Bogus BGP Route Data

Compiling and Reporting Actionable Intel
What bogus data?

- Prefixes that route for bogon address blocks
- Bogon ASNs in the path
- Other bogus prefixes
- Bogus origins
- Bogus paths
- Bogus attributes (e.g. communities)
- ...in the global, public Internet routing tables
Bogon prefixes

• Bogon exact match prefix
  • special use, reserved, unallocated prefix
• Route covering bogon
  • e.g. 203.0.112.0/23 covers TEST-NET-3
• More specific bogon
  • e.g. 172.17.0.0/24 is RFC 1918 space
Bogon ASNs

• Bogon ASN
  • special use, reserved, unallocated ASN
Why do we care?

• Address exhaustion
  • Do leaks become more common?
  • Is anyone watching IPv6 space?
• Route hijacking and squatting
  • Well known cases of unannounced usage by parties not delegated the address space
• What happens to traffic hitting bogon addresses?
## Initial bogon route leak report

<table>
<thead>
<tr>
<th>ASN</th>
<th>announcement</th>
<th>bogon</th>
</tr>
</thead>
<tbody>
<tr>
<td>81</td>
<td>192.154.32.0/19</td>
<td>192.154.59.0/24</td>
</tr>
<tr>
<td>701</td>
<td>198.168.0.0/16</td>
<td>198.168.0.0/24</td>
</tr>
<tr>
<td>701</td>
<td>198.168.0.0/16</td>
<td>198.168.105.0/24</td>
</tr>
<tr>
<td>1221</td>
<td>115.42.28.0/24</td>
<td>115.42.0.0/18</td>
</tr>
<tr>
<td>6342</td>
<td>2001:498::/32</td>
<td>2001:498::/29</td>
</tr>
</tbody>
</table>
## Planned bogon route leak report

<table>
<thead>
<tr>
<th>ASN</th>
<th>announcement</th>
<th>bogon</th>
<th>seen by</th>
</tr>
</thead>
<tbody>
<tr>
<td>81</td>
<td>192.154.32.0/19</td>
<td>192.154.59.0/24</td>
<td>TC, RV</td>
</tr>
<tr>
<td>701</td>
<td>198.168.0.0/16</td>
<td>198.168.0.0/24</td>
<td>TC, RIPE</td>
</tr>
<tr>
<td>701</td>
<td>198.168.0.0/16</td>
<td>198.168.105.0/24</td>
<td>RV, LG-ATT</td>
</tr>
<tr>
<td>1221</td>
<td>115.42.28.0/24</td>
<td>115.42.0.0/18</td>
<td>TC, LG-HE</td>
</tr>
<tr>
<td>6342</td>
<td>2001:498::/32</td>
<td>2001:498::/29</td>
<td>ALL</td>
</tr>
</tbody>
</table>
Psuedo-code

• Set bogon route table
• Create current RIB views
• Step 1, are bogons routed by RIB views?
• Step 2, are RIB view routes routed by bogons
• Step 3, build report with originating ASN
Other efforts

• CIDR report does some of this and much more
  • http://www.cidr-report.org/as2.0/#Bogons
  • Mostly on automatic pilot
  • Limited coverage
  • Doesn't handle covering prefixes
• Team Cymru already a key player here
  • http://www.team-cymru.org/Services/Bogons/
Who gets the data?

- Origin ASN
- Origin ASN also wants downstream data
  - how do you determine what downstream is?
- Can you publish everything publicly?
  - TC route data may not be suitable for public
  - exclude TC-only data from public reports
What happens with data?

• Data format
  • Integration with automated tools is key
• How do you automate the use of this data?
  • Do your own internal reporting?
  • Verify against your BGP policy configurations?
• How does it change?
• Graph, statistics
Where to from here?

• Build tools to deal with public views
  • Should be fast and reliable
• Construct bogus ASN report
• Consider other bogus BGP data
  • May require custom BGP data collection