

# Enterprise Wi-Fi Worms, Backdoors and Botnets for Fun and Profit

Vivek Ramachandran

Founder, SecurityTube.net

**SECURITYBYTE**

CONFERENCE & WORKSHOPS

2011

# Who am I?



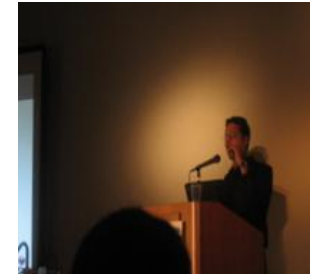
B.Tech, ECE  
IIT Guwahati



802.1x, Cat65k  
Cisco Systems



WEP Cloaking  
Defcon 19



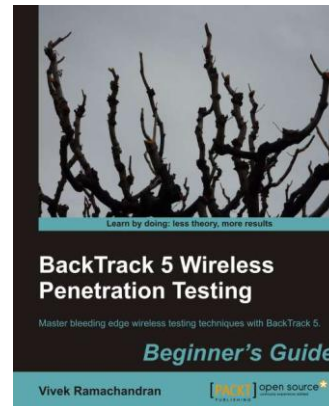
Caffe Latte Attack  
Toorcon 9



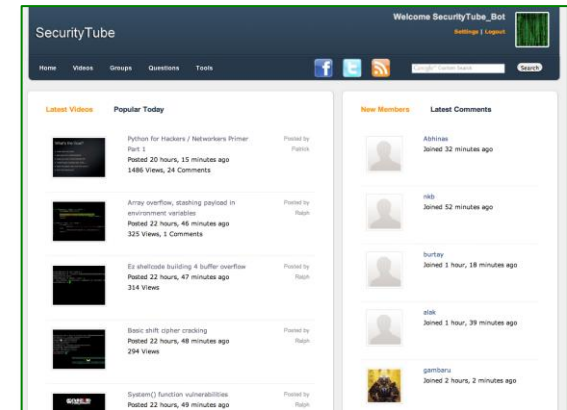
Media Coverage  
CBS5, BBC



Microsoft  
Security Shootout

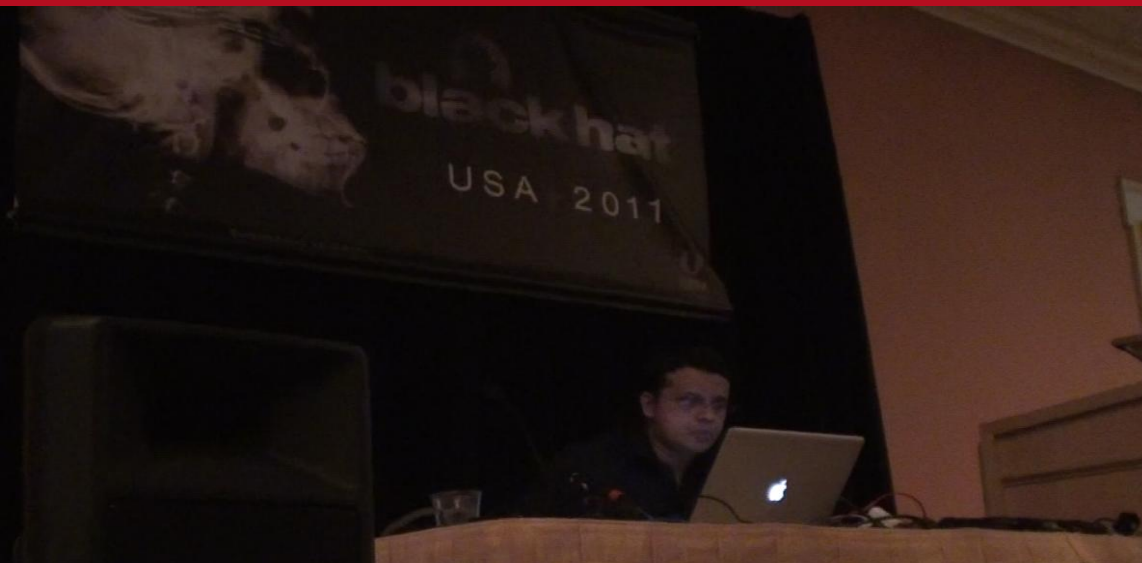


Sept, 2011



SecurityTube.net

# Focus on R&D



# Security Research at Hacker Cons in 2011



August, Las Vegas



August, Las Vegas



Sept, Belgium



Sept, Hungary



October, MIT, Boston



Oct, Switzerland



Oct, Kentucky, USA



August, UK



Nov, Columbia



HITB, Malaysia

**SECURITYBYTE**  
CONFERENCE & WORKSHOPS

2011



# Objective

- How Malware could leverage Wi-Fi to create
  - Backdoors
  - Worms
  - Botnets

# 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

# 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

## Generation 2.0 of Client Software – Hosted Network

- Available Windows 7 and Server 2008 R2 onwards
- Virtual adapters on the same physical adapter
- SoftAP 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.”*

<http://msdn.microsoft.com/en-us/library/dd815243%28v=vs.85%29.aspx>

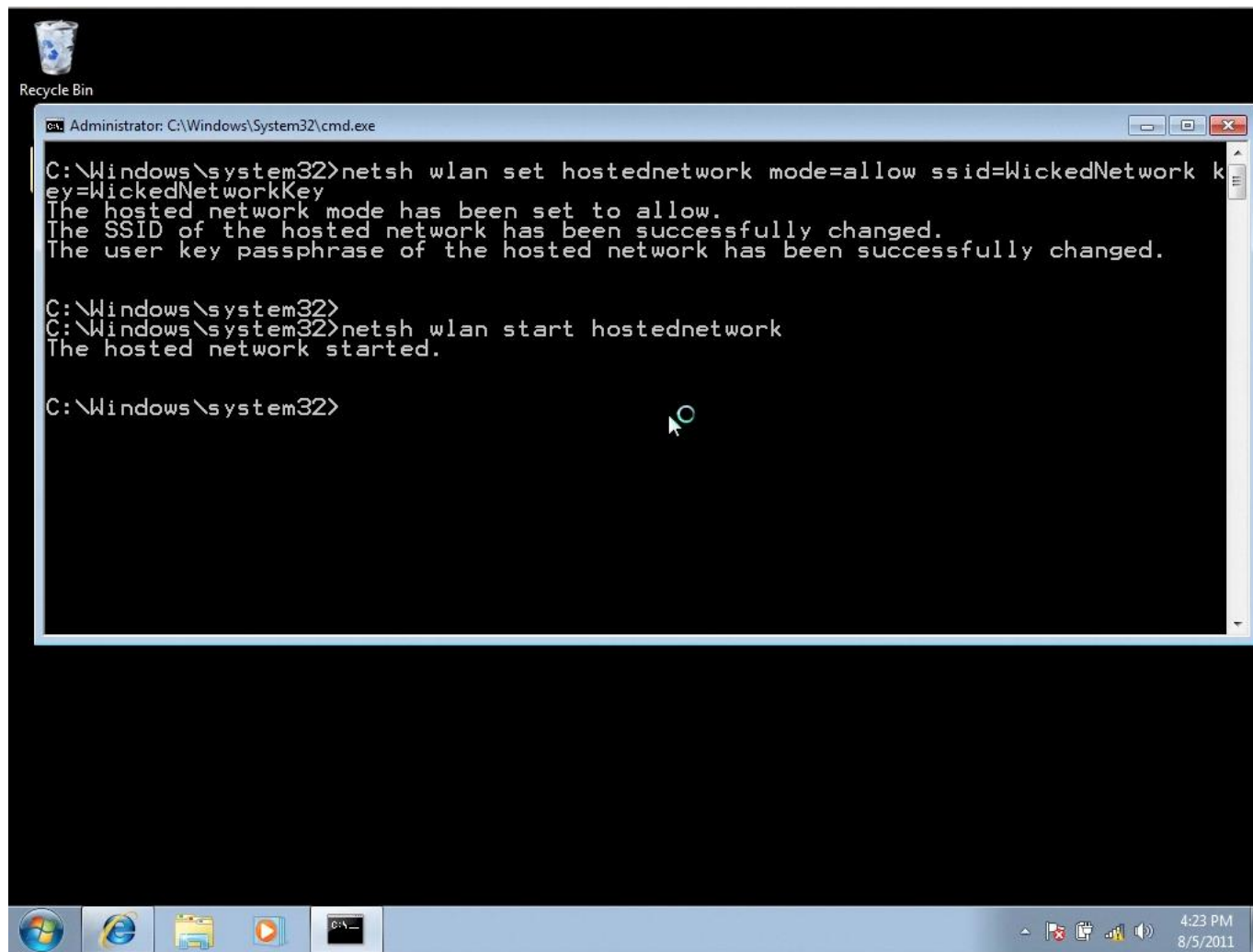


## Feature Objective

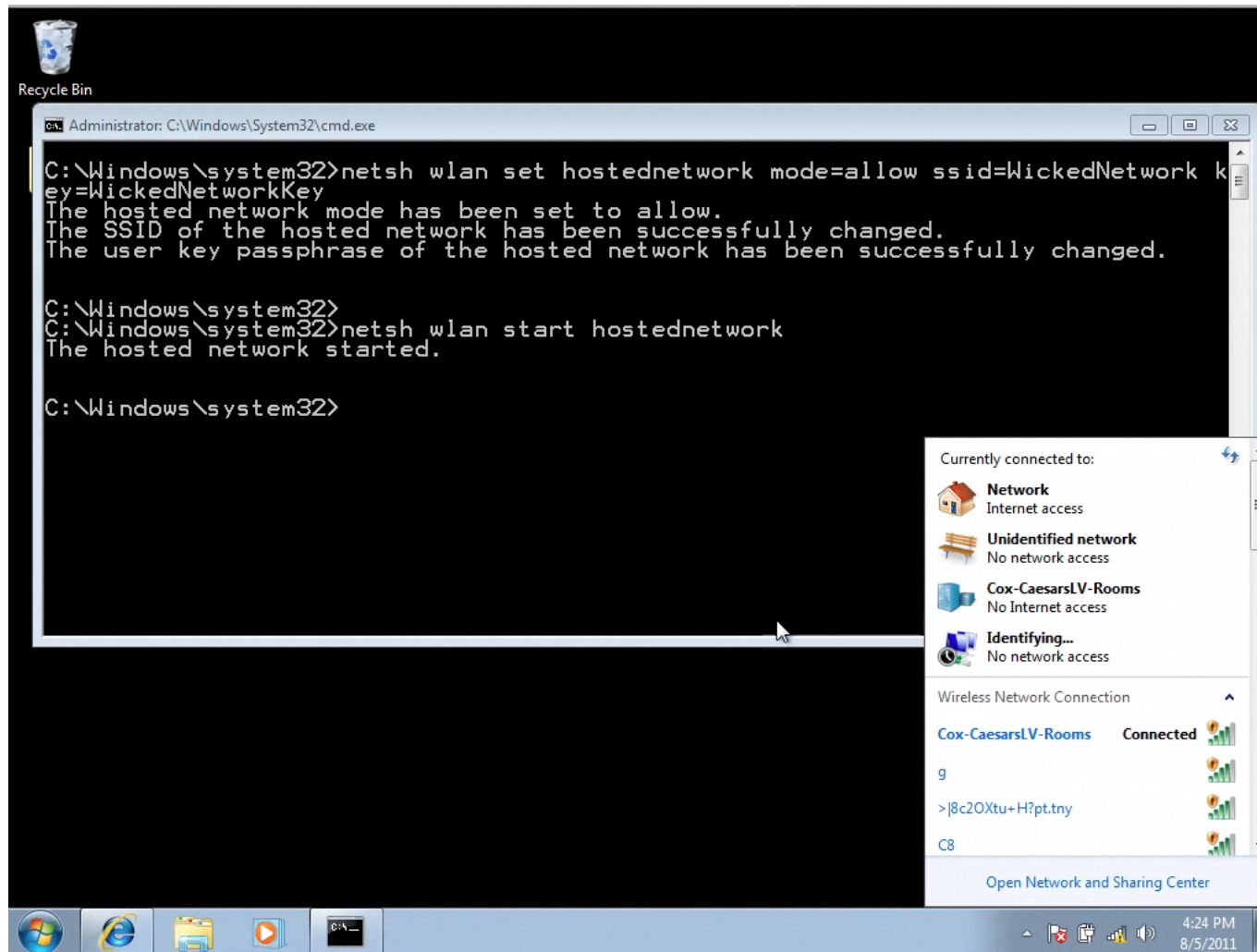
- To allow creation of a wireless Personal Area Network (PAN)
  - Share data with devices
- Network connection sharing (ICS) with other devices on the network

## Demo of Hosted Network

# Creating a Hosted Network



# Client still remains connected to hard AP!



## Hosted Network Feature – key points

1. Can connect to an authorized access point
2. Can create a software based access point on the same card
3. The connection in (1) remains unaffected
4. Physical Adapter multiplexes between both the connections

# Wi-Fi Backdoor

- Easy for malware to create a backdoor
- The 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



# 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 over to victim over a private network
  - Difficult if not impossible to trace back
  - Difficult 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

## 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

# 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?



# 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

# Replication

- Can breaking into the victim
  - Using a Zero Day ; Browser Autopwn
  - using social engineering ; Java applet etc.
- Create the same network
- As more and more get infected, the worm Wi-Fi network gets stronger 😊
  - More fall victim to the same

## Why is this interesting?

- Worm uses its own private Wi-Fi network to propagate
- Difficult for network defenses to detect and mitigate 😊

# APIs for the Hosted Network Feature

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

Questions?