RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

the adventures of alice & bob

Wireless Vulnerabilities in the Wild: View From the Trenches

Speaker：Gopinath KN
Job Title：Director, Engineering
Company Name：AirTight Networks

Agenda

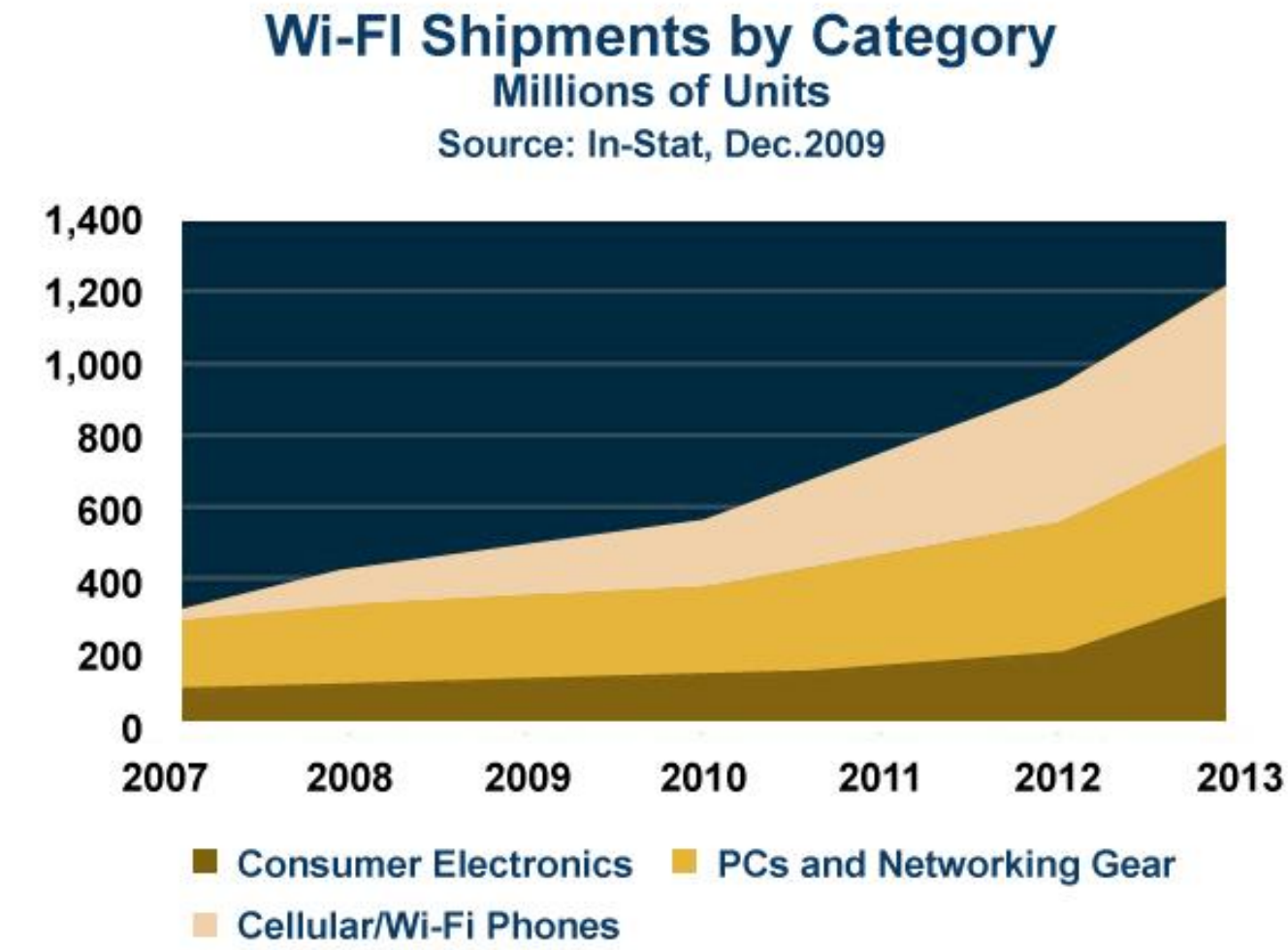
Why care about Wireless Vulnerabilities? (Motivation)

What's new in this talk and what are its implications?

Wireless Vulnerability Analysis (Measurements)

Threat/Vulnerability Mitigation

Era of Wireless Consumerization



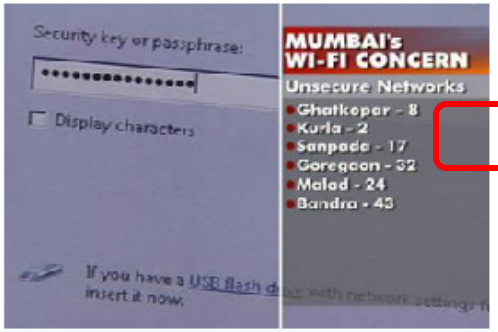
THE WALL STREET JOURNAL

Wifi networks remain to stay insecure in Mumbai

George Koshy , CNN-IBN
Posted on Sep 29, 2008 at 09:06am IST

Recommend | Sign Up to see what your friends recommend.

Share | 0 tweets | tweet



Click to play video

Mumbai: Convenience and ease have helped in introducing newer technologies in the country but if wifi networks are to stay so would their vulnerabilities.

Three instances in Mumbai – the wifi network of Kenneth Haywood, an American national, was used to sent a mail post for Ahmedabad blasts; from Khalsa college in Central Mumbai a terror e-mail was sent to country's media organisation and later the wifi of an engineering company in Chembur was used to sent an e-mail immediately after Delhi serial blasts – have already indicated the vulnerability of wifi networks.

And in all these instances the owners of the networks have been clueless about the hacking.

Paul, Minn

According to the court document, the hackers allegedly stole more than 130 million credit and debit card numbers (.pdf) from Heartland and Hannaford combined. Prosecutors say they believe these breaches constitute the largest data-breach and identity-theft case ever prosecuted in the United States. They're investigating other breaches and have not ruled out Gonzalez's involvement in even more intrusions.

cked via

TIX

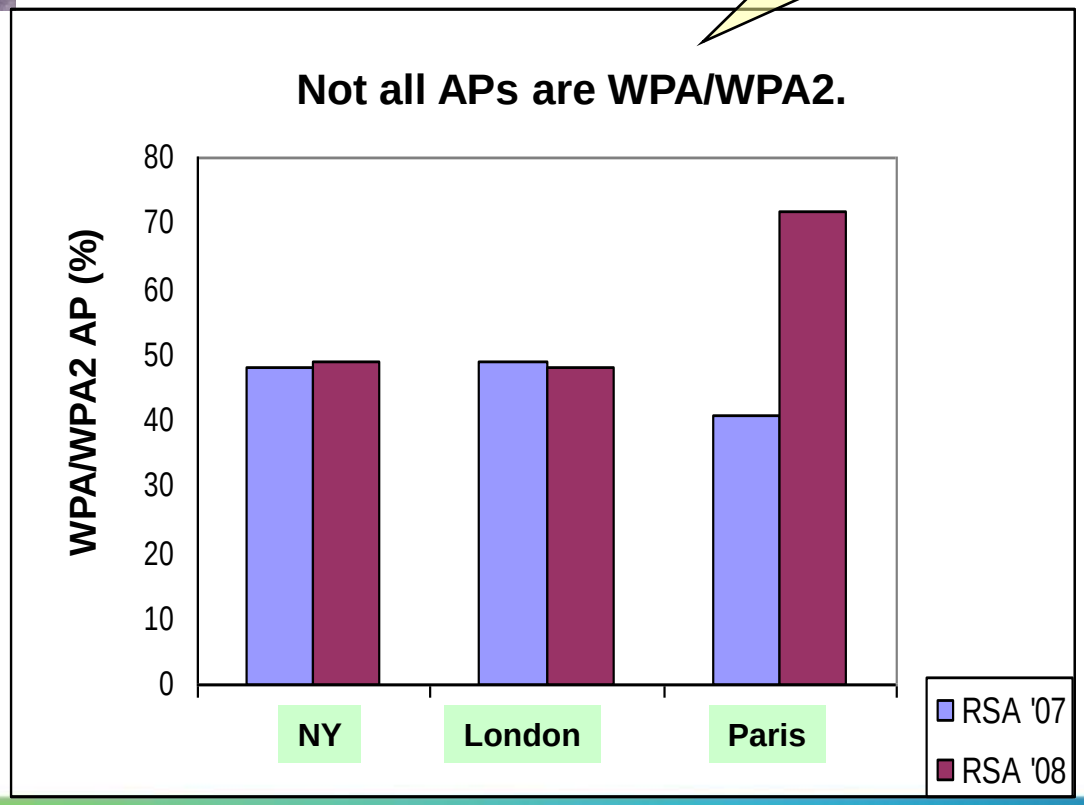
s

it

Are today’s enterprises secure enough to prevent the recurrence of such attacks?

Enter War Driving

How many of these are *actually* connected to my network?



War Driving Insufficient for Enterprise Threat Classification

MAC	SSID	Enc...
000FCC5AE59C	BPMVR	WEP
001C106C6928	zguest	
0019A9A7C131	gear6-guest	
0030AB1EF491	nothere	WEP
001C106C63D8	zguest	
000D9714A632	GoogleWiFiSecure	WEP
000D9704A632	GoogleWiFi	
0018F8A2595C	meeting	WEP
001D7E9ADB88	earth	WEP
000D97140B89	GoogleWiFiSecure	WEP
000D97040B89	GoogleWiFi	
000F66E8242D	Corp	WPA
000D9704845E	GoogleWiFi	
00119334BE90	Netgear102	WEP
000D9714845E	GoogleWiFiSecure	WEP
00237521D0C0	1037 1665	WEP
000FCCFEE1C0	7756 7014	WEP
001195E0F2D8	matissenetg	WPA2
001E5823BF27	matisseguest	WEP
00121762B57D	linksys-g	
000D0B2B0C1B	spectra	WEP
004005BECC17	dlink614	WEP
0014BFF480E8	Alice	WEP
001EE5F30E03	SIT Network	WEP
0020A6534D1C	anw	WPA2

Our Study

MAC	SSID	Enc...
000FCC5AE59C	BPMVR	WEP
001C106C6928	zguest	
0019A9A7C131	gear6-guest	
0030AB1EF491	nothere	WEP
001C106C63D8	zguest	
000D9714A632	GoogleWiFiSecure	WEP
000D9704A632	GoogleWiFi	
0018F8A2595C	meeting	WEP
001D7E9ADB88	earth	WEP
000D97140B89	GoogleWiFiSecure	WEP
000D97040B89	GoogleWiFi	
000F66E8242D	Corp	WPA
000D9704845E	GoogleWiFi	
00119334BE90	Netgear102	WEP
000D9714845E	GoogleWiFiSecure	WEP
00237521D0C0	1037 1665	WEP
000FCCFEE1C0	7756 7014	WEP
001195E0F2D8	matissenetg	WPA2
001E5823BF27	matisseguest	WEP
00121762B57D	linksys-g	
000D0B2B0C1B	spectra	WEP
004005BECC17	dlink614	WEP
0014BFF480E8	Alice	WEP
001EE5F30E03	SIT Network	WEP
0020A6534D1C	anw	WPA2

Authorized

External

Rogue

Sensor Based Statistical Sampling

Data collected over last two years

Total Number of	**Count**
Sites/Locations	2,155
Organizations	156
Sensors	4501
Total Access Points	268,383
Enterprise Clients	427,308
Threat Instances Analyzed	82,681

268,383 APs

Authorized

External/ Unmanaged

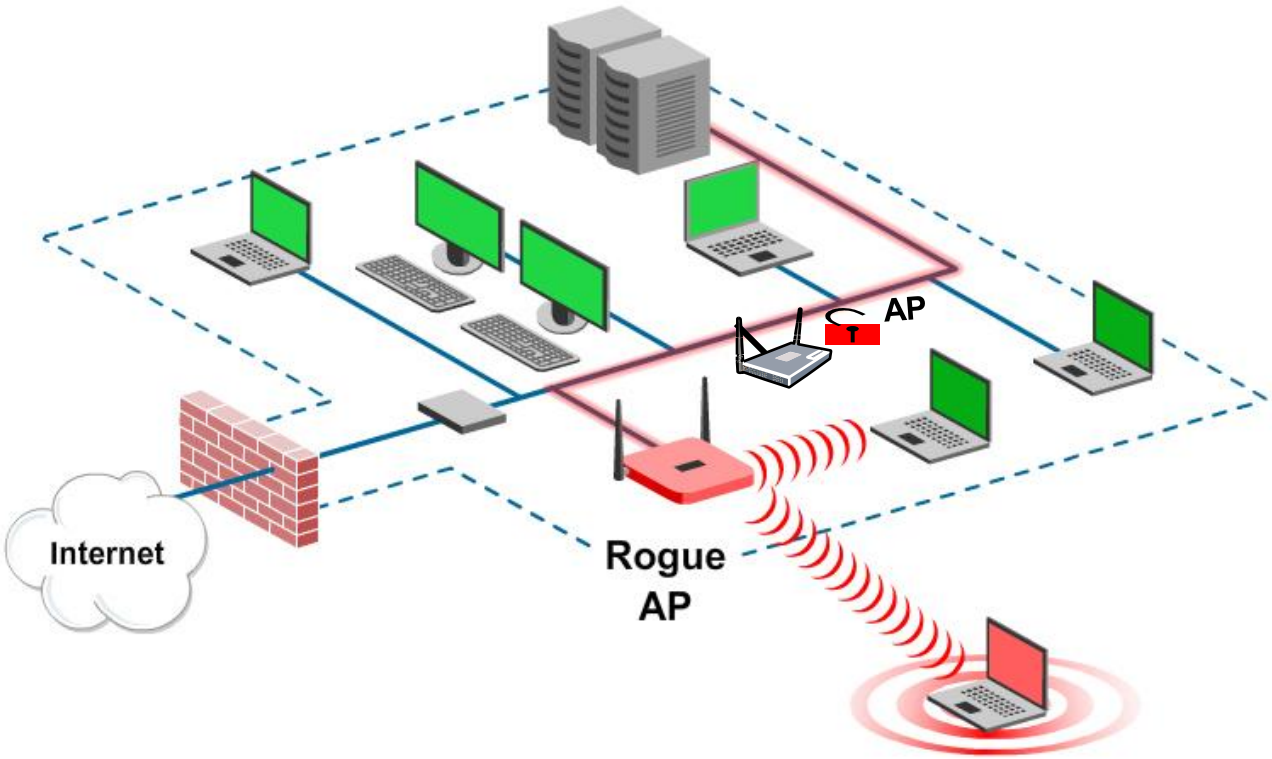
80,515

187,868

70% APs do NOT belong to the studied Organizations!

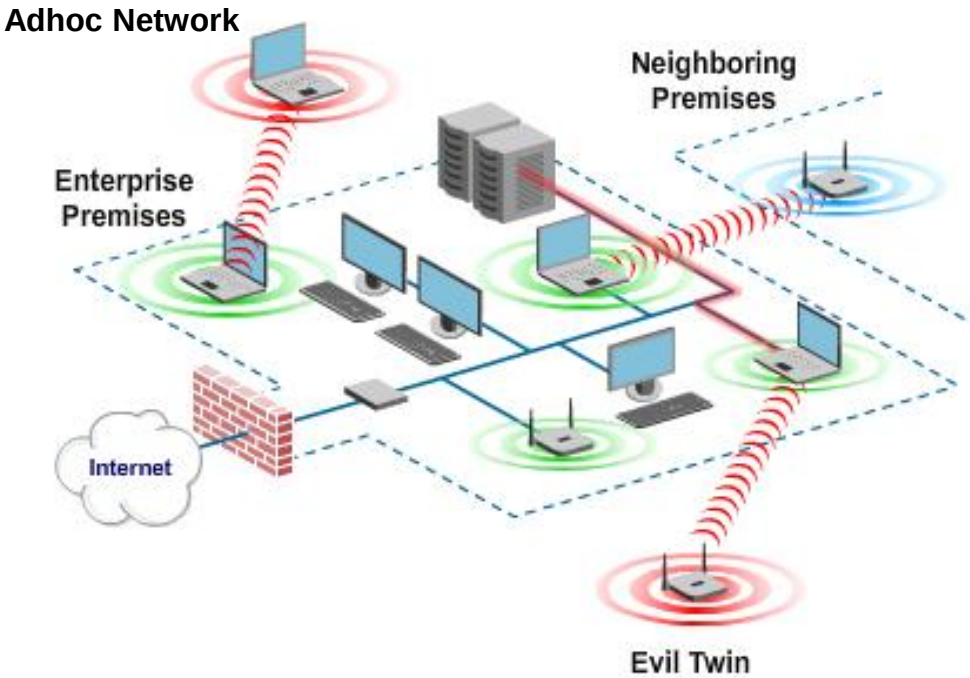
Similarly, About 87% Clients are Unmanaged/External!

AP Based Threats



- Rogue APs
- AP mis-configurations
- Soft/Client Based APs

Client based threats



- Client extrusions

Connections to neighbors, evil twins

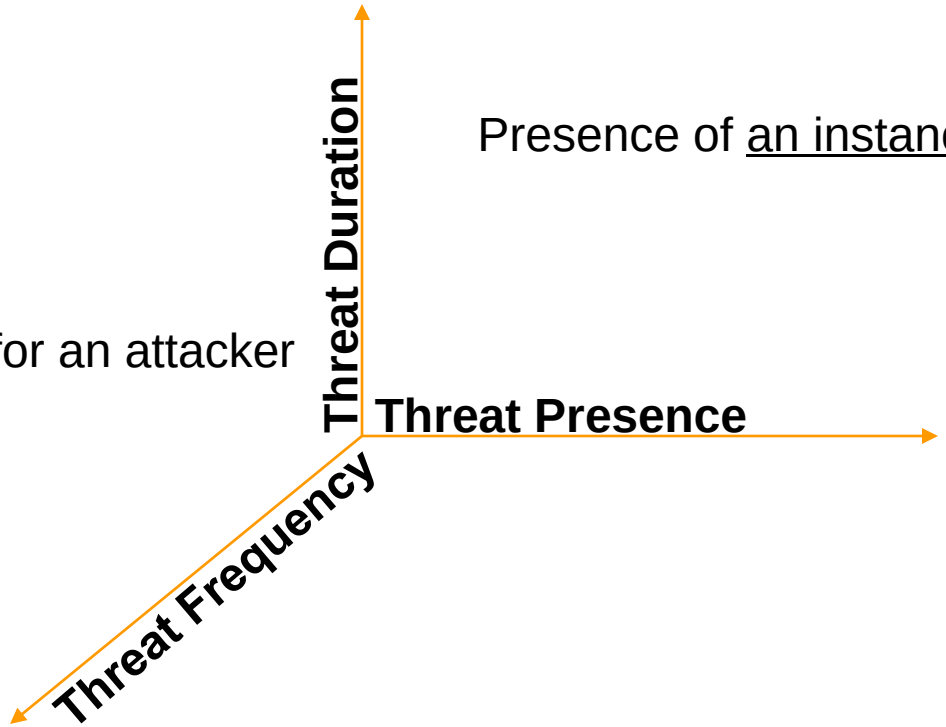
- Adhoc networks
- Client bridging

- Banned devices

T^3 (T-Cube) Parameters

Presence of <u>an instance</u> of a threat *(%)*

Window of opportunity for an attacker



Likelihood of presence of a threat instance

Real-life data Based & Accurate picture of Threats

How does this information help you?

Get an idea of Wi-Fi threat scenario in enterprises that may be like yours

Which wireless threats you should worry about first?

Plan your enterprise mitigation strategy

Simple (Yes/No) metric based on the presence of an instance of

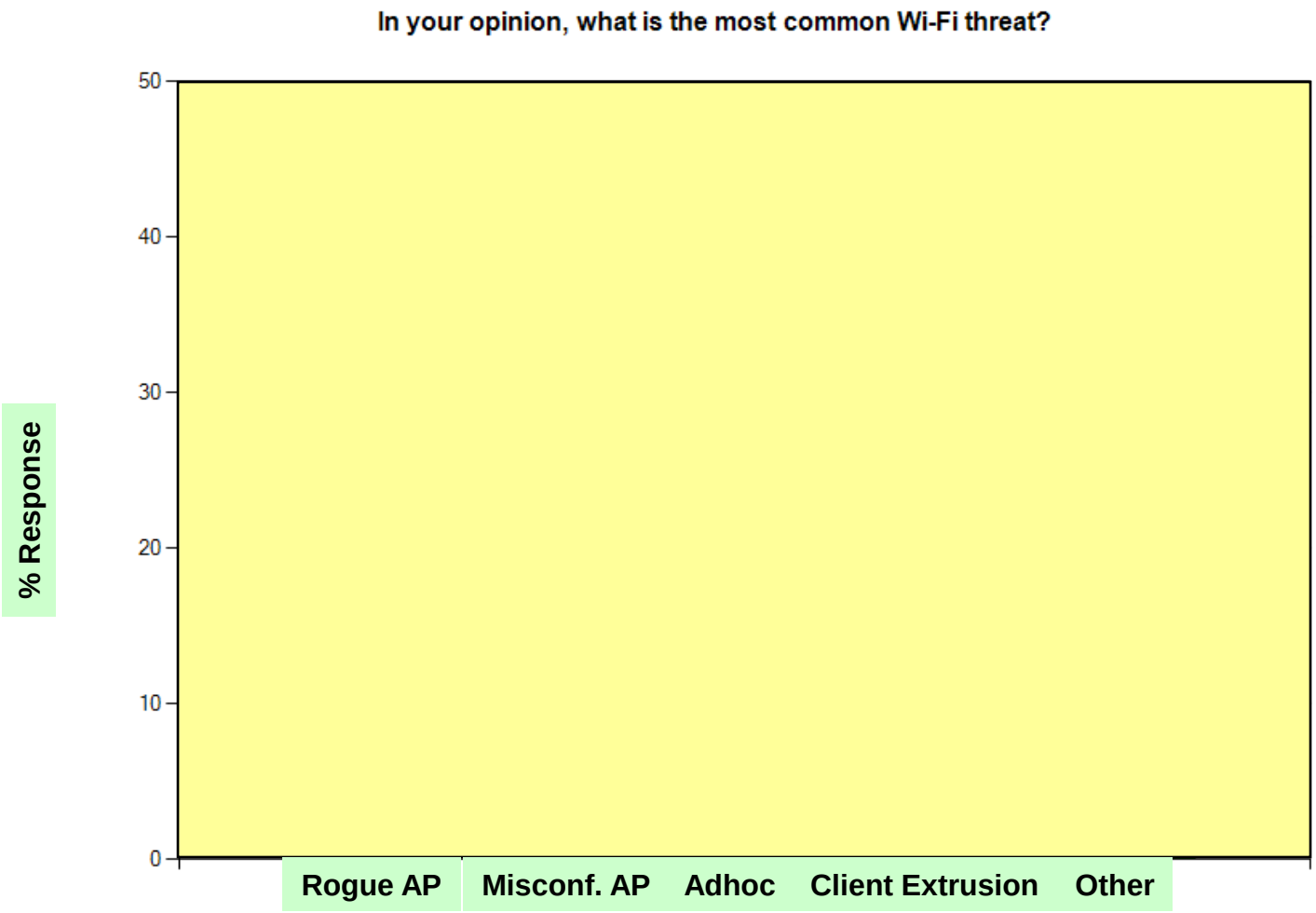
a threat *(%)*

Threat Presence

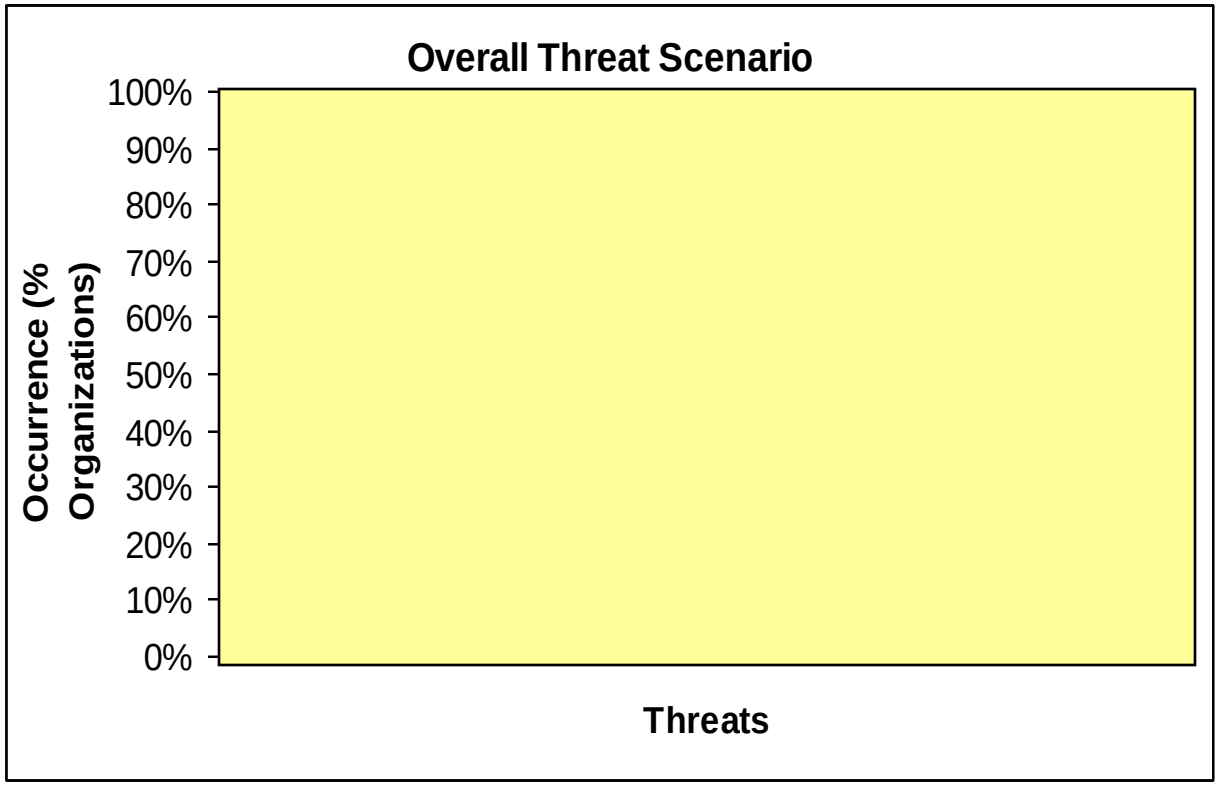
Threat Duration

Threat Frequency

Let us First Look At Survey Results



Results Based on Our Data Analysis

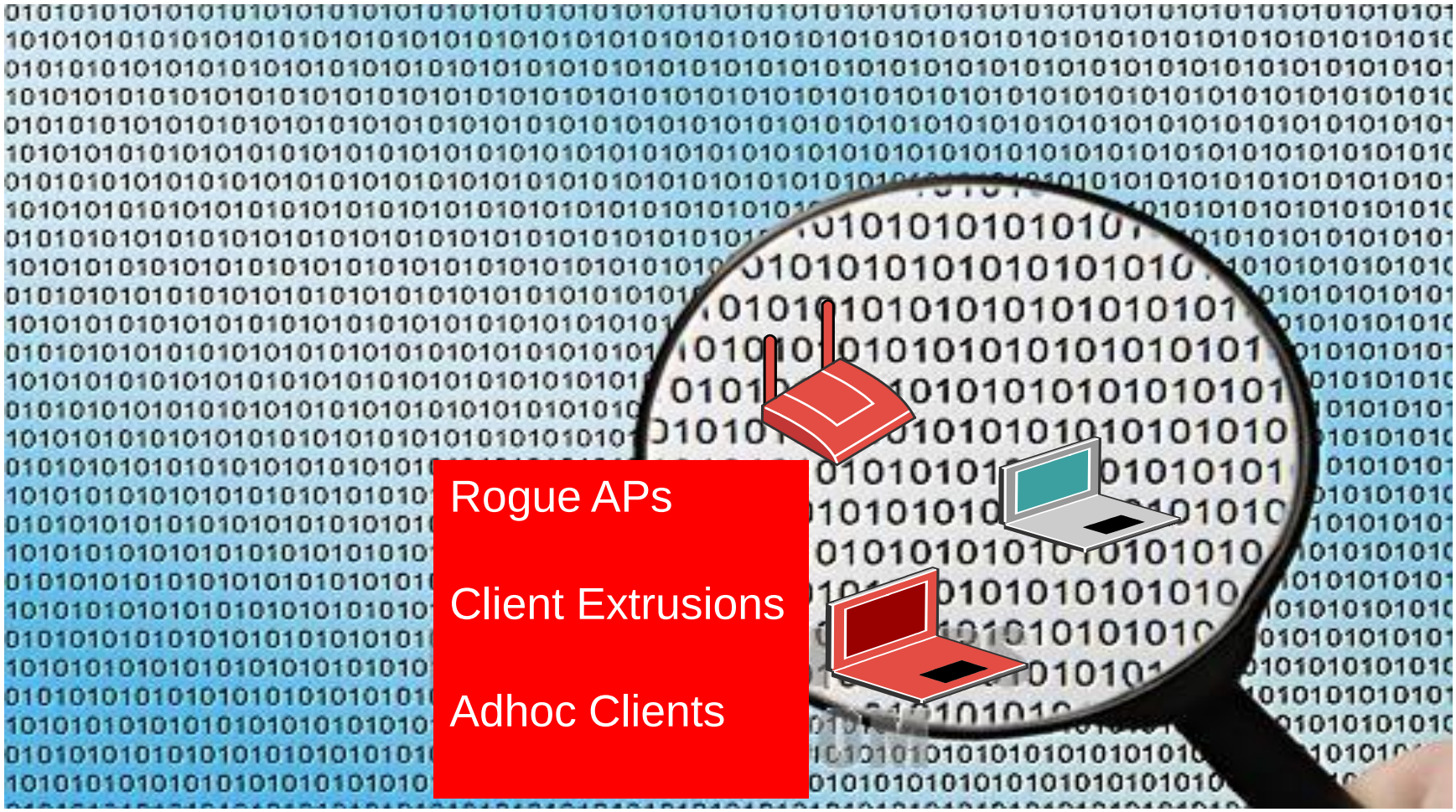


Key Observations

-Prominent Threats
- -Client extrusions
- -Rogue APs
- -AP mis-configurations
- -Adhoc clients

Key Implications

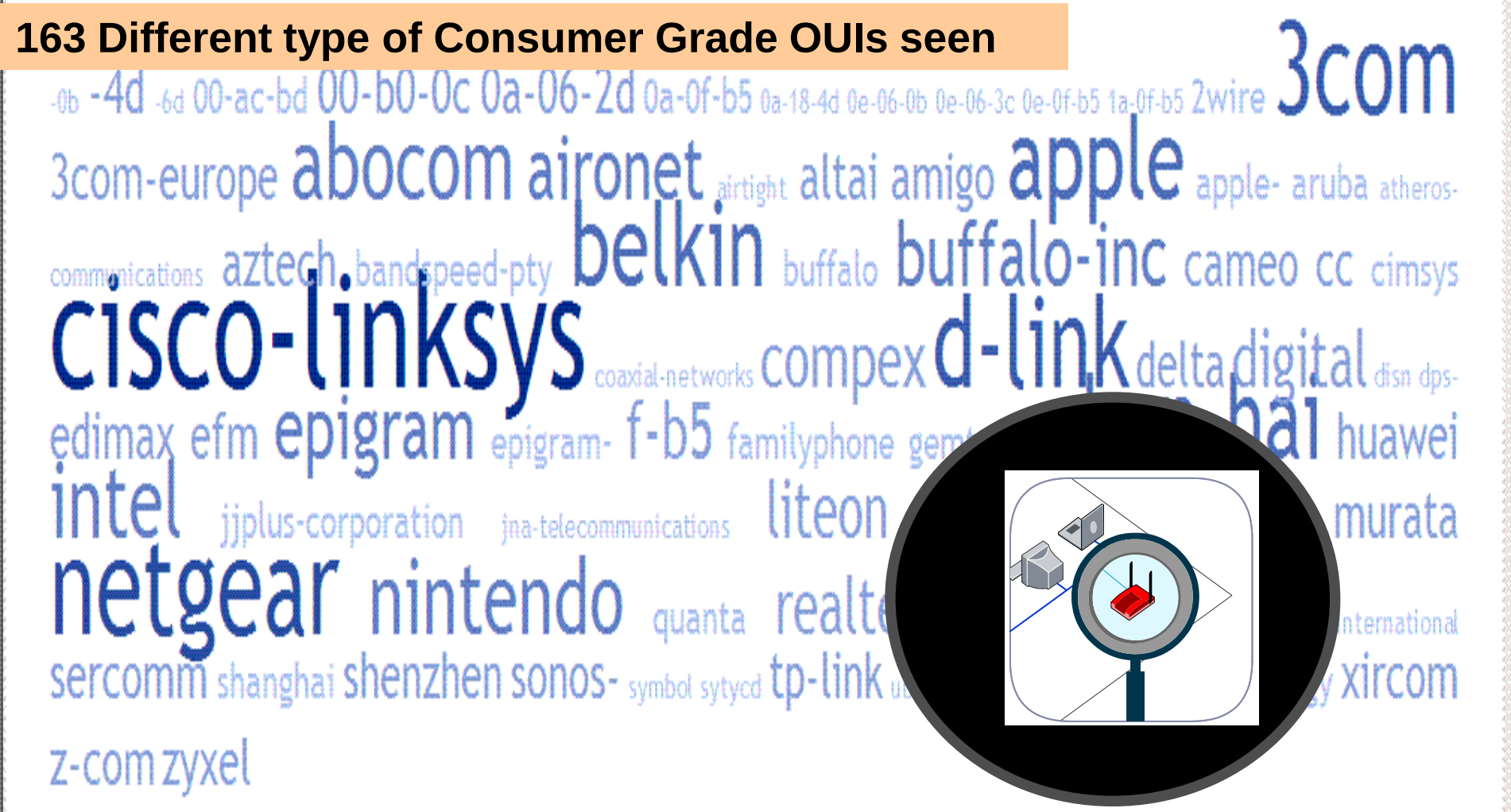
-Organization data is potentially at risk via Wi-Fi


Rogue APs
Client Extrusions
Adhoc Clients

Enterprise Wireless Consumerization: Rogue APs

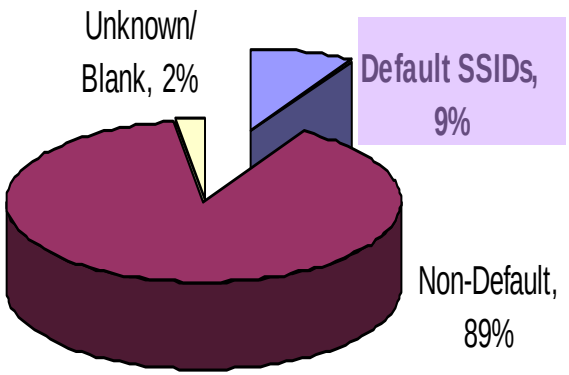
1521 Rogue APs seen in our study

163 Different type of Consumer Grade OUIs seen

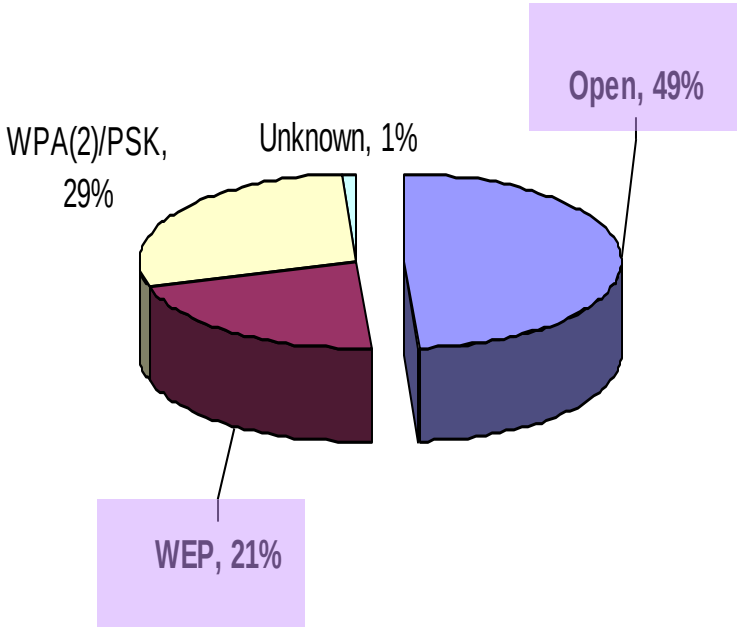


Rogue AP Details

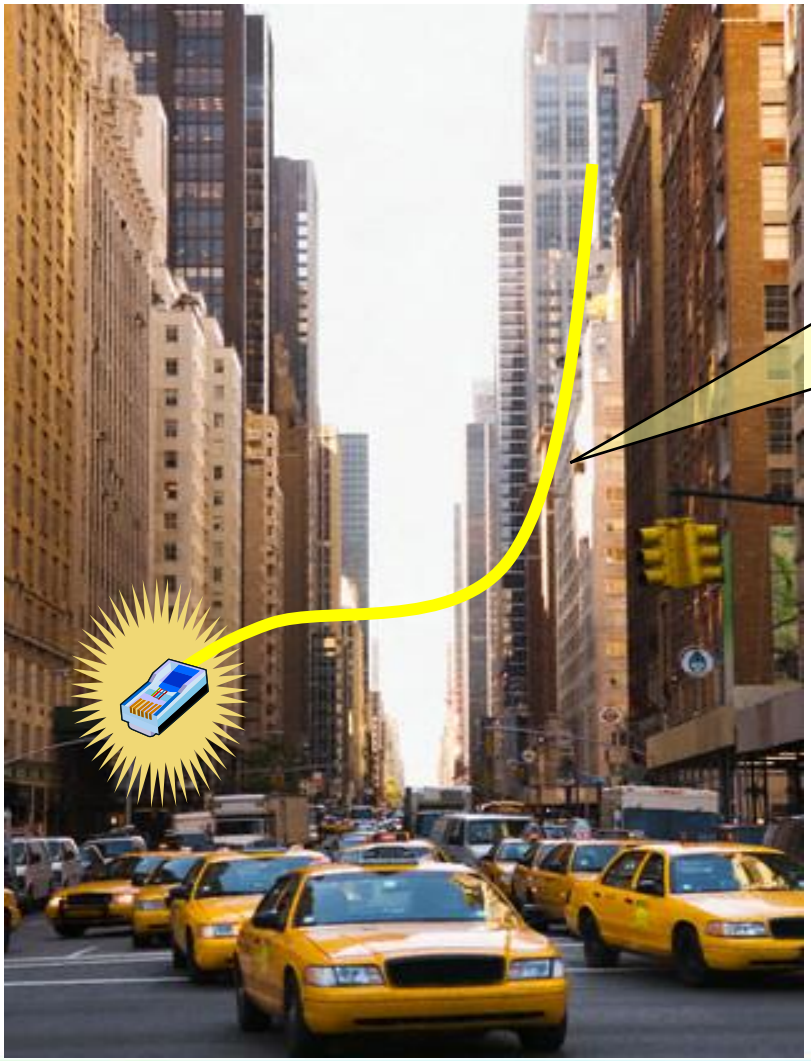
About 1 in 10 Rogue APs have Default SSIDs



About Half of Rogue APs Wide Open

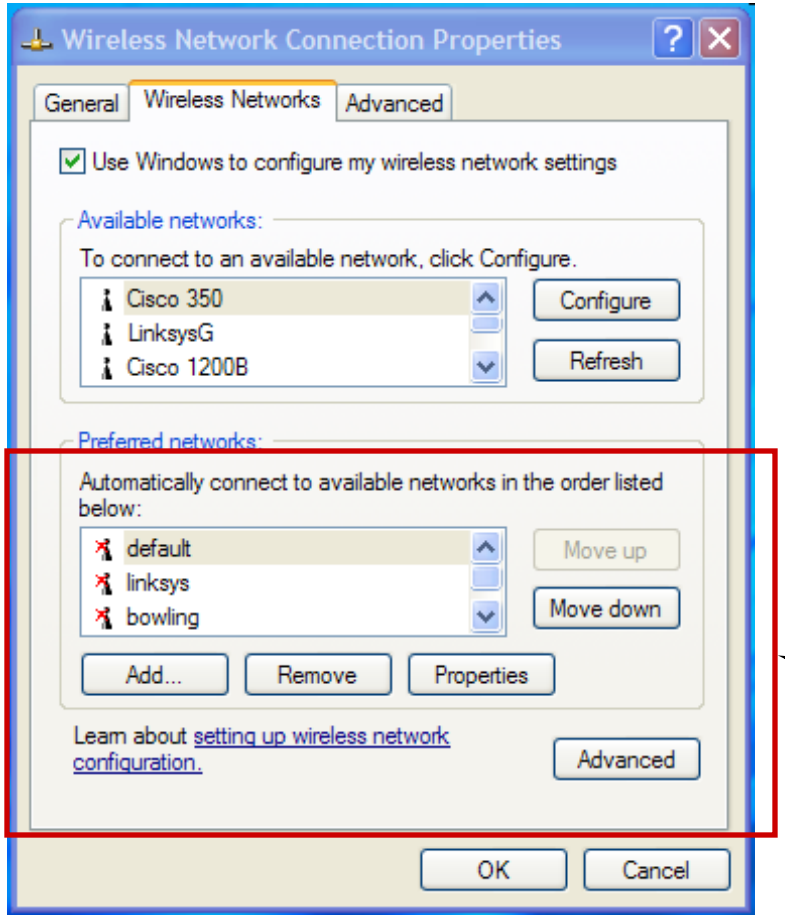


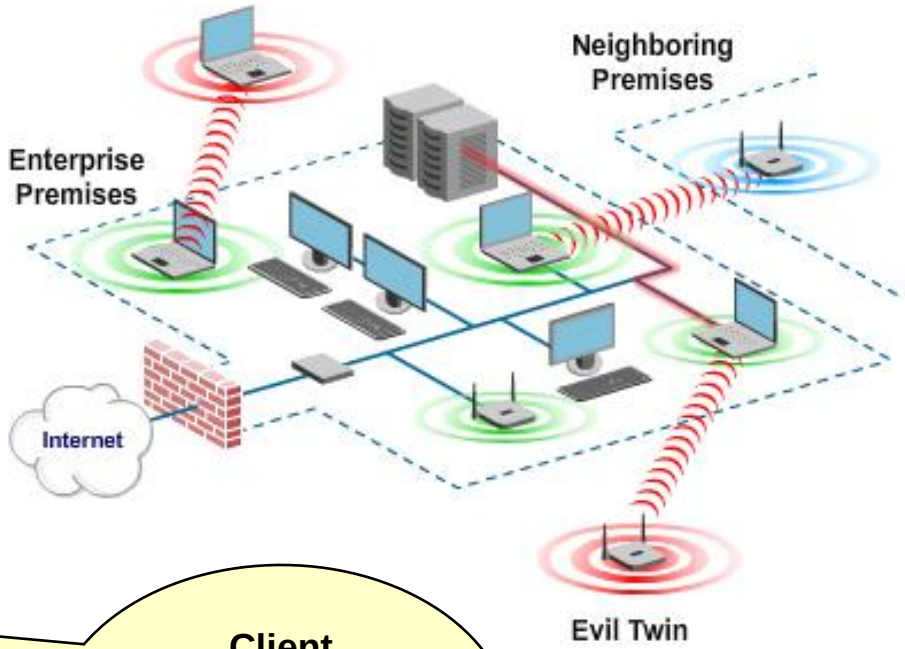
Rogue AP Details



An open Rogue AP is Virtually THIS!

Client Consumerization: Client Extrusion





Client (Smartphones & laptops both) probes for these SSIDs.

OP-ED CONTRIBUTOR

Won't You Be My Wireless Neighbor?

By HELEN RUBINSTEIN
Published: January 13, 2011

RECOMMEND
TWITTER
COMMENTS (381)
E-MAIL
PRINT
REPRINTS
SHARE

FOR a long time, I relied on my Brooklyn neighbors' generosity — that is, their unsecured wireless networks — every time I connected to the Web.

Enlarge This Image

Alan Dye

So, to linksers of Park Slope, in 2005, for allowing me to do my first freelance work from home; to Netgear 1 and Netgear 2 of the same neighborhood, in 2006, for supporting my electronic application to several graduate schools; to DHoffma, from 2007 to 2008, for letting me pay my taxes online and stream new episodes of "Friday Night Lights" each evening for a whole winter; to belkin54g, Cooley and, above all, to the blessed Belkin_G-Plus_MIMO of Ditmas Park, from 2009 to 2010, for the ability to speedily reply to student e-mails, video-chat with my sister, keep abreast of the latest literary hoo-ha, "like" as many of my friends' Facebook posts as I liked and learn all about lentil-sprouting or Prometheus whenever the mood struck: Thank you. And may you rest in peace.

Readers' Comments

Readers shared their thoughts on this article.
Read All Comments (381) »

Stealing Your Neighbor's WIFI Signal is Still Illegal

Tuesday, February 08, 2011

Contributed By:
Headlines

A recent poll by Wakefield Research and the Wi-Fi Alliance reveals that nearly one third of respondents admit to piggybacking on a neighbors unsecured WI-FI connection.

The percentage is about double the number that admitted to stealing WI-FI access in a previous poll in 2008.

Unsecured WI-FI connections pose a security threat to both the owner of the connection and to those who might "borrow" it from time to time.

Either way, an unsecured connection leaves sensitive data such as login passwords and credit card details vulnerable to harvesting by software such as Firesheep.

And yes, stealing your neighbors WI-FI signal is still illegal.

"Most consumers know that leaving their Wi-Fi network open is not a good thing, but the reality is that many have not taken the steps to protect themselves. Consumers can usually activate Wi-Fi security protections in a few simple steps, but much like the seatbelts in your car, it won't protect you unless you use it," said Kelly Davis-Felner of the Wi-Fi Alliance.

Owners of unsecured WI-FI connections also run the risk of having any illegal online activity potentially traced back to their ISP connection.

The Wi-Fi Alliance, a non-profit industry association, recommends WI-FI owners take a few easy steps to secure their connection:

Client Probing For Vulnerable SSIDs

Retail/SMB Organizations

118,981 Clients

Authorized | **Unmanaged**

12,002

106,979

636 (5.3%)

21,777 (20.4%)

Power of Accurate threat classification.

5.3% Vs 20.4%

"Known" Vulnerable SSIDs Probed For

103 **distinct SSIDs recorded**

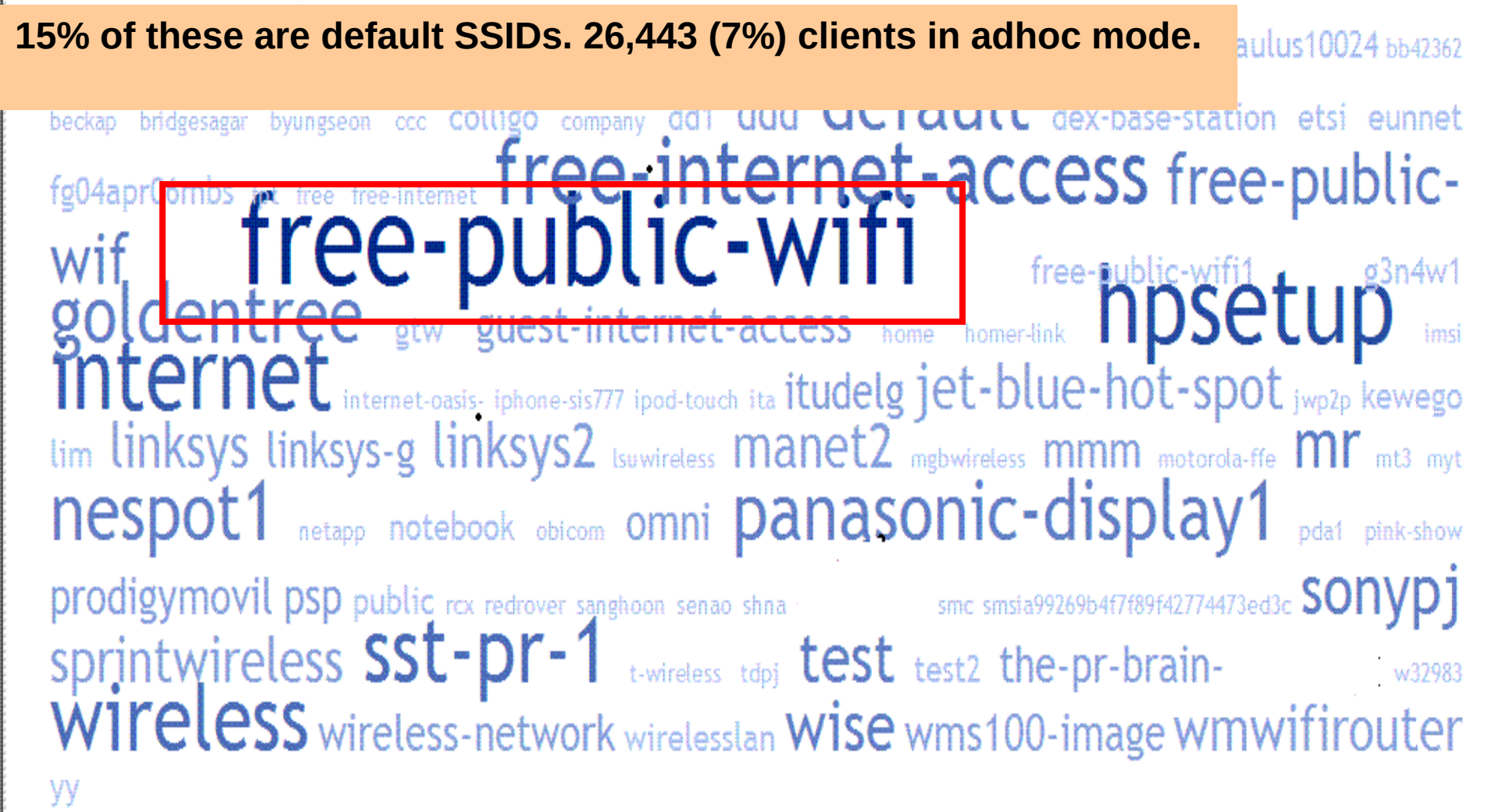
3com actiontec airport attwifi belkin belkin54g bestbuy box-fon-wlan-7170 brian
btopenzone buffalo ch concourse connectionpoint cox-hospitality daysinn dd-wrt
default dlink dlink-wireless earthlinkwifi ethostream free-internet-
access free-public-wifi fritz g604t-wireless globalsuitewireless
goesh goldentree googlewifi hawking hhonors holidayinn home home1 homenet
homenetwork homeoffice hotspot hpsetup ibahn ibm intermec internet kpn
linksys linksys-g linksys1 linksys2 matrix metrofi-free mobile monzoon motorola
mshome my-wireless-network-a mycloud net netgear netgear1 netpoint network office orange
panera print-server private public skyhighspeed skynet smc sonicwall speedlinks speedstream sst-pr-1
stayonline steve stsn surfandsip ta telenor test tmobile topcom tsunami untitled usr5461 usr8054
visitor wavelan-network wayport-access west wifi wireless wireless-network
wireless1 wlan wlan-ap zoom zyxel

Certain (8%) Authorized Clients Probing for 5 or more SSIDs

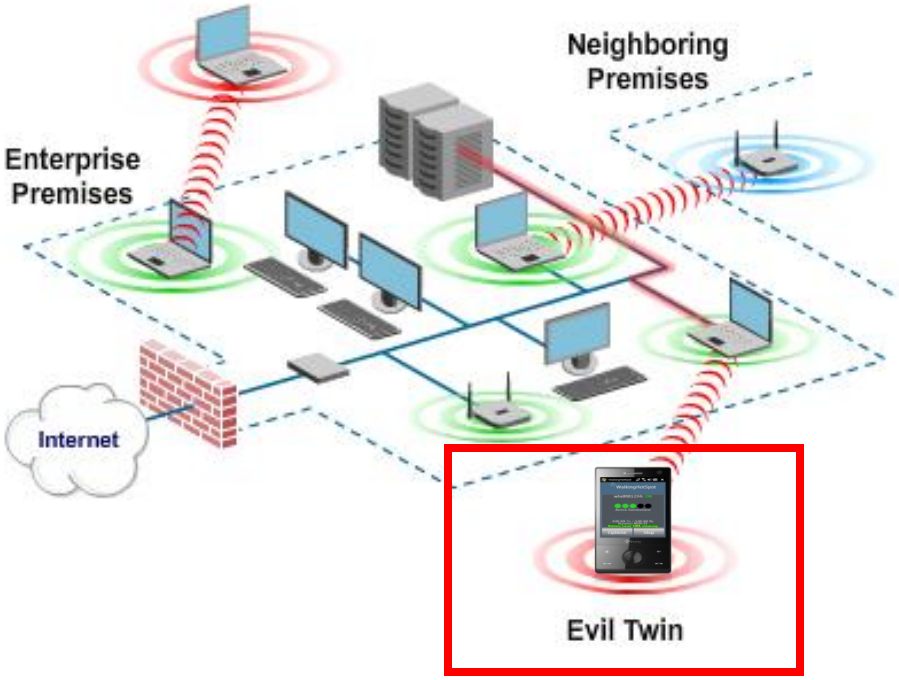
Adhoc Authorized Clients!

565 distinct Adhoc SSIDs found, About half of them Vulnerable

15% of these are default SSIDs. 26,443 (7%) clients in adhoc mode.



So What?
Illustrative Exploit via Client Extrusion



VIDEO DEMO: Smartpot MITM Attack

192.168.2.15 - SF - SSH Secure Shell

File Edit View Window Help

Quick Connect Profiles

```
CH  3 ][ Ela

BSSID

7A:D0:CE:1C:
00:0B:86:F9:
00:0B:86:F9:
00:0B:86:F9:
00:0B:86:F9:
00:0B:86:67:
00:0B:86:67:
00:0B:86:68:
00:0B:86:68:
00:0B:86:6C:
00:1C:10:A6:
00:0B:86:F9:
00:0B:86:F9:
00:1F:27:56:
00:1F:27:56:
00:1F:27:56:

BSSID

7A:D0:CE:1C:
(not associa
(not associa
(not associa
00:0B:86:F9:
00:0B:86:F9:
^C
Nokia-N900:/h
```

Nokia-N900:0.0

11:30 am 2.5 Mobile HotSpot

Start

Connection
AT&T Internet

Network name
FreeWiFi

Encryption
None

Connected to 192.168.2.15 SSH2 - aes128-cbc - hmac-md5 - none 124x46

How long (time interval) a threat is active before removal?

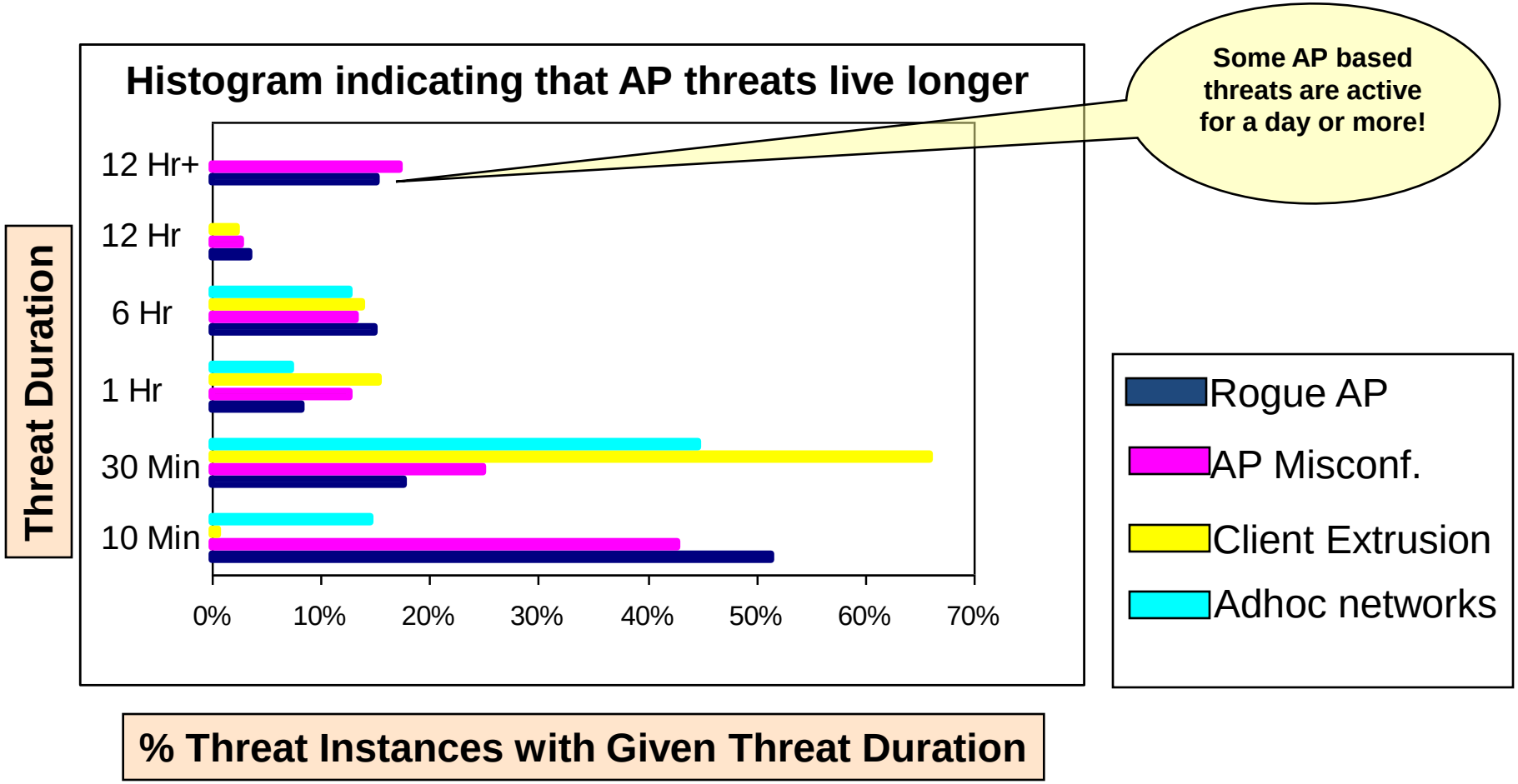
Threat Presence

Threat Duration

Threat Frequency

AP Threats live "longer" than Client Threats

15% client threats & 30 % AP threats live for > hr



Data from SMB/Retail (PCI) Segment

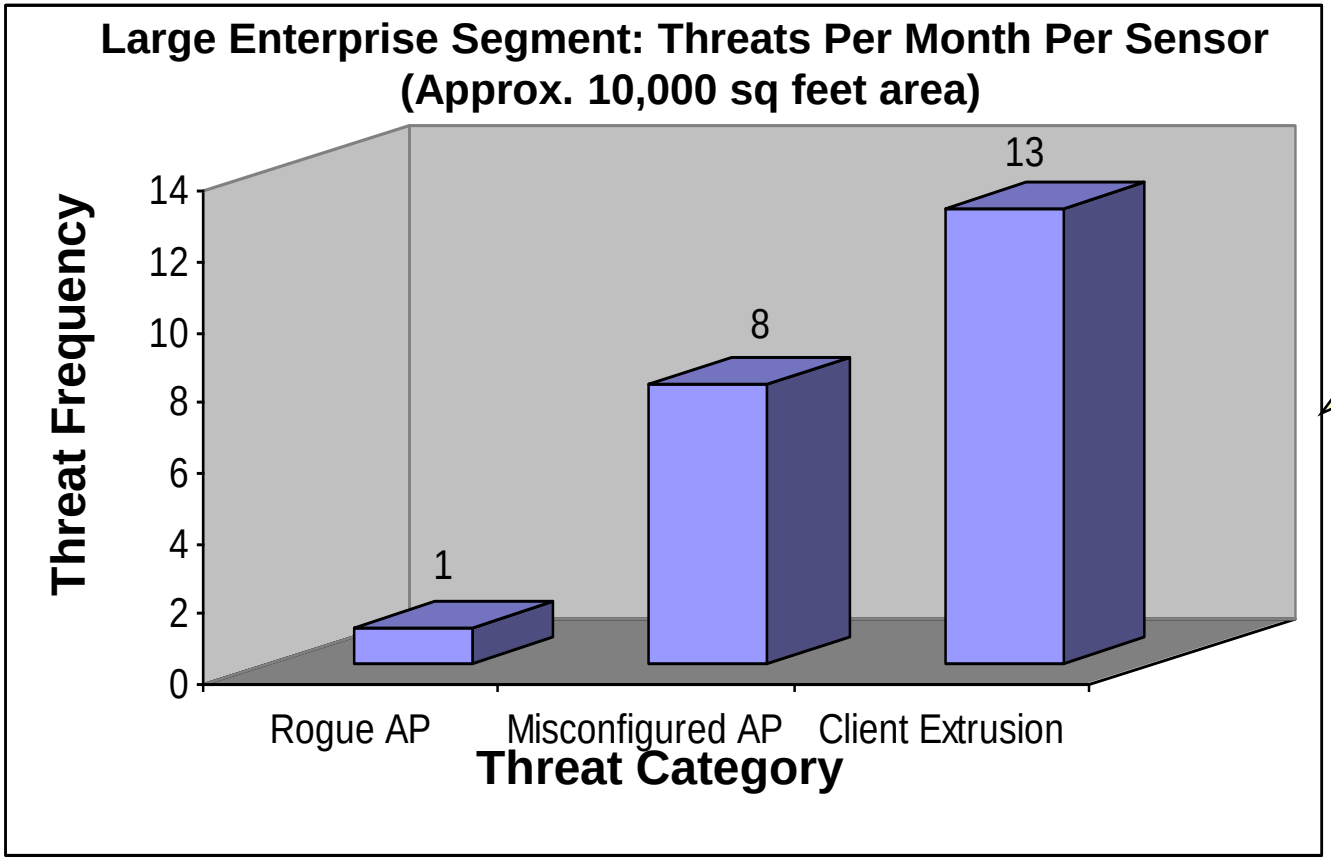
Threat instances per Sensor per month

Threat Presence

Threat Duration

Threat Frequency

Threat Frequency



Bigger your organization, higher the likelihood of finding the threats

Key Takeaways Summarized

- Wireless threats due to unmanaged devices are present
  - Enterprise wireless environment influenced by consumerization
- Certain threats more common than others
  - Client extrusions
  - Rogue AP
  - AP Mis-configurations
  - Adhoc clients
- Common threats affect large enterprise and SMB organizations
  - **Wireless threats persist regardless of sophistication of wired network security**

Threat Mitigation

Let’s Ban Wi-Fi!

Use WPA2 Enterprise For Your Authorized WLAN!

But, WPA2 does not protect against threats due to unmanaged devices

Best Practices

- Cleanup wireless profiles regularly
- Do not connect to networks such as "Free Public WiFi", "Free Internet"
- Do not connect to ad hoc networks
- Use Virtual Private Network (VPN) if you are on the road
- Conduct enterprise wireless scans periodically

Options for Wireless Scans

Laptop/Notebook based tools

- Public domain tools used for war driving can be re-purposed for scans
- Examples include Netstumbler, Backtrack, Kismet
- However, process is manual and suffers from limitations of wardriving (discussed earlier)

Centrally Managed tools

- Via deployment of wireless sensors
- Both onsite and SaaS models available
- Onsite models need an upfront CapEx, but, OpEx based SaaS based models combine best of both worlds –
  - Removes cumbersome manual process
  - Accurate threat classification

SpectraGuard® Enterprise — openview openview (Viewer) — AirTight Networks

Dashboard | Events | Devices | Locations | Reports | Forensics | Administration — Aug 26, 05:45 PM (GMT +0530)

Democorp
- Unknown
- USA
  - Arizona
  - California
  - Colorado
  - Florida
  - Georgia
  - Indiana
  - Michigan
  - New York
  - New Jersey
  - Pennsylvania
  - Texas
  - Virginia
  - Washington
  - West Virginia

Authorized | Mis-configured | Rogue | External — Active | Inactive — a | b only | b/g | a/b/g | Other — Non-802.11n | 802.11n — 802.11 | WPA | WEP | Open | Multi | Unknown

root@wirelessdefence:~

File Edit View Terminal Tabs Help

Network List (Autofit)

Name	T	W	Ch	Packts	Flags	IP Range
default	A	N	006	9	F	192.168.0.1
! iyonder.net	A	N	005	42	U4	10.254.178.254
! iyonder.net	A	N	001	22	A3	10.254.178.0
! eurospot	A	N	001	19	U4	204.26.5.166
! NETGEAR	A	O	006	5		0.0.0.0
. eurospot	A	N	011	14		0.0.0.0
! belkin54g	A	Y	011	17		0.0.0.0
! iyonder.net	A	N	011	16	A3	10.254.178.0
! tsunami	A	Y	007	17		0.0.0.0
! <no ssid>	A	O	003	11		0.0.0.0
Probe Networks	P	N	---	3		0.0.0.0
! iyonder.net	A	N	008	35		0.0.0.0
. <no ssid>	A	Y	011	5		0.0.0.0
NCDT_NET	A	Y	006	1		0.0.0.0
<no ssid>	A	Y	011	1		0.0.0.0

Info
Ntwrks 16
Pckets 228
Cryptd 4
Weak 0
Noise 0
Discrd 0
Pkts/s 8
Elapsd 00:00:20

Status
Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\036\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0
bssid 00:0A:8A:A2:C8:7F
Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP

Battery: AC 107%

Threat Mitigation Summary

Intrusions (AP Based Threats)

- Wire side controls as a first line of defense (e.g., 802.1X port control)
- Wireless IPS to automatically detect & block intrusions

Extrusions (Client Based Threats)

- Educate users: clean up profiles, Use VPNs & connect to secure Wi-Fi
- Deploy end point agents to automatically block connections to insecure Wi-Fi
- Wireless IPS to automatically detect & block extrusions in enterprise perimeter

Questions?

Thank You

gopinath.kn@airtightnetworks.com