Wi-Fi Malware for Fun and Profit

Vivek Ramachandran
Founder, SecurityTube.net
Who am I? (Shameless Self Promotion)

- 802.1x Cat6k, Cisco
- Broke WEP Cloaking (Defcon 15)
- Caffe Latte Attack (Toorcon 9)
- Microsoft Security Shootout
- “Backtrack 5 Wireless Penetration Testing” published
www.SecurityTube.net

http://www.securitytube.net/downloads

©SecurityTube.net
Software Requirements

• Windows 7 laptop with in-built Wi-Fi or external adapter
• Backtrack >= 4 in Virtualbox
• External USB card capable of Packet Injection

If you do not have all / part of the setup, you can still follow the class
Agenda

• Wireless Client Behavior
• Software Access Points
  – Linux
  – Windows
• Abusing Windows Soft Access Points
  – Backdoors
  – Worms and Botnets
• Future Roadmap

©SecurityTube.net
Background – Understanding Wi-Fi Client Software

- Allows Client to connect to an Access Point

- First time user approves it, Auto-Connect for future instances

- Details are stored in Configuration Files
Understanding Wi-Fi Clients

• Scanning the air for stored profiles
• Profiling the clients based on searches
• Different clients behave differently

• Demo
See All Wi-Fi Interfaces

Netsh wlan show interfaces
## Drivers and Capabilities

```
C:\Windows\system32>netsh wlan show drivers

Interface name: Wireless Network Connection

<table>
<thead>
<tr>
<th>Driver</th>
<th>D-Link DWA-125 Wireless N 150 USB Adapter&lt;rev.A2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td>D-Link Corporation</td>
</tr>
<tr>
<td>Provider</td>
<td>D-Link Corporation</td>
</tr>
<tr>
<td>Date</td>
<td>10/15/2009</td>
</tr>
<tr>
<td>Version</td>
<td>3.0.7.0</td>
</tr>
<tr>
<td>INF file</td>
<td>C:\Windows\INF\oem2.inf</td>
</tr>
<tr>
<td>Files</td>
<td>4 total</td>
</tr>
<tr>
<td></td>
<td>C:\Windows\system32\DRIVERS\Dnetr28u.sys</td>
</tr>
<tr>
<td></td>
<td>C:\Windows\system32\drivers\wifibus.sys</td>
</tr>
<tr>
<td></td>
<td>C:\Windows\system32\RaCoInst.dll</td>
</tr>
<tr>
<td></td>
<td>C:\Windows\system32\RaCoInst.dat</td>
</tr>
<tr>
<td>Type</td>
<td>Native Wi-Fi Driver</td>
</tr>
<tr>
<td>Radio types supported</td>
<td>802.11b 802.11g 802.11n</td>
</tr>
<tr>
<td>FIPS 140-2 mode supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Hosted network supported</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication and cipher</td>
<td>Open     None</td>
</tr>
<tr>
<td>supported in infrastructure</td>
<td>Open     WEP-40bit</td>
</tr>
<tr>
<td>mode:</td>
<td>Open     WEP-104bit</td>
</tr>
</tbody>
</table>
```

Netsh wlan show drivers
Scan for Available Networks

```
C:\Windows\system32>netsh wlan show networks

Network interface: Wireless Network Connection
There are 3 networks currently visible.

SSID 1:
  Network type: Infrastructure
  Authentication: WPA2-Enterprise
  Encryption: CCMP

SSID 2: Sen_Biac
  Network type: Infrastructure
  Authentication: WPA2-Personal
  Encryption: CCMP

SSID 3: TELENETHOTSPOT
  Network type: Infrastructure
  Authentication: Open
  Encryption: None
```

Netsh wlan show networks
View Existing Profiles

Netsh wlan show profiles
Starting a Profile

Netsh wlan connect name="vivek"
Netsh wlan export profile name="vivek"
Creating an Access Point on a Client Device

- Requirement for special drivers and supported cards
- Custom software used – HostAPd, Airbase-NG
- More feasible on Linux based systems
Linux Soft AP

- Airbase-NG
- HostAPd
- ...

©SecurityTube.net
Available Windows 7 and Server 2008 R2 onwards

Virtual adapters on the same physical adapter

SoXAP can be created using virtual adapters

– DHCP server included

“With this feature, a Windows computer can use a single physical wireless adapter to connect as a client to a hardware access point (AP), while at the same time acting as a software AP allowing other wireless-capable devices to connect to it.”

Feature Objective

• To allow creation of a wireless Personal Area Network (PAN)
  – Share data with devices

• Network connection sharing (ICS) with other devices on the network
Demonstration

Demo of Hosted Network
Creating a Hosted Network

```
C:\Windows\system32> netsh wlan set hostednetwork mode=allow ssid=WickedNetworkKey
The hosted network mode has been set to allow.
The SSID of the hosted network has been successfully changed.
The user key passphrase of the hosted network has been successfully changed.

C:\Windows\system32>
C:\Windows\system32> netsh wlan start hostednetwork
The hosted network started.
```

©SecurityTube.net
Client still remains connected to hard AP!
Wi-Fi Backdoor

• Easy for malware to create a backdoor
• They key could be:
  – Fixed
  – Derived based on MAC address of host, time of day etc.
• As host remains connected to authorized network, user does not notice a break in connection
• No Message or Prompt displayed
Understanding Rogue Access Points

Rogue AP
Makes a Rogue AP on every Client!
Best Part – No Extra Hardware!
Advantages?
Advantages?
Why is this cool?

• Victim will never notice anything unusual unless he visits his network settings
  – has to be decently technical to understand

• Attacker connects to victim over a private network
  – no wired side network logs: firewalls, IDS, IPS
  – Difficult, if not impossible to trace back
  – Difficult to detect even while attack is ongoing 😊

• Abusing legitimate feature, not picked up by AVs, Anti-Malware

• More Stealth? Monitor air for other networks, when a specific network comes up, then start the Backdoor
Chaining Hosted Networks like a proxy?

- Each node has client and AP capability
- We can chain them to “hop” machines
- Final machine can provide Internet access
- Like Wi-Fi Repeaters
Package Meterpreter for full access?

• Once attacker connects to his victim, he would want to have access to everything

• Why not package a Meterpreter with this? 😊

• How about a Backdoor post-exploitation script for Metasploit? 😊
Coupling Hosted Network with Metasploit
Increasing Stealth

- Passive Monitoring for SSIDs available

- Trigger SSID causes Wicked Hosted Network to start and create application level backdoor

- Attacker connects and does his job

- Shuts off Trigger SSID and Malware goes to Passive Monitoring again
Victim connects by mistake or misassociation
Victim opens browser, Metasploit Browser_Autopwn exploits the system
Hacker gets access!

Biggest Challenge – Victim notices he is connected to the wrong network and disconnects himself
Enhancing Karmetasploit

- Upon Exploitation, create the hosted network backdoor
- User disconnects, but this hosted network still remains active
- Attacker connects via this network
What about older clients and other OSs?

- Windows < 7, Mac OS do not have the Hosted Network or alike feature
  - Use Ad-Hoc networks
  - Use Connect Back mechanism 😊
    - When a particular SSID is seen, connect to it automatically
    - Blurb reporting “Connected to ABC”
      - Could we kill it? 😊
Dissecting Worm Functionality

Propagation Technique

Exploit

Worm
Hosted Network Encryption

• Uses WPA2-PSK for encryption
• Key is encrypted in configuration file
• Can be decrypted 😊

• What if there is an office network configured on the same machine with WPA2-PSK?
1. Infect Authorized Computer and Decrypt Passphrase
Alternate – Dump and Copy

C:\Users\vivek\Desktop\demo>netsh wlan export profile name=OfficeAP
Interface profile "OfficeAP" is saved in file "C:\Wireless Network Connection-OfficeAP.xml" successfully.

C:\Users\vivek\Desktop\demo>netsh wlan export hostednetworkprofile
Profile to connect to the hosted network is saved successfully in file "HostedNetwork.xml".

C:\Users\vivek\Desktop\demo>
C:\Users\vivek\Desktop\demo>
C:\Users\vivek\Desktop\demo>
2. Create a Soft Access Point with the same Credentials
3. Signal Strength Game

OfficeAP

Worm Infected Laptop

OfficeAP
4. Hop and Exploit

OfficeAP

Exploit

©SecurityTube.net
5. Replicate and Spread
Worms Wi-Fi Network Signal Strength > AP

OfficeAP

OfficeAP

OfficeAP

OfficeAP
Wi-Fi Worm

• Retrieve the network key for the network
• Create a hosted network with the same name
• When the victim is in the vicinity of his office, worm can be activated
• At some point the signal strength may be higher than real AP
• Other colleagues laptops may hop and connect
  – Conference rooms, Coffee and Break areas
Why is this interesting?

- Worm uses its own private Wi-Fi network to propagate

- Does not use the Wired LAN at all

- Difficult for network defenses to detect and mitigate 😊

- Targeted APT against an Enterprise
## APIs for the Hosted Network Feature

<table>
<thead>
<tr>
<th>Functions used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WlanHostedNetworkForceStart, WlanHostedNetworkStartUsing</strong></td>
<td>Start the wireless Hosted Network.</td>
</tr>
<tr>
<td><strong>WlanHostedNetworkForceStop, WlanHostedNetworkStopUsing</strong></td>
<td>Stop the wireless Hosted Network.</td>
</tr>
<tr>
<td><strong>WlanHostedNetworkInitSettings, WlanHostedNetworkSetSecondaryKey,</strong></td>
<td>Configure wireless Hosted Network settings (change the SSID, change the</td>
</tr>
<tr>
<td><strong>WlanHostedNetworkRefreshSecuritySettings</strong></td>
<td>secondary key, or request that the primary key is regenerated).</td>
</tr>
<tr>
<td><strong>WlanHostedNetworkQueryStatus,</strong></td>
<td>Query the wireless Hosted Network settings and information (status, SSID,</td>
</tr>
<tr>
<td><strong>WlanHostedNetworkQuerySecondaryKey,</strong></td>
<td>secondary key, primary key, or a list the devices currently connected).</td>
</tr>
<tr>
<td><strong>WlanHostedNetworkQueryProperty</strong></td>
<td></td>
</tr>
</tbody>
</table>
DVD Contents

WLAN Megaprimer Video List

- Megaprimer Home
- Part 1: Getting Started
- Part 2: Bands, Channels And Sniffing
- Part 3: Pwning Beacon Frames
- Part 4: Dissecting Ap-Client Connections
- Part 5: Dissecting Wlan Headers
- Part 6: Pwning Beacon Frames
- Part 7: Laughing Off Mac Filters
- Part 8: Hacking Wlan Authentication
- Part 9: Hotspot Attacks
- Part 10: Hacking Isolated Clients
- Part 11: Alfa Card Kung-Fu
- Part 12: Man-In-The-Middle Attack
- Part 13: SSL Man-In-The-Middle Attacks
- Part 14: Wep In-Depth
- Part 15: Wep Cracking
- Part 16: Caffe Latte Attack Basics
- Part 17: Caffe Latte Attack Demo
- Part 18: Koreks Chopchop Attack
- Part 19: Fragmentation And Hirte Attack
- Part 20: Understanding WPA/WPA2
- Challenge 1: There Is No Patch For Stupidity
- Challenge 1 Solution
- Challenge 2: Know Thy Packets
- Challenge 2 Solution: Know Thy Packets
- Challenge 3: Never Underestimate Your Enemy
- Challenge 3 Solution: Never Underestimate Your Enemy
- Part 21: WPA-PSK
- Part 22: WPA-PSK Cracking
- Part 23: WPA2-PSK Cracking
- Part 24: Speeding Up WPA/WPA2 PSK Cracking
- Part 25: Mood Swings Of A Wandering Client
- Part 26: Cracking WPA/WPA2-PSK With Just The Client
- Part 27: Questions And Answers
- Part 28: WPA_Supplicant
- Part 29: Setting Up Freeradius-WPE On Backtrack
- Part 30: EAP-MD5 Basics And Demo
- Part 31: Cracking EAP-MD5 With EAPMD5Pass And EAPMD5Crack
- Part 32: EAP Types And PEAP Demo
- Part 33: Cracking PEAP
- Part 34: Cracking PEAP In A Windows Network
- Part 35: Cracking EAP-TTLS
- Part 36: Insecurity In 3rd Party Wi-Fi Utilities
- Conclusion And The Road Ahead

http://www.securitytube.net/downloads

©SecurityTube.net
Questions?

Questions