The Machines That Betrayed Their Masters

Glenn Wilkinson
BlackHat Asia 2014
Machines? Betrayal?
Machines?
Betrayal?
A Device
A Unique Signature
aka
“Digital Terrestrial Footprint”
A Link from Signature to a Human
Snoopy Framework
Diagram showing a 3G connection and XBee devices.
A Unique Signature
98:03:ab:32:11:33
Linking the Signature
Linking the Signature

1. Passive Linking
BTHomeHub-AFV1, are you there?
Starbucks, are you there?
Virgin-AFVT, are you there?
Is anyone out there?

98:03:ab:32:11:33
<table>
<thead>
<tr>
<th>SSID</th>
<th>GPS Lat</th>
<th>GPS Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virgin-AFVT</td>
<td>50.507</td>
<td>-0.128</td>
</tr>
<tr>
<td>Starbucks</td>
<td>50.408</td>
<td>-0.041</td>
</tr>
<tr>
<td>BTBusinessHub-2DF1</td>
<td>50.601</td>
<td>-0.045</td>
</tr>
<tr>
<td>Starbucks</td>
<td>50.391</td>
<td>-0.050</td>
</tr>
</tbody>
</table>
BTHomeHub-AFV1, are you there?
Starbucks, are you there?
Virgin-AFVT, are you there?
Is anyone out there?

98:03:ab:32:11:33
Linking the Signature?

2. Active Linking
BTHomeHub-AFV1, are you there?
Starbucks, are you there?
Virgin-AFVT, are you there?
Is anyone out there?

Hey iPhone! It’s me, Starbucks!

98:03:ab:32:11:33
Scenarios
<table>
<thead>
<tr>
<th>Conference</th>
<th>Unique Devices</th>
<th>Number of Attendees</th>
<th>Device Per Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlackHatVegas ‘12</td>
<td>4778</td>
<td>6500</td>
<td>0.74</td>
</tr>
<tr>
<td>ITWeb ’12</td>
<td>1106</td>
<td>400</td>
<td>2.77</td>
</tr>
<tr>
<td>44CON ’12</td>
<td>969</td>
<td>350</td>
<td>2.77</td>
</tr>
<tr>
<td>BlackHatEU ’13</td>
<td>681</td>
<td>607</td>
<td>1.12</td>
</tr>
<tr>
<td>Securitay ’13</td>
<td>375</td>
<td>100</td>
<td>3.75</td>
</tr>
<tr>
<td>BSides ‘13</td>
<td>208</td>
<td>474</td>
<td>0.44</td>
</tr>
<tr>
<td>Hackito ’13</td>
<td>309</td>
<td>400</td>
<td>0.77</td>
</tr>
<tr>
<td>CERT Poland ’13</td>
<td>598</td>
<td>500</td>
<td>1.2</td>
</tr>
<tr>
<td>ZeroNights ‘13</td>
<td>507</td>
<td>600</td>
<td>1.18</td>
</tr>
<tr>
<td>BlackHat Brazil ’13</td>
<td>719</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>BlackHat Asia ’14</td>
<td>719</td>
<td>?</td>
<td></td>
</tr>
</tbody>
</table>