ISNIFF GPS

Virtual Wardriving

SyScan Singapore 2013

@hubert3
hubert(a)pentest.com
Anatomy of a leak: how iPhones spill the ID of networks they access

Yes, iPhones and other Apple devices routinely do expose the unique ...

by Dan Goodin - Mar 27 2012, 6:30pm CEST

Ars Technica article - March 2012
Introducing iSniff GPS...

iSniff_import.py uses scapy to sniff:

- Client MAC addresses
- Unicast ARPs (RFC 4436)
- MDNS (Bonjour) broadcasts
- SSID probes (802.11 Probe Requests)

Stored in Django backend database / web interface
$ ./isniff_import.py -h
usage: isniff_import.py [-h] [-r PCAP] [-i INTERFACE]

iSniff GPS Server

optional arguments:
  -h, --help       show this help message and exit
  -r PCAP          pcap file to read
  -i INTERFACE     interface to sniff (default mon0)

$ ./isniff_import.py -r ../chan11-03.cap
Reading ../chan11-03.cap...
Intel [00:24:d7:e2:61:5c] probe for LabPrivate
Intel [00:24:d7:e2:61:5c] probe for pentestdmz
Overview of clients detected

1337 devices probing for 3543 networks detected

<table>
<thead>
<tr>
<th>MAC</th>
<th>Name</th>
<th>Manufacturer</th>
<th>Probed for</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:c0:ca:...</td>
<td>ALFA</td>
<td>BlackHat</td>
<td>Open, Test, Secure WiFi, iSniff Channel 11</td>
</tr>
<tr>
<td>00:21:e9:...</td>
<td>Apple</td>
<td></td>
<td>ARP:00:14:7f:6f, ARP:00:14:6c:6f, Open, Test, Secure WiFi, iSniff Channel 11</td>
</tr>
<tr>
<td>00:23:6c:...</td>
<td>Apple</td>
<td>BlackHat</td>
<td></td>
</tr>
<tr>
<td>00:23:df:...</td>
<td>Dannys-iPhone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>74:e1:b6:...</td>
<td>Apple</td>
<td>hhhonors</td>
<td></td>
</tr>
<tr>
<td>74:e1:b6:...</td>
<td>Apple</td>
<td>linksys, majorhome</td>
<td></td>
</tr>
<tr>
<td>74:e1:b6:...</td>
<td>Apple</td>
<td>BlackHat, ARP:00:0b:86, iSniff Channel 11, home-down, BTOpenzone-H, BTHub3-CGF3, TALKTALK-69B453, SKY47597, fulwith, BTHomeHub-85B2, ARP:00:b0:0c:6f</td>
<td></td>
</tr>
<tr>
<td>74:e1:b6:...</td>
<td>Apple</td>
<td>gogoinflight, SFO-WiFi, testline, AMT, Claremont WiFi, greenwood, pier, SPH, SPH_244, Ratna Ling Public, sandpiper house, Gaia_Anderson9, The Cottages, BCC-WiFi, Larkspur, fiend, fiend_EXT</td>
<td></td>
</tr>
</tbody>
</table>
Overview by network...

### Clients probing for 3543 networks detected

<table>
<thead>
<tr>
<th>SSID / BSSID</th>
<th>Probed for by</th>
<th>Last probed for</th>
</tr>
</thead>
</table>

Clients probing for a particular network

### Clients probing for network HACKER (Unknown)

<table>
<thead>
<tr>
<th>MAC</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>7c:6d:62:17:2a:03</td>
<td></td>
</tr>
<tr>
<td>7c:6d:62:17:2a:03</td>
<td></td>
</tr>
<tr>
<td>f0:cb:a1:17:2a:03</td>
<td></td>
</tr>
</tbody>
</table>
Client 74:e1:b6 (Apple)

Probed for:

<table>
<thead>
<tr>
<th>SSID</th>
<th>BSSID</th>
<th>Lat</th>
<th>Lon</th>
<th>Comment</th>
<th>Last probe observed</th>
<th>Locate</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlackHat</td>
<td>00:0b:86:8c</td>
<td>36.11669159</td>
<td>-115.18044281</td>
<td></td>
<td>July 26, 2012, 10:11 p.m.</td>
<td></td>
</tr>
<tr>
<td>iSniff Channel 11</td>
<td>00:0b:86:8c</td>
<td></td>
<td></td>
<td></td>
<td>July 26, 2012, 9:46 p.m.</td>
<td></td>
</tr>
<tr>
<td>home-down</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>July 25, 2012, 10:16 p.m.</td>
<td></td>
</tr>
<tr>
<td>BTOpenzone-H</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>July 25, 2012, 10:16 p.m.</td>
<td></td>
</tr>
<tr>
<td>BTHub3-CGF3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>July 25, 2012, 10:16 p.m.</td>
<td></td>
</tr>
<tr>
<td>TALKTALK-69B453</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>July 25, 2012, 10:16 p.m.</td>
<td></td>
</tr>
<tr>
<td>SKY47597</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>July 25, 2012, 10:16 p.m.</td>
<td></td>
</tr>
<tr>
<td>fulwith</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>July 25, 2012, 10:16 p.m.</td>
<td></td>
</tr>
<tr>
<td>BTHomeHub-85B2</td>
<td>00:b0:0c:8c</td>
<td>53.1234567</td>
<td>-2.12345678</td>
<td></td>
<td>July 25, 2012, 10:21 p.m.</td>
<td></td>
</tr>
</tbody>
</table>
Help WiGLE: Please [donate] your points to the WiGLE commercial dataset

Find a wireless network by [searching] or [browsing the interactive map]

Add a wireless network to WiGLE [from a stumble file] or [by hand]

Add [remarks] to an existing network
Locations for SSID ‘BlackHat’ from wigle.net
How to locate a wifi router by MAC address?

Samy Kamkar “How I met your girlfriend”

Geolocation via XXXSS

- Upon MAC acquisition, ask the Google
- See FF source for Location Services

POST /loc/json HTTP/1.0
Host: www.google.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv: 1.9.2b4) Gecko/20091124 Firefox/3.6b4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: none
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Content-Length: 127
Content-Type: text/plain; charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache

{"version": "1.1.0", "request_address": true, "wifi_towers": [{"mac_address": "Smac", "ssid": "g", "signal_strength": -72}]}
How to locate a wifi router by MAC address?

- Skyhook Wireless
- Google (http://samy.pl/androidmap/)
Google API restricted...

android map - by samy kamkar

Android map exposes the data that Google has been collecting from virtually all Android devices and street view cars, using them essentially as global wardriving machines. You can use this tool to accurately locate virtually any router in the world, as well as position iPhones and Android phones.

When the phone detects any wireless network, encrypted or otherwise, it sends the BSSID (MAC address) of the router along with signal strength, and most importantly, GPS coordinates up to the mothership.

This page allows you to ping that database and find exactly where any Wi-Fi router in the world is located. Note that iPhones also send this BSSID and Cell Tower Information up to Apple, as well.

You can enter any router BSSID/MAC address to locate the exact physical location below, or try the demonstration router by hitting "Probe" below.

Follow me on twitter to hear about more of my extremely thrilling projects.

Note: Google has taken steps to stop my tool from working, including explicitly blocking me directly. Additionally, their geolocation API will now only share information that Google has on "you" only if you provide them not only information about your router, but unwittingly provide information about "other" people's routers.

MAC Address / BSSID

00:11:24:EC:72:CF

Probe

Like 2,862 people like this. Be the first of your friends.
iOS device HTTPS request to Apple - Where am I?
Response from Apple

HTTP/1.1 200 OK

Wifi BSSID : e0:91:f5:fe:f6:60
Latitude : 48.87655264
Longitude : 2.32190334
Confiance : 42

Wifi BSSID : 0:1e:8c:4c:25:7b
Latitude : 48.87650626
Longitude : 2.32190334
Confiance : 42

Wifi BSSID : e0:a1:d7:73:94:0c
Latitude : 48.87662076
Longitude : 2.32189691
Confiance : 45
Response from Apple (Visualization)
Response from Apple (Visualization)
iOS device HTTPS request to Apple - Contributing data

Decoded sample request from http://fxaguessy.fr/rapport-pfe-interception-ssl-analyse-donnees-localisation-smartphones/
Opt Out?

Configure access points with Google Location Service

To improve your use of location-based services, Google, as a location service provider, uses publicly broadcast Wi-Fi data from wireless access points, as well as GPS and cell tower data.

Location services play an important part in enabling many of today’s most popular location-aware applications, in particular on smart phones, laptops and other devices that are WiFi enabled. The inclusion of your WiFi access point in the Google Location Service enables applications like Google Maps to work better and more accurately.

Only publicly broadcast Wi-Fi information is used to estimate the location of a device.

You can control whether or not your access point is included in GLS by following the steps below.

How do I opt out?

You can opt out by changing the SSID (name) of your WiFi access point (your wireless network name) so that it ends with ".nomap". For example, if your SSID is “12345,” you would need to change it to “12345_nomap”.

You can click on the link below that corresponds to the manufacturer of your access point, to find specific instructions on changing your access point’s SSID. If you received your access point from your ISP, you may wish to contact them to find out how to change the SSID.

- Apple
- Belkin
- Linksys (Cisco)
- Netgear
Apple iOS...

Makes no difference...
Experiment (Sample size = 2)

**Netgear DG834 v3**

Turned on 2013-02-27

SSID
"NETGEAR" (Broadcast disabled), no clients

First found in Apple Database 2013-03-15

~16 days

**Netgear CG3100 Cable Modem**

Turned on 2013-03-05

SSID broadcast enabled

First found in Apple Database 2013-03-18

~13 days
BSSID d8:c7:c8:d2:6a:21

2174 APs (0 added)
BSSID d8:c7:c8:d2:6a:21

114 APs matching aruba
iSniff GPS KML export in Google Earth
THANKS

iSniff GPS tool and slides by @hubert3
hubert(a)pentest.com

https://github.com/hubert3/isniff-gps

Using code published by François-Xavier Aguessy and Côme Demoustier
http://fxaguessy.fr/rapport-pfe-interception-ssl-analyse-donnees-localisation-smartphones/