



Tool Talk: Jasager and Karmetasplit

By: Matthew Neely

Presented: April 15th 2009 at NEO InfoSec Forum



- Matt Neely CISSP, CTGA, GCIH, GCWN - Manager of the Profiling team at SecureState:
 - Areas of expertise include: wireless security, penetration testing, physical security, security convergence and incident response
 - 10 years of security experience
 - Presented at DEFCON 13 and ShmooCon 2009
- Outside of work:
 - Co-host of the Security Justice Podcast
 - Board member for the North Eastern Ohio Information Security Forum



- Introduction to WZC Service
- Karma and Jasager
- Karmetasplit
- Questions/Open Discussion

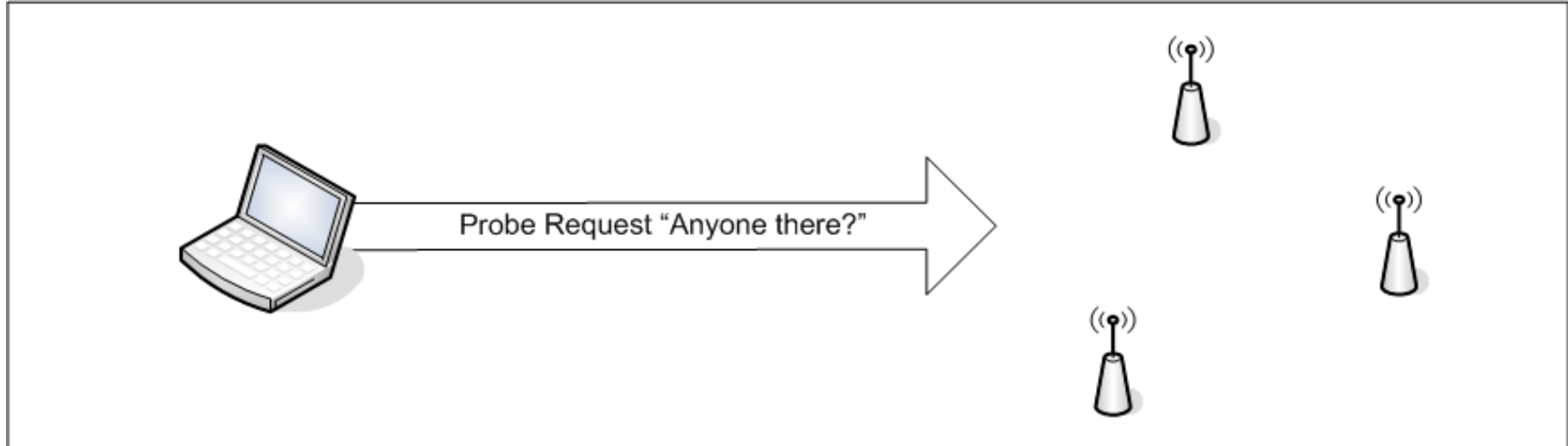


- Windows Zero Configuration Service: A service used to make sure the NIC gets the “right” SSID, authentication mode, encryption keys and encryption mode.
 - Does not select the AP.
 - Does not take into account signal strength.
- Alternate name: Windows XP Wireless Auto Configuration (WZCSVC).
- Different from third party configuration utilities shipped with some cards.



WZC Process: Step 1

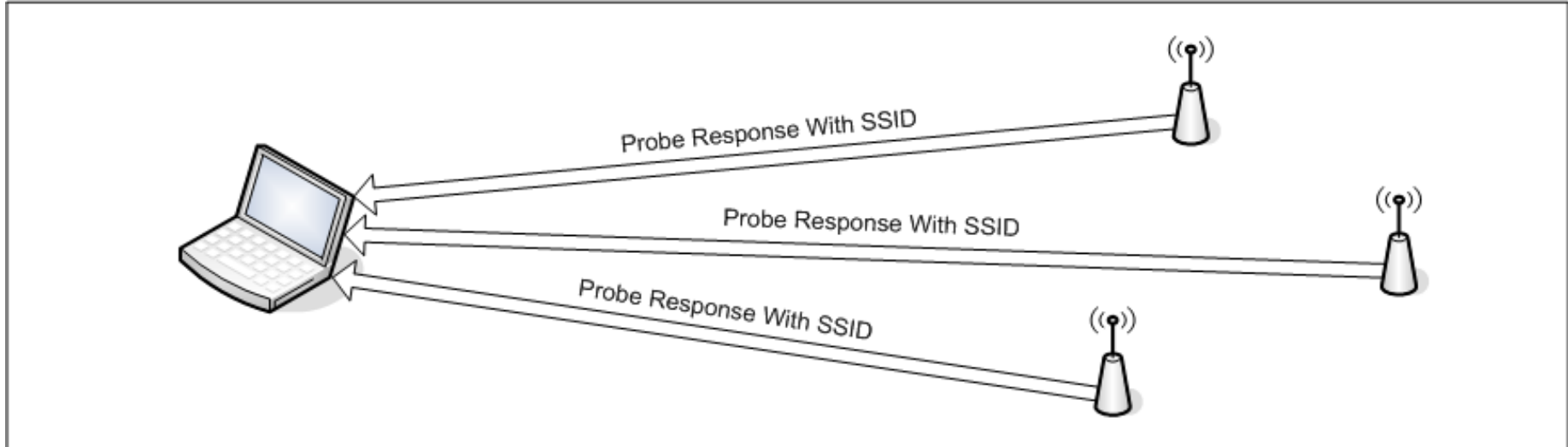
- Client sends a broadcast Probe Request on each channel and creates a list of available networks.





WZC Process: Step 2

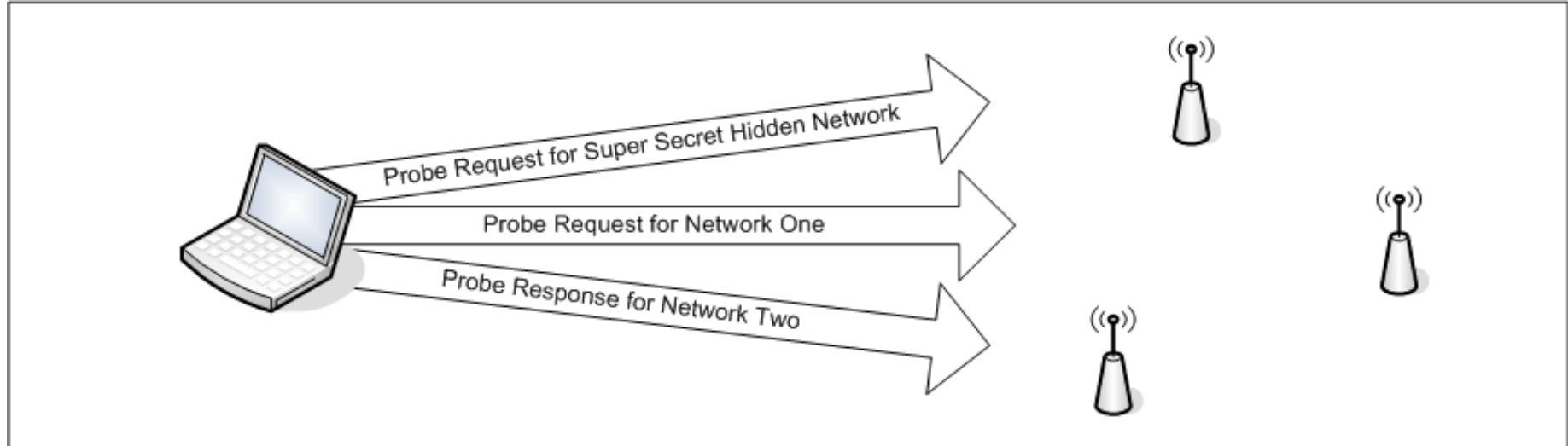
- Access points within range respond with Probe Response packets.
- If Probe Responses are received from networks on the Preferred Network List (PNL) the client connects to them in PNL order.





WZC Process: Step 3

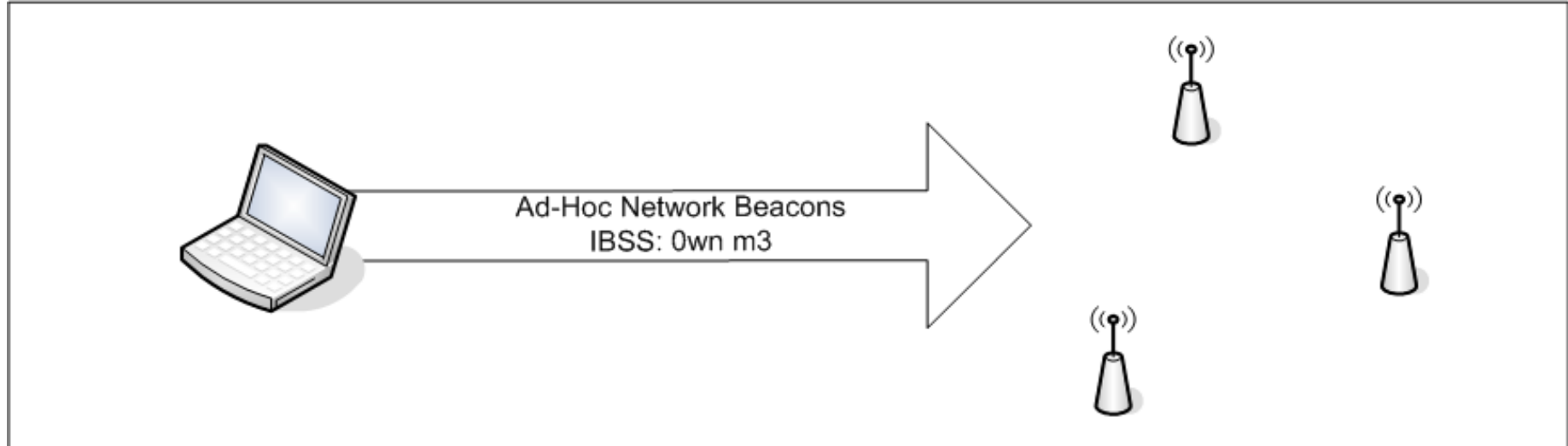
- If no available networks on the PNL respond, specific Probe Requests are sent for each preferred network in case they are “hidden”





WZC Process: Step 4

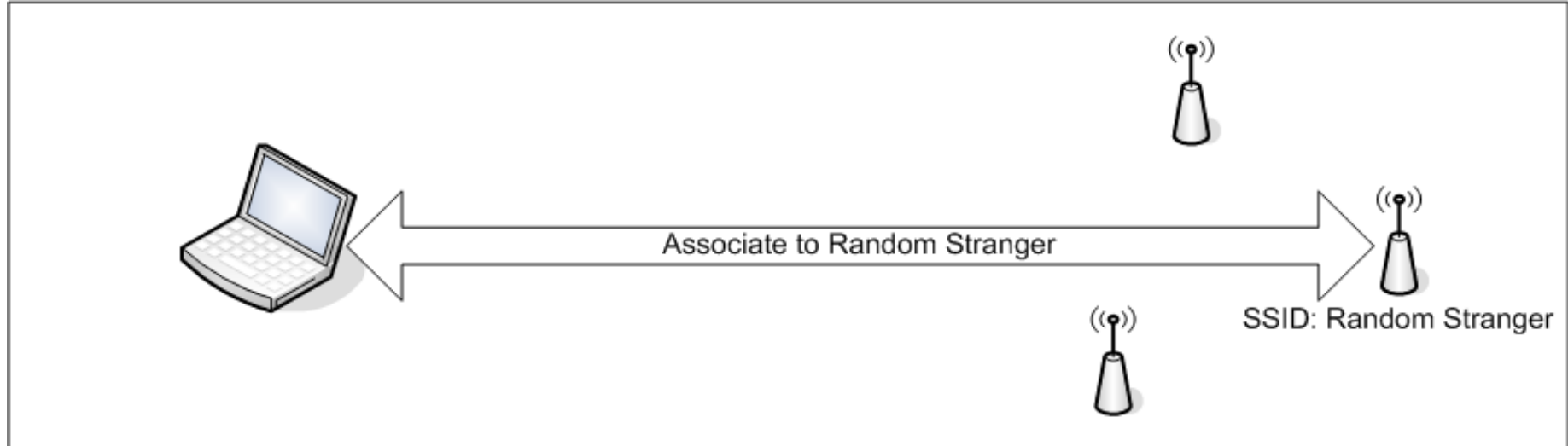
- If client is not associated and there is an ad-hoc network on the PNL the client will:
 - Establishes the ad-hoc network
 - Becomes the first node
 - Begins sending beacon packets
- Self-assigns an IP address in the Windows Automatic Private Address range of 192.168.0.0/16





WZC Process: Step 5

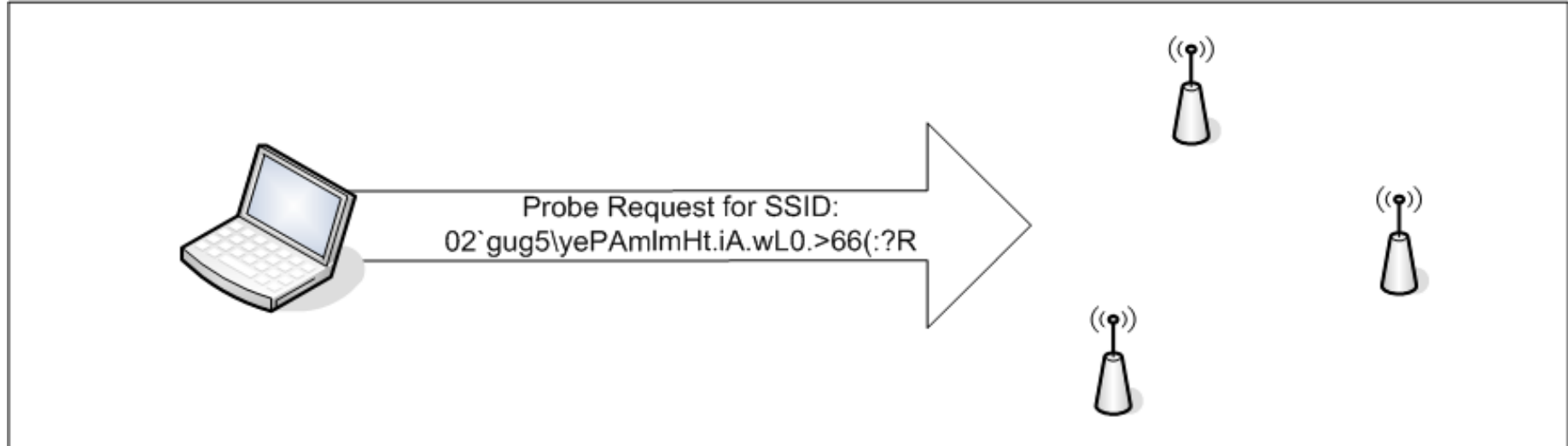
- If “Automatically connect to a non-preferred networks” is enabled (disabled by default) the client connects to any network in the order in which they are detected.





WZC Process: Step 6

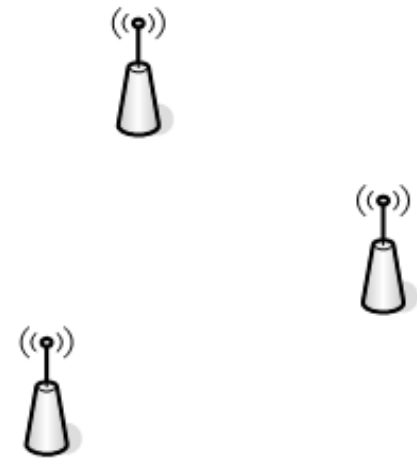
- If not in ad-hoc mode or associated to a network, Windows sets the NIC to Infrastructure mode and assigns a random 32 character SSID.
- Probe Requests are sent to look for this network.
- Also occurs if the PNL is empty.





WZC Process: Step 7

- WZC sleeps for 60 seconds
- Algorithm restarts





Once WZC Selects an SSID

- SSID is sent to the NIC.
- NIC decides which AP with select SSID to connect.
- Algorithm used to pick the AP is dependant on drivers and firmware.
 - Usually determined by signal strength, speed and stability.



- Attacker creates a fake AP with a common SSID or creates an AP that will reply to any SSID probe.
 - If the client is looking for SSID “default” the AP will appear to have an SSID of “default” to that client.
 - Simplifies the random SSID attack.
 - Any un-encrypted network in the PNL will connect to the AP.
- Tools:
 - Karma
 - Jasage – Karma for embedded devices
 - Airbase-ng



KARMA DEMO



- Collection of tools designed to launch client-side attacks against wireless users.
- Commonly used to exploit vulnerabilities in Internet Explorer.
- Performed by combining the following tools:
 - Karma or Airbase-ng
 - DHCP server
 - Metasploit



DEMO



DEFENSE



- Apply all patches quickly.
- Run Anti-Virus software and keep definitions up to date.
- Run a spyware protection package and update regularly.
- Have users login with a non-administrative level account.
- Encrypt sensitive data on the drive.
- Disable filesharing.



Wireless Specific Protection

- Safe wireless habits.
- Deploy a 802.11 aware personal firewall or security aware connection manager.
- Only keep secure networks on the PNL.



- Turn off wireless when not in use
- Do not form or connect to ad-hoc networks
 - Can be enforced through group policy
- Remove networks from the PNL when the session is complete
- Use a VPN when accessing sensitive data
- If a VPN is not available
 - Use HTTPS when logging in or sending sensitive information
 - “Look for the lock”
 - Select a secure login connection
- Do not accept invalid certificates



Personal Firewall & Connection Manager

- If possible, select a personal firewall with an integrated connection manager.
- If not, enable a separate firewall and connection manager.
 - Test for interoperability
- Features to look for:
 - Prevents ad-hoc network
 - Limits what SSIDs a user can connect to:
 - Only allows connections to authorized SSIDs of encrypted networks.
 - Disables wireless network card when on a wired network.
 - Prevents network bridging.
 - Only allows “secure” networks in the Preferred Network List.
 - Ability to block client-to-client connections:
 - Only allows traffic to and from the AP.
 - Ability to block inbound and outbound traffic.
 - Easy central management.
- Example:
 - * Example does not imply endorsement
 - Personal or Enterprise versions of “AirDefense”
 - ZoneAlarm’s Wireless PC Protection



- Startup script to turn off wireless.
- Script to remove insecure networks from the PNL on shutdown or startup.
- Script to remove all networks from the PNL so only GPO networks are listed.
- Insert a long SSID into the PNL and monitor for an AP with this SSID.
- Working on getting example scripts available to the public.



NEXT MONTH: MORE FUN WITH FONTS!

QUESTIONS?

More Information:

www.SecureState.com

www.matthewneely.com

mneely@securestate.com