IPv4 Hijacking: Our Experiences

Ingrid Wijte
Registration Services
In This Talk

- Our definition of hijacking
- Background
- Common approaches by hijackers
- RIPE NCC processes abused and forged documentation
- Investigations and interventions
- Common difficulties and typical responses
- Protecting your resources
Our Definition of Hijacking

“Taking control of *issued* Internet number resources under false pretences.”

- Re-registered to hijackers or another (innocent) organisation
- Addresses have economic value due to IPv4 scarcity
Hijacking: Background

• 12 September 2012: the RIPE NCC starts allocating from the last /8
• Since then, the RIPE NCC sees an increase in hijackings of apparent unused and/or abandoned address space

<table>
<thead>
<tr>
<th>Resource</th>
<th>Ongoing</th>
<th>Resolved</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy</td>
<td>1</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>PI</td>
<td>140</td>
<td>67</td>
<td>207</td>
</tr>
<tr>
<td></td>
<td>141</td>
<td>81</td>
<td>222</td>
</tr>
</tbody>
</table>
The hijackers’ approach:

- Research company histories and provide paper trails to demonstrate changes in business structure.
- Conduct BGP test announcements to check if addresses are unused.
- Re-register expired domain names to make email change requests look legitimate.
- Copy websites, with identical pages hosted on (almost) identical domain names.
• RIPE Database maintainer password resets
• Company acquisitions or organisation name changes
• Posing as resource holders looking for a sponsoring LIR for 2007-01 compliance
Forged Documentation Submitted

- Faked IDs
- Faked company registration papers
- Forged signatures of real people on contracts
- Forged stamps and signatures of notaries and resource holders
Why We Look Closer

- A resource holder sends us a complaint or abuse report
- An experienced IPRA notices something out of the ordinary
- Follow-up from existing investigations: one case often leads to another
How We Investigate

• We check changes in company structure:
  - Public records
  - National registries

• We contact former and current resource holders (where possible):
  - Contact people and organisations found on documentation
  - Phone calls, sending emails and faxes
  - Using other contact information beyond what was provided
When We Find Something Wrong

• We revert all changes immediately
• Allow time to support their claim to the address space
• Resources are de-registered if no legitimate holder found (in 2007-01 cases)
• Where member involvement can be proven: closure of LIR account and de-registration of LIR resources
• Report to authorities where appropriate
• We work with the resource holder to protect their resources
Common Difficulties

• The resource holder expects immediate action while we are investigating
• It can be difficult to find and contact the resource holder in question
• We see things happening but we cannot take action (yet)
• We can catch them — but we can’t stop them from trying again (they can open a new RIPE NCC membership account)
• No effective penalty and lots to gain
Typical Responses

- Silence…
- “We are a victim of fraud”
- Denial and anger:
  - IPRAs are insulted and threatened with lawsuits against them personally and/or the RIPE NCC
  - Threats “to come to the office and…”
  - IPRAs’ names are spread on mailing lists and fora
- Arbitration is offered but not taken
Finding The Right Balance

- We are trying to maintain a relationship that is based on trust.
- We try to find a balance between ensuring that we are talking to the legitimate holder vs being overly cautious or inflexible:
  - End Users might find the RIPE NCC becoming more strict in our verification requirements as a result.
  - Recent mailing list discussion on due diligence processes.
  - We need understanding and support from the community — we are trying to protect your resources.
What You Can Do

• Protect your resources against hijacking by making sure your RIPE Database objects and contact information are up to date
• If acquiring resources, ensure you are in contact with the legitimate holder or representative
• If you need help, or think your resources may have been hijacked, contact: reg-review@ripe.net

https://www.ripe.net/lir-services/resource-management/address-hijacking-in-the-ripe-ncc-service-region
Questions?