IT INTRUSION - FinFisher Product Suite
Usage

- Information Gathering
- PC Surveillance
- Hacking
- Information Exploitation
- Information Interception
Components

- FinFisher USB Suite
- FinFisher Remote Hacking Kit
- FinSpy
- FinFly
- FinTraining
- FinAudit
- New Products - 2008
FinFisher USB Suite

- Suite to locally extract information from target systems with little or no user interaction
- Data analysis/Report generation at Headquarters
Components

• **FinFisher USB Suite**
  - FinFisher HQ
  - FinFisher 1
  - FinFisher 2
  - FinFisher 3

• **FinFisher Remote Hacking Kit**

• **FinSpy**

• **FinFly**

• **FinTraining**

• **FinAudit**

• **New Products - 2008**
FinFisher HQ

- Graphical User Interface for FinFisher 1 and 2
- Used to configure operational options
- Generates certificates for encryption
- Deciphers and imports data from dongles
- Generates reports from gathered data
- Updates FinFisher 1 and 2 systems
<table>
<thead>
<tr>
<th>ID</th>
<th>Date</th>
<th>Type</th>
<th>Username</th>
<th>Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>ffa02956</td>
<td>Sat Sep 22 16:04:09 2007</td>
<td>1</td>
<td>MaJoMu</td>
<td>MJM</td>
</tr>
<tr>
<td>ffa00268</td>
<td>Mon Jul 30 10:22:38 2007</td>
<td>1</td>
<td>MaJoMu</td>
<td>MJM</td>
</tr>
</tbody>
</table>
Components

- **FinFisher USB Suite**
  - FinFisher HQ
  - **FinFisher 1**
    - FinFisher 2
    - FinFisher 3
- **FinFisher Remote Hacking Kit**
- FinSpy
- FinFly
- FinTraining
- FinAudit
- New Products - 2008
**FinFisher 1**

- **U3 USB Dongle**
- **Executes on insertion with little or no user intervention**
- **Obtains system and account information for:**
  - Windows Accounts
  - E-Mail Accounts (Microsoft Outlook / Express, ...)
  - Instant Messenger Accounts (MSN, Yahoo, ICQ, ...)
  - System Details (Product Keys, Hotfixes, ...)
  - Network Information (Open Ports, Cookies, History, ...)
- **All gathered data is asymmetrically enciphered**
- **Bypasses installed Anti-Virus/Anti-Spyware software**
Components

- **FinFisher USB Suite**
  - FinFisher HQ
  - FinFisher 1
  - FinFisher 2
  - FinFisher 3
- FinFisher Remote Hacking Kit
- FinSpy
- FinFly
- FinTraining
- FinAudit
- New Products - 2008
FinFisher 2

- U3 USB Dongle
- Executes on insertion with little or no user intervention
- Gets a copy of all locally stored E-Mails from the target system
- Obtains specific files by file-extension (e.g. all .doc and .xls files)
- All gathered data is asymmetrically enciphered
- Bypasses installed Anti-Virus/Anti-Spyware software
FinFisher 2

**Generic Settings**
- Bypass Anti-Virus / Anti-Spyware Tools
- Display Progress During Operation

**E-Mails**
- Outlook / Outlook Express
- Mozilla Thunderbird
- Opera Mail

**Files By Type**
- Activate File Gathering
  - Search All Disks
  - Search %HOMEPATH%
  - Search Location: 
  - File Extensions: `doc; xls`
    
    (separate extensions with ';')

[OK] [Cancel]
Components

- FinFisher USB Suite
  - FinFisher HQ
  - FinFisher 1
  - FinFisher 2
  - FinFisher 3
- FinFisher Remote Hacking Kit
- FinSpy
- FinFly
- FinTraining
- FinAudit
- New Products - 2008
FinFisher 3

- 2 Bootable CD-Roms:
  1. Removes password for selected Windows user account
  2. Securely wipes local hard-disks
Components

- FinFisher USB Suite
- FinFisher Remote Hacking Kit
- FinSpy
- FinFly
- FinTraining
- FinAudit
- New Products - 2008
FinFisher Remote Hacking Kit

- Used for remote information gathering
- Provides up-to-date hacking environment
- Can target public servers and personal computers
FinFisher Remote Hacking Kit

- Ruggedized notebook
- FinTrack operating system
- Various scripts for automating attack procedures
- All major up-to-date hacking tools
FinFisher Remote Hacking Kit

- High-power Wireless LAN adapter
- Bluetooth adapter with antenna plug
- Directional/Omni-directional antenna
- 500 GB USB disk containing Rainbow Tables, default password lists, etc.
- USB-to-Ethernet adapter
- PS/2 and USB Keylogger
- Other
Components

- FinFisher USB Suite
- FinFisher Remote Hacking Kit
- FinSpy
- FinFly
- FinTraining
- FinAudit
- New Products - 2008
FinSpy

- Professional Trojan Horse
- Monitor and remotely access one or multiple systems
- Presence on target system is hidden
- All communication is hidden and enciphered
- Components:
  - FinSpy Client
  - FinSpy Server
  - FinSpy Target
  - FinSpy USB-U3 Dongle (Target)
  - FinSpy Antidote
FinSpy

• Features:
  - Custom Executables
  - Bypasses Anti-Virus/Anti-Spyware Software
  - Location Tracing
  - Scheduled Operations
  - Key Logging
  - Password Gathering
  - Webcam/Microphone Access
  - Communication Sniffing:
    • Skype
    • Instant Messengers (ICQ, Yahoo, ...)
  - Other
Components

- FinFisher USB Suite
- FinFisher Remote Hacking Kit
- FinSpy
- **FinFly**
- FinTraining
- FinAudit
- New Products - 2008
FinFly

- Used to infect executables while downloading
- Components:
  - Transparent HTTP Proxy
  - EXE Loader
- Proxy attaches Trojan Horse software to downloaded executables on-the-fly
- Loader removes attached software from downloaded executable after installation
- Can be used on local networks (e.g. Wireless LANs)
- ISP Version to come in 2008
Components

- FinFisher USB Suite
- FinFisher Remote Hacking Kit
- FinSpy
- FinFly
- **FinTraining**
- FinAudit
- New Products - 2008
FinTraining: Basic Hacking Courses

• 1 or 2 week basic hacking overview
• Covers various common hacking techniques
• Practical examples, demonstrations and exercises
• Topics include:
  - Footprinting/Scanning/Enumeration
  - Networks
  - Exploits
  - Wireless LANs
  - Bluetooth
  - Other
FinTraining Advanced: Exploiting Software

- 1 week course
- Covers bugs in software and exploiting these
- Practical examples, demonstrations and exercises
- Topics include:
  - Software Bugs
  - Exploit Archives/Frameworks
  - Shellcode
  - Finding Bugs
  - Customizing Exploits
  - Other
FinTraining Advanced: Rootkits

- 1 week course
- Covers RootKit and Trojan horse techniques
- Practical examples, demonstrations and exercises
- Topics include:
  - Analysis
  - Usage
  - Detection
  - Development
  - Other
FinTraining Advanced: Hacking VoIP

- 1 week course
- Covers Voice-over-IP eavesdropping and various attack techniques
- Practical examples, demonstrations and exercises
- Topics include:
  - RTP Sniffing
  - RTP Insertion
  - SIP Account Brute-Forcing
  - SIP Account Cracking
  - Other
FinTraining Advanced: Wireless Hacking

- 1 week course
- Covers Wireless LANs, Bluetooth and Wireless Keyboards
- Practical examples, demonstrations and exercises
- Topics include:
  - Wireless LAN WEP/WPA Cracking
  - Bluetooth Link-Key Cracking
  - Wireless Keyboard Sniffing
  - Other
FinTraining Advanced: Covert Comms

- 1 week course
- Covers steganography, encryption, network and application protocols
- Practical examples, demonstrations and exercises
- Topics include:
  - Hiding data in objects
  - Hiding data in streams
  - Hiding VoIP communication
  - Other
FinTraining Advanced: More

- More topics upon request
- Courses are customized according to customers needs and skill-set
Components

- FinFisher USB Suite
- FinFisher Remote Hacking Kit
- FinSpy
- FinFly
- FinTraining
- FinAudit
- New Products - 2008
FinAudit

• 1 or 2 week penetration test
• Security check of networks, systems and software
• Helps analyzing various attack vectors and finding vulnerabilities
• Prevents data disclosure and intrusion
• Finalizing report and consulting services
Components

- FinFisher USB Suite
- FinFisher Remote Hacking Kit
- FinSpy
- FinFly
- FinTraining
- FinAudit
- New Products - 2008
News 2008: FinFly ISP

- FinFly that is capable of working in ISP networks
- Can infect en-masse or targeted systems
- Ready: Mid/End of 2008
News 2008: FinCrack

- Super-Cluster to crack Passwords/Hashes
- Size and Speed customized to requirements
- Supports:
  - Microsoft Office Documents
  - NTLM/LM
  - WPA Networks
  - Unix DES
  - WinZIP
  - PDF
- Other modules can be provided upon request
- Ready: Mid/End of 2008
News 2008: FinWifiKeySpy

- Wireless Keyboard Sniffer
- Sniffs all keystrokes of wireless keyboard within antenna range
- Able to inject keystrokes to remote computers
- Supports all major vendors (Microsoft, Logitech)
- Ready: End of 2008
News 2008: FinBluez

• Product for various Bluetooth attacks, e.g.:
  - Utilize Bluetooth headsets as audio bugs
  - Record audio stream between headset and mobile phone
• Ready: End of 2008