The Anti-Hijacking Policy Proposal

Carlos Friaças
RCTS CERT, FCT | FCCN
24th May 2019, TF-CSIRT 57
Hijacks Happen. Everyday.

- bgpstream.com
  - See «possible hijacks»

- Several different goals
  - Traffic interception
  - Diversion for law enforcement/jurisdiction
  - Injecting/sending toxic content without being identified or bothered
  - More...?
Are there any consequences?

• Hardly.
  – Upstreams might cancel service
  – IXPs may kick hijackers out, if they hijack through the IXP

• **NONE, at REGISTRY level.**
  – Hijackers are able to maintain service agreements and allowed to be part of the registry ecosystem
  – Hijackers keep their legitimately obtained numbering resources -- which they use in hijacks
Who Manages Numbering Resources? Who makes the rules?

• Regional Internet Registries do.

• You might have heard about the RIPE NCC...

• Is the RIPE NCC making the policies that allow the «hijacking party to go on»?
  – NO
  – The «RIPE community» builds policies – i.e. «me», «you», «us».
The Policy Development Process...

• https://www.ripe.net/participate/policies
What are we proposing?

• Persistent Intentional Hijacks are to be declared a RIR policy violation

• Hijacks are not tolerated
  – Mistakes are out of scope

• If more than one policy violation occurs, RIR membership may be lost
  – RIR Service Contract terminated
    • Numbering resources revoked
  – Only after the company involved had the chance to object and explain there is a misunderstanding
    • «Checks & Balances»
The main hurdle...

<any org here> is not the Routing Police.

• It is a design feature that no entity alone can supervise routing.

• But how this justifies nothing can be done, when org X is announcing address space from org Y, without their approval.
  – ...and anyone can see it!
Arguments Opposing 2019-03

• The registry is like a «land registration office»
  – RIRs are membership-based; RIRs distribute assets.
• The registry doesn’t have anything to do with routing
  – So why is a registry needed?
• This policy, if accepted, could be weaponised
  – There is a number of safety knobs; several experts will look at each case.
• There are huge legal risks to the registry itself
  – Closure of membership is already established; that can happen only if members don’t follow established registry rules/policies.
**Arguments Supporting 2019-03**

- The gap in the policies needs to be closed
  - Consequences for hijackers are needed in order to reduce this «technique»
- There are several sources with abundant routing information
  - Which can be used to determine if an hijack took place and if it was intentional
- Tools like RPKI and MANRS are not enough
  - For the time being, given their limited adoption
Important detail to have in mind...

• Who are the victims of an hijack?

1) The legitimate number resource holder

2) Anyone who receives an hijacked route announcement
   – i.e. potentially *everyone*
**Fresh News about RIPE NCC members' closures...**

- **Stats published last week**

<table>
<thead>
<tr>
<th>Year</th>
<th>Closures</th>
<th>By Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>3</td>
<td>1 PL, 1 IR, 1 UA</td>
</tr>
<tr>
<td>2015</td>
<td>1</td>
<td>1 RU</td>
</tr>
<tr>
<td>2016</td>
<td>5</td>
<td>3 IR, 1 GR, 1 DM</td>
</tr>
<tr>
<td>2017</td>
<td>1</td>
<td>1 UK</td>
</tr>
<tr>
<td>2018</td>
<td>52</td>
<td>37 SC, 4 US, 3 UK, 3 HL, 2 CN, 2 RU, 1 AU</td>
</tr>
<tr>
<td>2019</td>
<td>7</td>
<td>4 RU, 1 HK, 1 KZ, 1 NL</td>
</tr>
<tr>
<td>Total</td>
<td>69</td>
<td></td>
</tr>
</tbody>
</table>
How to participate?

• Subscribe to the Anti-Abuse Working Group Mailing List
  – https://www.ripe.net/mailman/listinfo/anti-abuse-wg/

• Do express your opinion on the list
  – «I support 2019-03»
  – Write «why», if you can spare the time

• You can obviously instead oppose 2019-03
  – Saying «why»
  – Or saying where the proposal can be improved (in further versions)
Policy-wise: A Global Effort

- RIPE: 2019-03
- LACNIC: LAC-2019-05
- ARIN: PROP-266
- AFRINIC: <queued>
- APNIC: <queued>
Questions

https://anti-hijacking-proposal.tk
(text, mailing list archives and subscription links)

THANKS!
DANKE!
MERCI!
OBREGADO!