BGP Flexibility and... Its Consequences

Alexander Azimov
Qrator Labs aa@qrator.net
Rights

- Get address space from RIR...
Rights

• Get address space from RIR...
• Establish BGP sessions...
Rights

• Get address space from RIR...
• Establish BGP sessions...
• Get traffic...

and do with it whatever you want!
Obligations

• Pay fee to RIR...

That’s all!
Home Credit Bank

https://radar.qrator.net/blog/when-bank-plays-in-ip-transit-games
Who Is to Blame?

The problem is not mistake/anomaly itself. The problem is that it was *globally* distributed!
What is Globally Distributed?

• Accepted by Regional Tier-1;
• Accepted by Global Tier-1;
• Accepted by RS of IXes.
No RPKI-filtering – no ROAs?
Route Objects

IPv4

IPv6

Valid  Invalid  No object

Valid  Invalid  No object
Invalid Objects & No Object

Invalid:
• Common situation for company with multiple ISPs;
• May happen between c2p;
• Or may be a hijack.

No object:
How do they pass filters?
Methodology

• Route Object Aggregator (RIPE, APNIC, ARIN, AFRINIC, RADB... 27 sources);
• Analyze only globally visible prefixes;
• Analyze only prefixes passing c2p links.
## No Object: Russian Tier-1

<table>
<thead>
<tr>
<th>ISP</th>
<th>Announced</th>
<th>Accepted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>v4</td>
<td>v6</td>
</tr>
<tr>
<td>Rostelecom (AS12389)</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>TTK (AS20485)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Vimpelcom (AS3216)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Megafon (AS31133)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MTS (AS8359)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RETN (AS9002)</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
37.79.208.0/20

whois -h whois.radb.net '!'r37.79.208.0/20,L'

No filters?!
## No Object: IXes

<table>
<thead>
<tr>
<th>IXP</th>
<th>v4</th>
<th>v6</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE-CIX (AS6695)</td>
<td>211</td>
<td>6</td>
</tr>
<tr>
<td>AMS-IX (AS6777)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IX Equinix (AS24115)</td>
<td>67</td>
<td>117</td>
</tr>
<tr>
<td>HKIX (AS4635)</td>
<td>1762</td>
<td>2142</td>
</tr>
<tr>
<td>MSK-IX (AS8631)</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Key Findings

- ROAs are still little deployed;
- No filters between regional and global Tier-1;
- A lot of invalid ASN-prefix pairs, it requires further investigation;

People's Choice Award goes to AMS-IX and MSK-IX!

Exceptions in ingress filtering = security holes;
Horror Stories for the Night
Horror Stories for the Night
Horror Stories for the Night

And suddenly credentials are gone...
What Can Transit Do?

• IRR filters at your customer links, no exceptions!
• Consider using IRR filters with your private peers;
• Ad-hoc filtering ([NTT Peering Lock](#));
• Consider using RPKI-cache inside your network;
• Constant BGP monitoring.
What Can IX Do?

Strict security check: RPKI, BGPSec...
What Can Multihomed Do?

• Keep your Route Objects up to date.
• Create ROA records ([RIPE Wizard](#));
• Consider using RPKI-cache inside your network;
• Consider using prefix-asn filtering;
• Constant BGP monitoring.