Route Security

NANOG 74: Security Track
Recent BGP incidents

Andree Toonk
andree@bgpmon.net
Censorship gone wrong

July 2018

Instagram rerouted to Iran

10 Instagram prefixes
8 more specifics

58224 (Iran Telecommunication Company PJS)

https://bgpstream.com/event/1440
We've seen this movie before

Youtube hijack, 2007

Turk Telekom, 2014
Popular destinations rerouted to Russia

- 80 prefixes for Google, Apple, NTT, Facebook, Riot Games, and more
- Origin AS 39523 (DV-LINK-AS), Russia.

December 2017

https://bgpmon.net/popular-destinations-rerouted-to-russia/
Hijacking financial services, example 1

April 2017

Russian ISP hijacks financial services’ Internet traffic

Visa, MasterCard, and Symantec among dozens affected.

AS12389 (PJSC Rostelecom), Russia

https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
<th>Affected Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2018</td>
<td>BGP/DNS Hijacks Target Payment Systems</td>
<td>Savvis, Vantiv, Q9 Networks Inc, UltraDNS, Internet Media Network, CenturyLink, Mercury Payment Systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital Wireless Indonesia (AS38146), Extreme Broadband (AS38182)</td>
</tr>
</tbody>
</table>

Hijacking DNS Infrastructure services

The route53 incident

April 2018

BGP/DNS Hijack

AWS Route53

Myetherwallet.com

eNet (AS10297), Ohio USA

https://arstechnica.com/?post_type=post&p=1298417
# DNS traffic to route53 according to Kentik

## Top Dest AS Number by Average packets/s

![Graph showing DNS traffic to route53](https://www.kentik.com/blog/aws-route-53-bgp-hijack-what-kentik-saw/)

### Destination AS Number

<table>
<thead>
<tr>
<th>Destination</th>
<th>Average packets/s</th>
<th>95th Percentile packets/s</th>
<th>Max packets/s</th>
<th>Last datapoint packets/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENET-2 - eNET Inc.,US (10297)</td>
<td>347.96</td>
<td>1,472.85</td>
<td>1,636.69</td>
<td>0.00</td>
</tr>
<tr>
<td>AMAZON-02 - Amazon.com, Inc.,US (16509)</td>
<td>506.05</td>
<td>718.51</td>
<td>1,112.75</td>
<td>773.12</td>
</tr>
</tbody>
</table>

### Total of Top 2

<table>
<thead>
<tr>
<th></th>
<th>Average packets/s</th>
<th>95th Percentile packets/s</th>
<th>Max packets/s</th>
<th>Last datapoint packets/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total of Top 2</td>
<td>853.01</td>
<td>2,191.36</td>
<td>2,749.44</td>
<td>773.12</td>
</tr>
</tbody>
</table>

We've seen this movie before

Spamhaus (DDOS) attack

The Canadian Bitcoin hijack (2014)
What did AWS do?
/24’s appeared, 6 days later (till now)
route53 ROA’s appeared 3 days later!

$ whois -h whois.bgpmon.net ' --roa 16509 205.251.193.0/24'
0 - Valid
------------------------
ROA Details
------------------------
Origin ASN: AS16509
Not valid Before: 2018-04-27 04:00:00
Not valid After: 2028-04-27 04:00:00 Expires in 9y323d8m1.39999997615814s
Trust Anchor: rpki.arin.net
Prefixes: 205.251.193.0/24

$ whois -h whois.bgpmon.net ' --roa 16509 2600:9000:5300::/48'
0 - Valid
------------------------
ROA Details
------------------------
Origin ASN: AS16509
Not valid Before: 2018-04-27 04:00:00
Not valid After: 2028-04-27 04:00:00 Expires in 9y323d7m57.3999999761581s
Trust Anchor: rpki.arin.net
Prefixes: 2600:9000:5300::/48
RPKI to the rescue?

All of the incidents mentioned would have been prevented if Origin Validation would have been fully deployed.
We did not talk about path validation, yet route leaks and AS path spoofing remain a big challenge.

Most large ISP’s do a decent job filtering. IX’s remain the wild west.
Questions and comments?
Rights

• Get address space from RIR;
• Establish BGP sessions;
• Advertise prefixes;
• Receive traffic.
Responsibilities

• MUST not hijack foreign address space;
• MUST not create route leaks;
• MUST support anti-spoofing policies;
• MUST configure Ingress/Egress filters;
• MUST pay fee to RIR.
Responsibilities

• MUST not hijack foreign address space;
• MUST not create BGP leaks;
• MUST adopt anti-spoofing policies;
• MUST configure Ingress/Egress filters;
• MUST pay fee to RIR – that’s all!
BGP Anomalies

BGP Hijacks
Illegitimate advertisement of foreign address space.

BGP Route Leaks
Illegitimate announce of a route received from peer or upstream to another peer or upstream.
Outages Become Regular

• 24\textsuperscript{th} April: ENET, AS10297, US: Malicious BGP and DNS hijack. The attack was successful.

• 26\textsuperscript{th} April: DPSTL, AS267286, Brazil: Mega-hijack. A Brazilian ISP announced 16 /8 prefixes plus several smaller prefixes; ~5% of the entire IPv4 address space in total.

• 4\textsuperscript{th} May: ELCAT, AS8449, Kyrgyzstan: Giant route leak between China and Russia.

• 18\textsuperscript{th} May: PBNET, AS263086, Brazil: Full table leak disrupting Brazil segment.
I will never create BGP hijack again
BGP Ingress Filtering: AS-SETs

AS-SET to ASNs
- 200449, 197068, ...

ASNs to route objects
- 178.248.232.0/21, 185.65.148.0/22, 45.116.91.0/24, 89.218.31.0/24 ...

IRR filters doesn’t perform origin validation!
AS-SETs & AS Cone

In ‘Ideal World’ AS-SETs = AS Cone
AS-SETs & AS Cone

Not in AS-SET? Drop it!

In ‘Ideal World’ AS-SETs = AS Cone
AS-SETs & AS Cone

In ‘Ideal World’ AS-SETs = AS Cone
But even in ‘Ideal World’ it has limitations
What Do We Know?

- IRR filters can’t validate the origin;
- AS-SET objects are not authorized;
- Poorly maintained AS-SETs become less effective;
- There are ISPs that do not use any IRR filters.
How many filters have been already violated?
Methodology

• Aggregate (RIPE, APNIC, ARIN, AFRINIC, RADB... 27 sources);
• Retrieve prefixes with unique asn in route objects;
• Detect c2p links through which route leaks were propagated;
• Detect c2p links through which bogon prefixes were propagated;
• Check that origin doesn’t belong to customer cone.
## Results

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>At least 7% of ISPs have problems with filters</td>
<td>At least 1% of ISPs have problems with filters</td>
</tr>
</tbody>
</table>
Results: Explained

Percent of Violated Filters by ISP size

- Top10
- Top100
- Top200
- Top300
- Top400

IPv4, IPv6
Boundary Case

If network
  • Accepts leaks originated by transit-free networks;
  • Accepts bogon prefixes;

There are no IRR filters!
# No IRR Filters

## Russia

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>174 - Cogent</td>
<td>6939 - HE</td>
</tr>
<tr>
<td>4809 - China Telecom</td>
<td>16735 - ALGAR</td>
</tr>
<tr>
<td>4837 - China Unicom</td>
<td>23106 - Cemig</td>
</tr>
<tr>
<td>6695 - DECIX</td>
<td>49697 - Joey-Network</td>
</tr>
<tr>
<td>6939 - HE</td>
<td>199524 - G-Core</td>
</tr>
<tr>
<td>7363 - YOMURA</td>
<td></td>
</tr>
<tr>
<td>7552 - Viettel</td>
<td></td>
</tr>
<tr>
<td>7713 - Telkomnet</td>
<td></td>
</tr>
<tr>
<td>7843 - TWCABLE</td>
<td></td>
</tr>
<tr>
<td><strong>8732 - Comcor</strong></td>
<td><strong>50384 - W-IX</strong></td>
</tr>
<tr>
<td>9583 - Sify</td>
<td>53211 - ISPRJ</td>
</tr>
<tr>
<td><strong>12389 - Rostelecom</strong></td>
<td></td>
</tr>
</tbody>
</table>
## No IRR Filters

### China

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>174 - Cogent</td>
<td>12586 - GHOSTnet</td>
</tr>
<tr>
<td><strong>4809 - China Telecom</strong></td>
<td>13536 - TVC-AS1</td>
</tr>
<tr>
<td><strong>4837 - China Unicom</strong></td>
<td>20485 - TTK</td>
</tr>
<tr>
<td>6695 - DECIIX</td>
<td>20562 - Opentransit</td>
</tr>
<tr>
<td>6939 - HE</td>
<td>22356 - Durand</td>
</tr>
<tr>
<td>7363 - YOMURA</td>
<td>22773 - CXA</td>
</tr>
<tr>
<td>7552 - Viettel</td>
<td>31025 - GHOSTnet</td>
</tr>
<tr>
<td>7713 - Telkomnet</td>
<td>35104 - Kaztranscom</td>
</tr>
<tr>
<td>7843 - TWCABLE</td>
<td>40805 – JMFSOLUTIONS</td>
</tr>
<tr>
<td>8732 - Comcor</td>
<td>50384 - W-IX</td>
</tr>
<tr>
<td>9583 - Sify</td>
<td>53211 - ISPRJ</td>
</tr>
<tr>
<td>12389 - Rostelecom</td>
<td>6939 - HE</td>
</tr>
<tr>
<td></td>
<td>16735 - ALGAR</td>
</tr>
<tr>
<td></td>
<td>23106 - Cemig</td>
</tr>
<tr>
<td></td>
<td>49697 - Joey-Network</td>
</tr>
<tr>
<td></td>
<td>199524 - G-Core</td>
</tr>
</tbody>
</table>
## No IRR Filters

### IXes

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>174 - Cogent</td>
<td>6939 - HE</td>
</tr>
<tr>
<td>4809 - China Telecom</td>
<td>16735 - ALGAR</td>
</tr>
<tr>
<td>4837 - China Unicom</td>
<td>23106 - Cemig</td>
</tr>
<tr>
<td><strong>6695 - DECIX</strong></td>
<td><strong>49697 - Joey-Network</strong></td>
</tr>
<tr>
<td><strong>20562 - Opentransit</strong></td>
<td><strong>199524 - G-Core</strong></td>
</tr>
<tr>
<td>6939 - HE</td>
<td>7363 - YOMURA</td>
</tr>
<tr>
<td>22356 - Durand</td>
<td>22773 - CXA</td>
</tr>
<tr>
<td>7552 - Viettel</td>
<td>31025 - GHOSTnet</td>
</tr>
<tr>
<td>7713 - Telkomnet</td>
<td>35104 - Kaztranscom</td>
</tr>
<tr>
<td>7843 - TWCABLE</td>
<td>40805 – JMFSOLUTIONS</td>
</tr>
<tr>
<td>8732 - Comcor</td>
<td><strong>50384 - W-IX</strong></td>
</tr>
<tr>
<td>9583 - Sify</td>
<td>53211 - ISPRJ</td>
</tr>
<tr>
<td>12389 - Rostelecom</td>
<td></td>
</tr>
</tbody>
</table>
No IRR Filters

### IPv4

<table>
<thead>
<tr>
<th>Number</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>174</td>
<td>Cogent</td>
</tr>
<tr>
<td>4809</td>
<td>China Telecom</td>
</tr>
<tr>
<td>4837</td>
<td>China Unicom</td>
</tr>
<tr>
<td>6695</td>
<td>DECIX</td>
</tr>
<tr>
<td>6939</td>
<td>HE</td>
</tr>
<tr>
<td>7363</td>
<td>YOMURA</td>
</tr>
<tr>
<td>7552</td>
<td>Viettel</td>
</tr>
<tr>
<td>7713</td>
<td>Telkomnet</td>
</tr>
<tr>
<td>7843</td>
<td>TW-CABLE</td>
</tr>
<tr>
<td>8732</td>
<td>Comcor</td>
</tr>
<tr>
<td>9583</td>
<td>Sify</td>
</tr>
<tr>
<td>12389</td>
<td>Rostelecom</td>
</tr>
<tr>
<td>12586</td>
<td>GHOSTnet</td>
</tr>
<tr>
<td>13536</td>
<td>TVC-AS1</td>
</tr>
<tr>
<td>20485</td>
<td>TTK</td>
</tr>
<tr>
<td>20562</td>
<td>Opentransit</td>
</tr>
<tr>
<td>22356</td>
<td>Durand</td>
</tr>
</tbody>
</table>

### IPv6

<table>
<thead>
<tr>
<th>Number</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>6939</td>
<td>HE</td>
</tr>
<tr>
<td>16735</td>
<td>ALGAR</td>
</tr>
<tr>
<td>23106</td>
<td>Cemig</td>
</tr>
<tr>
<td>49697</td>
<td>Joey-Network</td>
</tr>
<tr>
<td>199524</td>
<td>G-Core</td>
</tr>
<tr>
<td>50384</td>
<td>W-IX</td>
</tr>
<tr>
<td>53211</td>
<td>ISPRJ</td>
</tr>
<tr>
<td>40805</td>
<td>JMFSOLUTIONS</td>
</tr>
</tbody>
</table>
Key Findings: IRR Filters

IRR Filters Can be Used to:
• Filter *some* hijacks;
• Filter *some* route leaks.

In reality:
• Many AS-SETs are *poorly maintained*;
• *No filters* at some huge Tier-2 networks;
• Even some *Tier1 networks fail* to configure filters;
Resource Public Key Infrastructure
check_roa(asn, prefix)

Valid – prefix matches ROA with corresponding asn and within maximum length;
Invalid – ROA(s) record exists, but without corresponding asn or prefix length exceeds maximum length;
Unknown – ROA that covers prefix does not exist.

Integration with AS-SET? Ooops…
ROA Records

IPv4

IPv6

Valid  Invalid  No object

Valid  Invalid  No object
No ROA validation – no ROAs?
ROA Validation: Bypassed

ROA (178.248.232.0/21, 197068, 32)

ASXXX

178.248.232.0/21
AS_PATH: ASXXX AS197068

ASYYY

ROA check OK!
Key Findings: ROA Validation

ROA Validation Can be Used to:
• filter mistake hijacks;

ROA Validation Can’t be Used to:
• filter route leaks;
• filter malicious hijacks.

In reality:
• Only 10% of prefixes are signed, transit ISPs doesn’t perform origin validations.
• There is progress at IXes!
# BGP Quadrant

<table>
<thead>
<tr>
<th>Mistake</th>
<th>BGP Hijacks</th>
<th>BGP Route Leaks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IRR Filters; ROA;</td>
<td>IRR Filters; Route Leak Detection Draft</td>
</tr>
<tr>
<td>Malicious</td>
<td>BGPSec</td>
<td>BGPSec</td>
</tr>
</tbody>
</table>
09-28-2017

RFC 8205: BGPsec Protocol Specification
RFC 8206: BGPsec Considerations for Autonomous System (AS) Migration
RFC 8207: BGPsec Operational Considerations
RFC 8208: BGPsec Algorithms, Key Formats, and Signature Formats
RFC 8209: A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests
RFC 8210: The Resource Public Key Infrastructure (RPKI) to Router
RFC 8211: Adverse Actions by a Certification Authority (CA) or Repository Manager in the Resource Public Key Infrastructure (RPKI)
Secure AS_PATH

Everything is signed and validated, no more hijacks! Right?
BGPSec: Bypassed

ROA (178.248.232.0/21, 197068, 32)

ASXXX 🔄 🔄 🔄 🔄 🔄 ASYYY

I don’t know BGPSec

178.248.232.0/21
AS_PATH: ASXXX AS197068

Ok, plain BGP.

ROA check OK!

To secure BGP, do we require attacker to support BGPSec?
Key Findings: BGPSec

BGPSec can be used to:
  • detect malicious hijacks at 100% adoption rate!

In reality:
  • Great computation cost;
  • Backward compatibility makes it vulnerable;
  • Nobody is going to use BGPSec!
# BGP Quadrant

<table>
<thead>
<tr>
<th>Mistake</th>
<th>BGP Hijacks</th>
<th>BGP Route Leaks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRR Filters; ROA;</td>
<td></td>
<td>IRR Filters; <a href="#">Route Leak Detection Draft</a></td>
</tr>
<tr>
<td>Malicious</td>
<td>!</td>
<td>!</td>
</tr>
</tbody>
</table>
BGP Evacuation Plan?
You can’t fix all BGP issues now

But you can make it a safer place
What Can Transit Do?

- IRR filters at all customer links, no exceptions!
- Work with customers, that corrupt AS-SETs;
- Ad-hoc filtering (NTT Peering Lock);
- Consider using IRR filters with your private peers;
- Perform constant BGP monitoring.
What Can IXes Do?

- IRR filters at all links, no exceptions!
- Work with customers, that corrupt AS-SETs;
- Ad-hoc filtering (NTT Peering Lock);
- Consider using ROA validation at RS.
What Can Multihomed Do?

• Keep route objects up to date;
• Keep AS-SETs up to date;
• Create ROA records;
• Perform constant BGP monitoring.
Questions and comments?
Legal Barriers to Securing the Routing Architecture

Christopher S. Yoo
David A. Wishnick
Global RPKI Deployment

ARIN’s repository appears less utilized than others (Cartwright-Cox, 2018)
Law and Routing Security

- Non-legal barriers are more significant than legal ones
  - Limited demand for RPKI
  - Limited budgets
  - Chicken-and-egg problem
  - BUT growing interest appears to be changing the balance
- Legal issues create institutional barriers
  - Legal agreements increase friction inside organizations
  - Legal controversy and uncertainty exacerbate the chicken-and-egg problem
Areas Where We Have Already Made Progress

- Remove indemnification, arbitration, and choice-of-law clauses for appropriate government entities
- Potentially embed click-through approval of RPA in validator software distributions
- Potentially revise the prohibited conduct clause to permit sharing of RPKI-derived information in a machine readable format
Legal Structure of TAL Access

- Leading validator software comes preloaded with all TALs except ARIN’s

The Trust Anchor Locator (TAL) files for four Regional Internet Registries are included with this distribution: AFRINIC, APNIC, LACNIC and RIPE NCC.

To access ARIN's TAL, you will have to agree to ARIN's Relying Party Agreement. Please visit this ARIN web page for more information:

https://www.arin.net/resources/rpki/tal.html

- Four Regional Internet Registries (RIRs) allow access to TALs without agreements
- ARIN requires acceptance of a Relying Party Agreement (RPA)
Potential Strategies to Improve TAL Access

- Keep ARIN’s RPA, but enable software implementations that require click-through acceptance of the RPA
- Keep ARIN’s RPA, but remove the indemnification clause
- Eliminate ARIN’s RPA
Three Ways to Form a Contract

- Click-through or clickwrap – requires explicit acceptance of terms and conditions
- Browsewrap – posts terms and conditions next to the button for downloading software and infers that download = acceptance
- Posting terms and conditions on a separate webpage

- Clickwrap and browsewrap are likely to form contracts
- Simply posting terms and conditions is unlikely to form contracts under U.S. law
Comparison to Other Resources

- Many resources are provided without RPAs
  - Comodo TLS/SSL root
  - DNSSEC root (IANA)
  - AfriNIC, LACNIC RPKI repositories

- Many resources are provided “as is” via browsewrap licenses
  - Geotrust TLS/SSL root
  - RIPE NCC RPKI repository
Evaluating Keeping/Eliminating the RPA

- Primary arguments *in favor of* eliminating the RPA
  - Would ensure the widest possible distribution of RPKI keys
  - Is not required by other resources, such as DNSSec

- Primary arguments *against* eliminating the RPA
  - Would eliminate “as is” disclaimer relied on in many other contexts
  - Would leave allocation of risk to ex post litigation

- Ultimate choice depends on how the community would like to resolve the tradeoffs
Evaluating Exclusive Reliance on “As Is”

- **Arguments in favor**
  - Would bring ARIN in line with other RIRs
  - Would ensure reasonable risk-sharing
    - Depends on the community understanding best-practices compliance (RFC 7115)
    - Should be backed by clear disclosure in ARIN’s Certification Practice Statement
    - Example: adopt policies that do not automatically treat “unknown” as “invalid”

- **Arguments against**
  - Would be less protective to ARIN than other agreements (*i.e.*, ISP service agreements)
  - May impose greater costs on ARIN for benefits to the larger community
Legacy Registration Services Agreement (LRSA)

- Debate the merits of decoupling residual ownership of the address space from RPKI by following RIPE NCC’s example of a non-member services agreement
- Depends on recognizing that creating a non-member services agreement would not implicitly validate either position
Next Steps

- Build on current progress
  - Potentially embedding approval of RPA in validator software distribution
  - Potential revisions to the prohibited conduct clause
  - Acknowledgement of exceptions for government entities
- Evaluate proposals to alter ARIN’s RPKI-related agreements
- Evaluate including RPKI in procurement requests
- Address the non-legal barriers to RPKI adoption
- Engage in dialogue re community-level goals and best practices for routing security
Questions and comments?
This presentation contains projections and other forward-looking statements regarding future events or our future routing performance. All statements other than present and historical facts and conditions contained in this release, including any statements regarding our future results of operations and routing positions, business strategy, plans and our objectives for future operations, are forward-looking statements (within the meaning of the Private Securities Litigation Reform Act of 1995, Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended). These statements are only predictions and reflect our current beliefs and expectations with respect to future events and are based on assumptions and subject to risk and
Why are we doing any of this?

• Creating filters based on public data, forces malicious actors to leave a trail in IRR, WHOIS or other data sources: **auditability**

• **Bugs happen!** – your router may suddenly ignore parts of your configuration, you’ll then rely on your EBGP peer’s filters

• **Everyone makes mistakes** – a typo is easily made
Average view on routing security
Perception: it is hopeless, too many holes…
TOP 18 VIDEO GAMES FINAL BOSSIES OF ALL TIME
 Exhaustive list of issues in the current ecosystem

• IRRdb / database inaccuracy (stale, autopiloted, non-validated)
• IXPs not filtering
• Lack of Path Validation
• Lack of sufficient and good enough software
IRR – what is broken what can be fixed?

• Some IRR dbs do not perform validation
  • Meaning that virtually anyone can create virtually any route/route6 object and sneak those into the prefix-filters

• Eleven relevant IRRs not validating: RIPE, NTTCOM, RADB, ALTDB, ARIN IRR, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE

• Two solutions:
  • Lock the database down (RIPE / RIPE-NONAUTH)
  • Filter on the mirror level
RIPE NWI-5 proposal & implementation

• RIPE NCC’s IRR previously allowed anyone to register any non-RIPE-managed space if it had not yet been registered. *DANGER*
• The “RPSL” password & maintainer was used for this

Three steps were taken:
• Cannot register non-RIPE-managed space any more
• All non-RIPE space moved to separate “RIPE-NONAUTH” database
• Route/route6 ASN authorization rules have been improved

More info: https://www.ripe.net/manage-ips-and-asns/db/impact-analysis-for-nwi-5-implementation
OK – so current status

• Ten relevant IRRs not validating: NTTCOM, RADB, ALTDB, ARIN IRR, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE

• Done: RIPE
ARIN IRR allows anyone to register anything

hanna:~ job$ whois -h rr.arin.net 2001:67c:208c::
% This is the ARIN Routing Registry.
% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '2001:67c:208c::/48AS15562'

route6: 2001:67c:208c::/48
descr: 2001:67c:208c::/48 - Job's net
remarks: Job asked me to steal his net. Honest!
origin: AS15562
mnt-by: MNT-ATTW-Z
source: ARIN # Filtered
ARIN community also recognized this is an issue

- Consultation at [NANOG](https://www.nanog.org) and through [ARIN-Consult](https://lists.arin.net) mailing list
- [https://teamarin.net/2018/07/12/the-path-forward/](https://teamarin.net/2018/07/12/the-path-forward/)

“Improve, or kill it”
OK – so current status

• Nine relevant IRRs not validating: NTTCOM, RADB, ALTDB, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE
• Done: RIPE, ARIN IRR

• How to deal with the remaining nine … ?
• Not all of these are so easily communicated with, not all are really actively managed
The “IRR” system access

• The IRR is access through predominantly two “gateways”
  • whois.radb.net (the bgpq3 and peval default)
  • rr.ntt.net

• All mirroring is essentially done with one software: IRRd

Solution: Let’s use the hegemonic duopoly for good!
Improving security at the "aggregator"?
Proposal: Let RPKI “drown out” conflicting IRR

• RPKI can be used for *BGP Origin Validation* – but also for other things!

• A RPKI ROA is sort of a route-object
  • It has a “prefix”, “origin” and “source” (the root)
  • We can [use RPKI ROAs for provisioning BGP prefix-filters](#)

• Extend IRRd so that when IRR information is in direct conflict with a RPKI ROA – the conflicting information is suppressed ([Github](#))
RPKI filter at the aggregators

Data sources
- RIPE IRR
- NTTCOM
- RADB
- APNIC
- ...

Aggregators
- whois.radb.net
- rr.ntt.net

Client
- bgpq3
RPKI suppressing conflicting IRR advantages

• Industry-wide common method to get rid of stale proxy route objects – by creating a ROA you hide old garbage in IRRs
• By creating a ROA – you will significantly decrease the chances of people being able to use IRR to hijack your resource
OK – so current status

• IRRs not validating: no longer relevant

• Done: RIPE, ARIN IRR, NTTCOM, RADB, ALTDB, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE

NTT & Dashcare have started a full rewrite of IRRd to make this possible:

https://github.com/irrdnet/irrd4
"Filtering at IXPs is hard"

- Many IXPs have come to realize their responsibilities to the Internet ecosystem and the commercial benefits of a more secure product.
- [http://peering.exposed/](http://peering.exposed/)
  - 9 out of top 10 IXPs are filtering, tenth will later this year. **IX.br** making good progress
- IXP filtering has become much easier, there are multiple fully featured configuration generators:
  - [https://www.ixpmanager.org/](https://www.ixpmanager.org/)
  - [http://arouteserver.readthedocs.io/](http://arouteserver.readthedocs.io/)
Route servers must begin dropping RPKI Invalids

• Route servers by definition provide partial Internet tables
• No guarantees whatsoever that a given route will be available via RS
• When a route server drops a prefix, worst case scenario is rerouting – not an outage.
Not everyone needs to do RPKI

• Because of the centralization of the web, if a select few companies deploy RPKI Origin Validation – millions of people benefit

• (google, cloudflare, amazon, pch/quad9, facebook, akamai, fastly, liberty global, comcast, etc…)

• I think only 20 companies or so need to do Origin Validation for there to be big benefits…

• https://dyn.com/blog/bgp-dns-hijacks-target-payment-systems/
“RPKI Origin Validation is useless without Path Validation aka BGPSEC”

• The lack of path validation can be resolved through two methods:
  • Densely peer with each other (Example: Google & Akamai have 126+ facilities in common with each other)
  • An AS_PATH blocking mechanisms like “peerlock”
• Both effectively are “path validation for 1 hop”
• Perhaps “1 hop” already is good enough 😊
“There is no healthy software ecosystem”

- RIPE NCC Validator v3 is works and actively maintained
- NLNetlabs is writing a RPKI Cache Validator (Routinator 3000)
- A company I can’t name is secretly writing one too

- Almost all serious routing vendors have RPKI support (Cisco, Juniper, BIRD, Nokia, FRR – and more are on the way)

- Solution: more users results in better software, start using!
Timeline

• IXPs – start doing RPKI Origin Validation on your route servers now

• Quite some companies are deploying RPKI OV before the end of the year!

• ISPs / CDNs
  • if you are pointing default somewhere, do it now
  • If you are transit-free, wait a

• In 2019 RPKI data will be used to clean up IRR

• Hopefully the ARIN RPKI TAL situation will improve
Conclusion
Questions and comments?
So I Need to Start Route Filtering Peers

Chris Morrow
christopher.morrow@gmail.com
Who’s a Transit ISP?
AS15169?
Route Data Sources

IRR, RPKI, <internal TE>

- IRR data for what peers think they will be sending
- RPKI data where available to validate IRR data
- Internal TE sources to limit further if required
Procedure

1. Notify peers (howdy!) that this is going to start happening

2. Collect data regularly (daily?)

3. Parse and place into internal data service

4. Create per-ASN filter content

5. Apply changes to network device(s)

6. Mark today, drop tomorrow
Notification
Notify Peers
Notifying peers through standard mechanisms

Portal update to explain timelines and display current data for your ASN

Implement ability to request ‘update because I updated’ by peer(s)

Feedback once this is working will be important
Collect Data
Collect and Parse IRR/RPKI data, easy?
Collection is the ‘simple’ part of the problem

IRR data is relatively easy to find:

ftp://ftp.radb.net/

Decide on which IRR databases to collect and parse.
Parse IRR data
IRR, Y U Be SoWeird?

IRR data is generally formatted

Follow the AS -> Maintainer ->
AS-SET trees... ‘Everyone’ keeps
theirs updated, right?

(these aren’t really IRR problems as
such)

What tooling exists for this
today?

Irrtoolset - no

Bgpq3 - not usable (internal
problems)

Run a local IRRd... doesn’t
actually solve the problem of
making the data available to the
other tooling used
Create per-ASN data/filters
Vendor Neutral Formatting

OpenConfig (OC) sounds right
Request from the internal service
Output for configuration generation
system in OC form

Probably OC is fine
Tooling already knows OC
Tooling may have to know
prefix-list vs route-filter
Application
Apply Changes as Required

When changes arrive, apply them in the normal fashion

Follow existing device configuration processes

New processes are bad/hard/problems
Conclusion

Goal is to start marking routes based on filter inclusion / exclusion by 01/2019
Reject/Drop by 03/2019
Questions and comments?
Open Mic

Questions and discussion
Thank you!

NANOG 74: Security Track