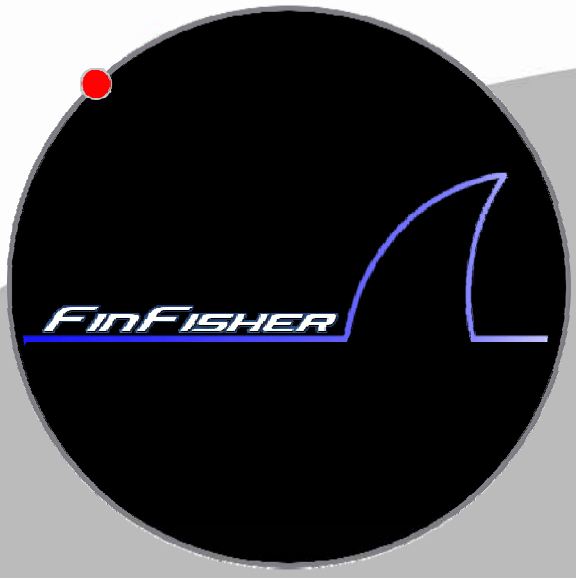
FinAudit is a 1 or 2 week professional penetration testing for a given network to discover the possible vulnerabilities in systems and software and helps in securing the network IT environment.

The audit can be done remotely and locally. A local audit should be always considered to detect all attack vectors for local, physical and especially insider attacks.
FinAudit includes a complete IT-based penetration test against the available and publicly used infrastructure and all public and internal systems.
A complete audit and fixing of discovered vulnerabilities helps to prevent attacks and information disclosure.
Single software can also be checked for vulnerabilities, including a full source-code analysis.
At the end of the penetration testing, a detailed report including all possible attack vectors and vulnerabilities, including a presentation of the report and consulting, are delivered.
On request, a service to help secure the network, system and communications can also be provided.

elaman
GERMAN SECURITY SOLUTIONS

GOVERNMENTAL SECURITY SOLUTIONS

FinFisher IT Intrusion Products



I- FinFisher Introduction
II- FinFisher Products Review
III- FinFisher Training Courses
IV- FinFisher New Products Developments
V- FinFisher Presentation

Finfisher Training List

FinTraining Course Overview				
Course No.	*Course name*	*Duration*	*Location*	*Number of students*
8601-1	**FinTraining Intensive Basic Hacking Course** Aim: Practical knowledge of IT hacking of networks and exploiting their weaknesses using the FinFisher Remote Hacking Kit	1 week	Europe or in-country	2 to 4 students
8601-2	**FinTraining Extended Basic Hacking Course** Aim: In-depth knowledge of IT hacking of network and exploiting their weaknesses using the FinFisher Remote Hacking Kit	2 weeks	Europe or in-country	2 to 4 students
8602	**FinTraining Advanced Exploiting Software** Aim: How to exploit bugs in software for intell manipulations	1 week	Europe or in-country	2 to 4 students
8603	**FinTraining Advanced RootKits** Aim: How to use, detect, and enhance rootkits	1 week	Europe or in-country	2 to 4 students
8604	**FinTraining Advanced VoIP Hacking** Aim: How to manipulate VoIP servers and clients as well as monitoring of VoIP communications	1 weeks	Europe or in-country	2 to 4 students
8605	**FinTraining Wireless Hacking** Aim: How to gain access to wireless LAN networks/Bluetooth devices/wireless keyboards	1 week	Europe or in-country	2 to 4 students
8606	**FinTraining Covert Communications** Aim: How to hide specific information in protocols/media/cryptography.	1 week	Europe or in-country	2 to 4 students
8608	**FinSpy Training** Aim: Specialized training on FinSpy Trojan horse usage	1 week	Europe or in-country	2 to 4 students

Finfisher Hacking Course

Course 8601 Intensive/Basic/Extended

FinTraining 8601-02: Basic Hacking Course For Beginner (2 weeks) indepth					
	Monday	*Tuesday*	*Wednesday*	*Thursday*	*Friday*
Week 1	**FinFisher** • FinFisher HQ • FinFisher 1 • FinFisher 2 • FinFisher 3 **Toolset** • FinFisher Hacking PC • Equipment • FinTrack	**Profiling** Foot printing • Search Engines • Archives • Target Websites • "Who is" Records • DNS Analysis • First Contact Scanning • Mapping • Port scanning • Service Fingerprinting • OS Fingerprinting • Analysis	**Profiling** Enumeration • CGI • NetBIOS • SNMP • RPC • NFS • Other	**Attacking** Passwords • Bypass • Default • Brute force • Cracking • Trusted	**Attacking** Web security • Code Exposure • Input Validation • CGI • XSS • SQL Injection • Other
Week 2	**Attacking** Exploits • Overflows • Format Strings • Race Conditions • Archives • Exploiting • Frameworks • Fuzzer	**Attacking** Root-kits • Backdoors • Hiding • Log-cleaner	**Attacking** Network • Sniffing • Rerouting • War-dialing	**Attacking** Wireless LAN • Discovery • Encryption • Advanced • Hardware	**Attacking** Bluetooth • Discovery • Attacks • Hardware Advanced • Custom Exploits

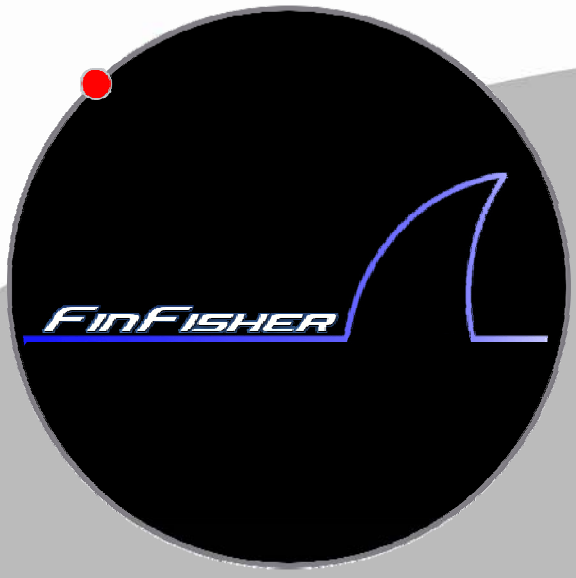
Course 8602: Advance Exploiting Software

Fintraining: Exploiting Software					
	Monday	*Tuesday*	*Wednesday*	*Thursday*	*Friday*
Week 1	**Introduction** • Famous Examples **Vulnerabilities** • Code Exposure • Authentication Bypass • Unexpected Input • SQL Injection • XSS • Race Conditions • Overflows • Format Strings	**Exploits** • Online Archives • Modification and / Customization • Frameworks	**Finding Bugs** • Source-Code Analysis • Fuzzing • Debugging	**Writing Exploits** • Unexpected Input • Overflow • Format-String	**Examples** • Web-Applications • Server • Clients • Embedded

elaman
GERMAN SECURITY SOLUTIONS

GOVERNMENTAL SECURITY SOLUTIONS

FinFisher IT Intrusion Products



I- FinFisher Introduction
II- FinFisher Products Review
III- FinFisher Training Courses
IV- FinFisher New Products Developments
V- FinFisher Presentation

Finfisher Development 2008

FinFly-ISP

FinFly is a transparent HTTP proxy that can modify files while they are being downloaded. The FinFly-ISP can be integrated into an Internet Provider's network to infect en masse or targeted computers.

FinCrack

Elaman has developed FinCrack – a high-speed supercluster for cracking passwords and hashes. It currently supports password recovery for:

- Microsoft Office Documents
- NTLM/LM – Windows user hashes
- WPA wireless networks
- UNIX DES – Unix password hashes
- WinZip protected files
- PDF password-protected files

Modules for other files and hash types can be provided upon request. The size of the supercluster is completely customized according to the customer's requirements.
The FinCrack will be available at the end of 2008.

FinWifiKeySpy

FinWiFiKeySpy is a device for remotely sniffing keystrokes of commercial wireless keyboards (e.g. Microsoft, Logitech) that are within the Wi-Fi device range (20-50 m). The device also enables the customer to remotely control the wireless keyboard and thus control the target's computer.
The FinWiFiKeySpy will be available at the end of 2008.

FinBluez

Elaman is developing the FinBluez – a product that enables agencies to do various advanced attacks against Bluetooth devices like mobile phones, headsets and computers. For example, FinBluez is able to record the audio stream between a headset and a mobile phone or utilize common Bluetooth headsets as audio bugs.
More information coming soon! The FinBluez will be available at the end of 2008.