BGP Flexibility and… Its Consequences

Alexander Azimov

Qrator Labs aa@qrator.net

Rights

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

Obligations

- 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.

Obligations

- 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 – that’s all!

BGP Anomalies

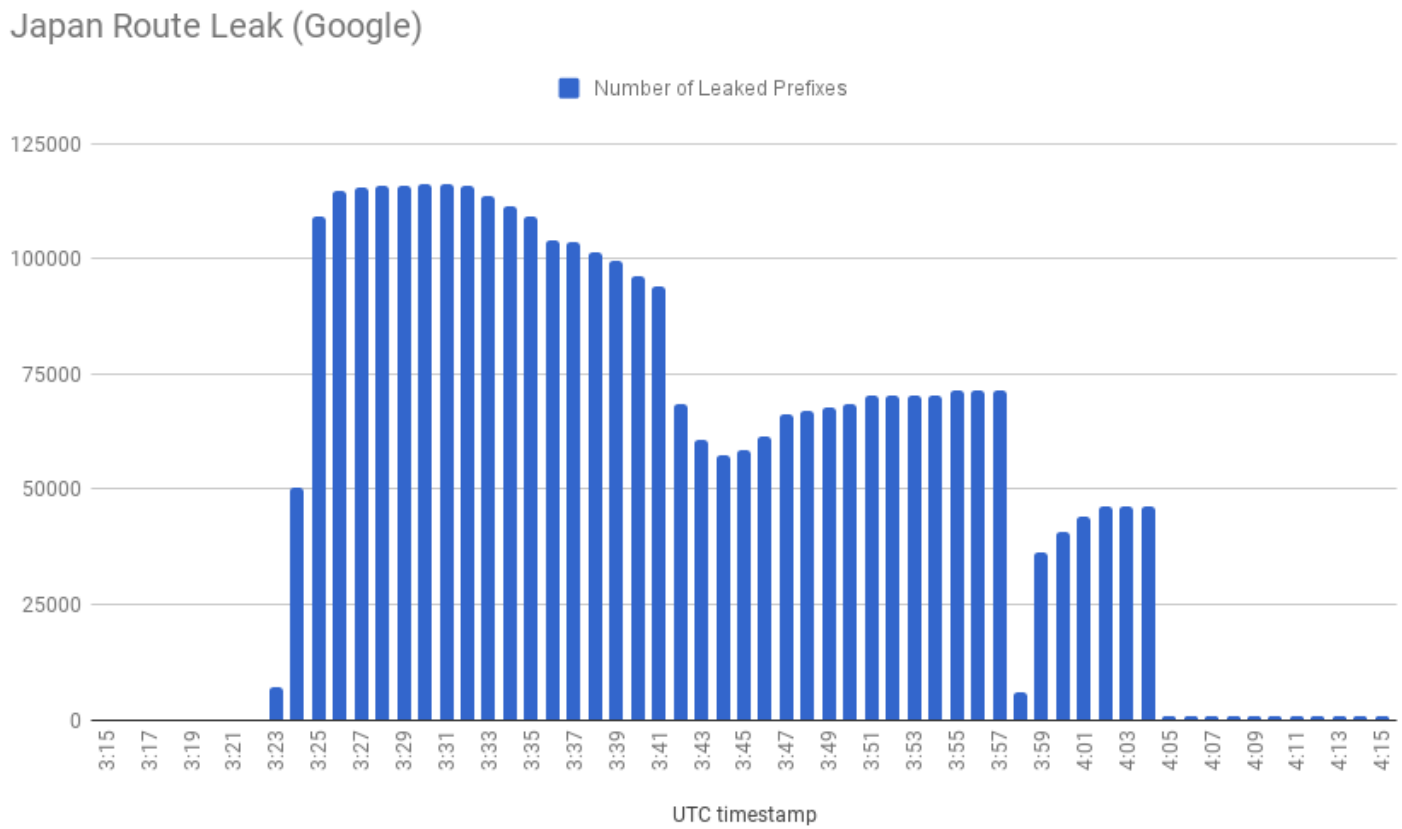
BGP Hijacks

Illegitimate advertisement of foreign address space.

BGP Route Leaks

Illegitimate announce of a route received from peer or upstream to another peer or upstream.

Google



It will ~~never~~ happen again!

BGP in the Headlines

Data Centre ▸ Networks

Google routing blunder sent Japan's Internet dark on Friday

Another big BGP blunder

NATIONAL

Google linked to internet disruptions in Japan

KYODO, STAFF REPORT

Google hijack made Japan 'land of no internet' for more than 30 minutes

Google accidentally broke the internet throughout Japan

A mistake led to internet outages for about half of the country.

24th April
AS10297, ENET, US

BGP Hijack

+

DNS Hijack

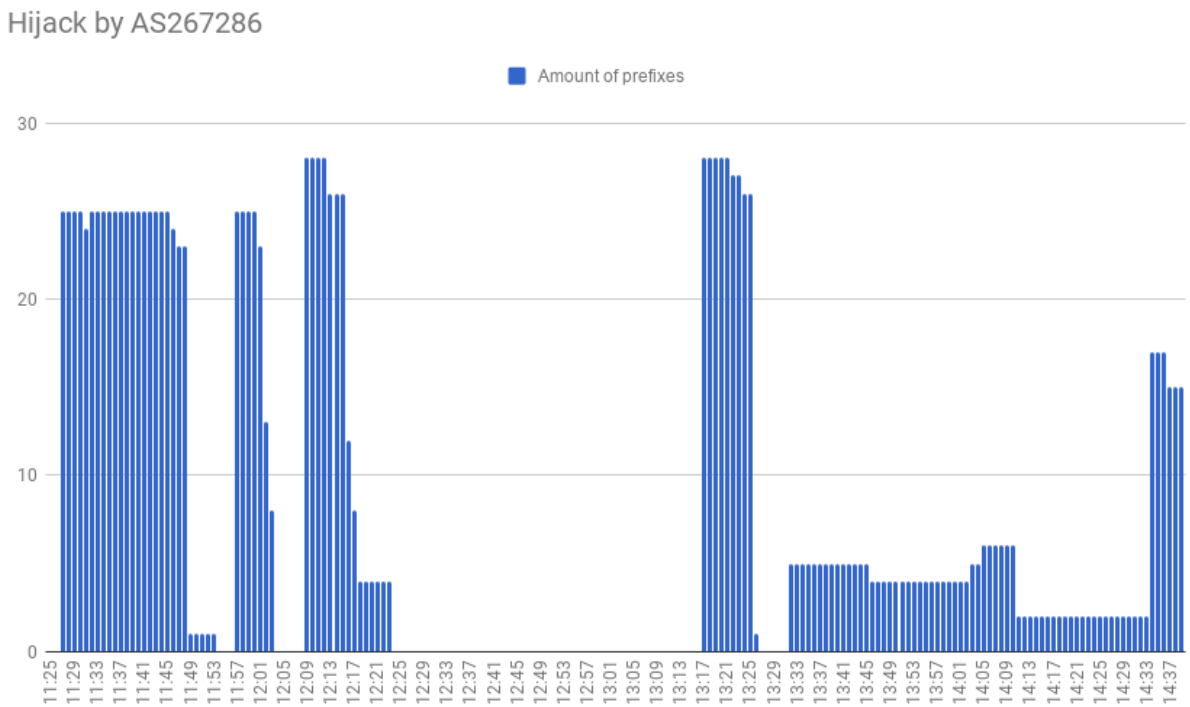
=

Money

https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/

26th April
AS267286, DPSTL, Brazil

~268 million unique IPs



https://radar.qrator.net/blog/bgp-hijacks-malicious-or-mistakes

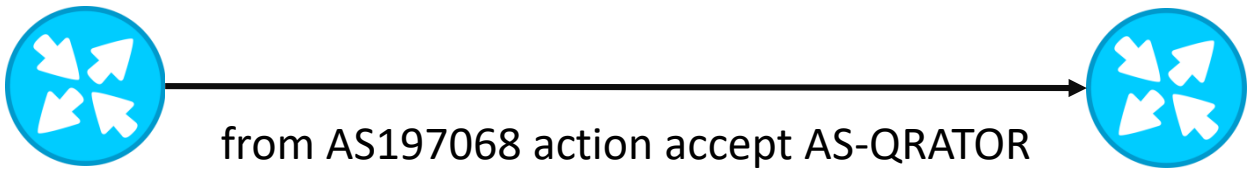
4th May
AS8449, ElCat, KYRGYZSTAN

Route Leak – Connecting People! Oh not?

BGP Exams?

I will never create BGP hijack again.
I will never create BGP hijack again.
I will never create BGP hijack again.
I will never create BGP hijack again.
I will never create BGP hijack again.
I will never create BGP hijack again.
I will never create BGP hijack again.
I will never create BGP hijack again.
I will never create BGP hijack again.
I will never create BGP hijack again.
I will never create BGP hijack again.

BGP Ingress Filtering: AS-SETs



from AS197068 action accept AS-QRATOR

AS-SET to ASNs

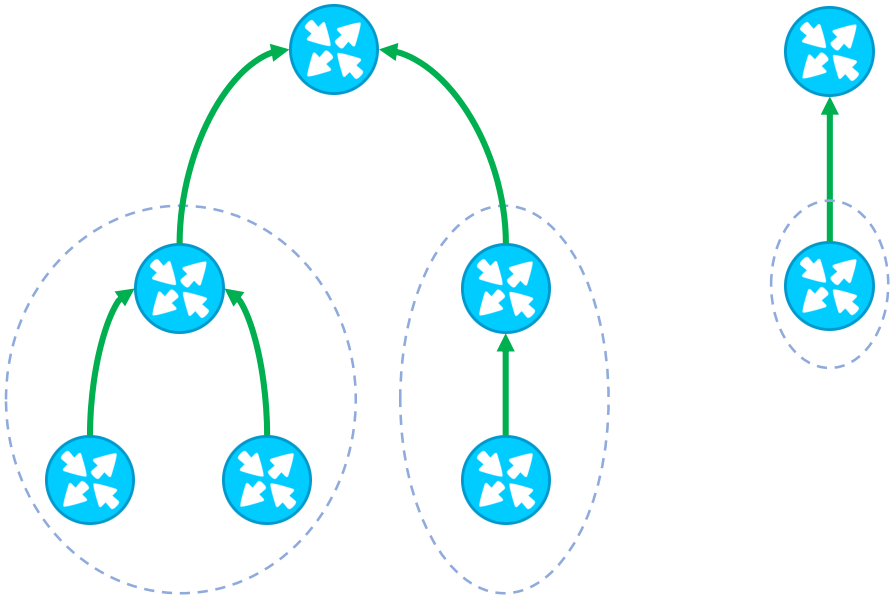
200449, 197068, …….

ASNs to route objects

178.248.232.0/21, 185.65.148.0/22,
45.116.91.0/24, 89.218.31.0/24 …

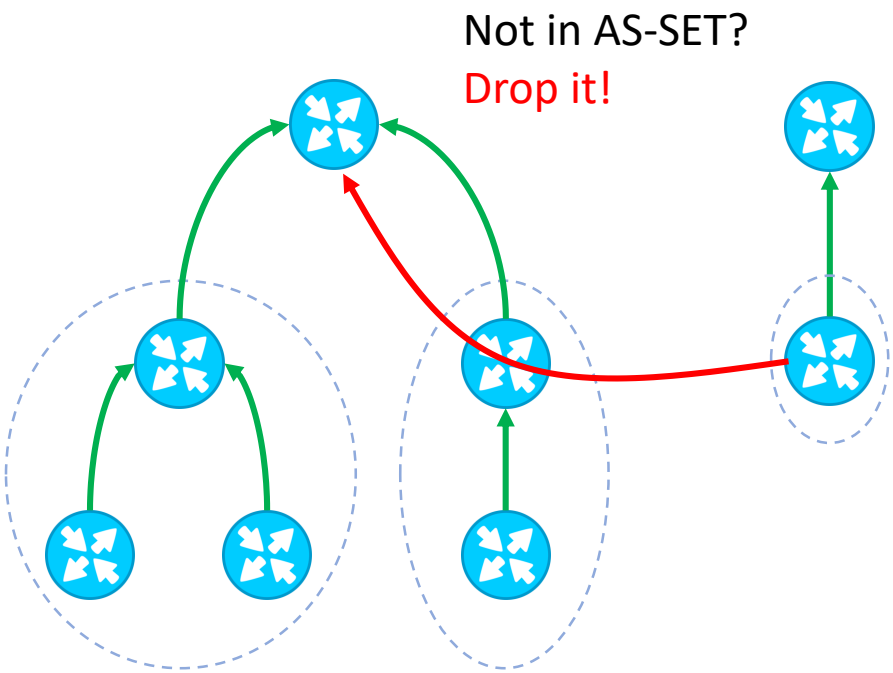
IRR filters doesn’t perform origin validation!

AS-SETs & AS Cone



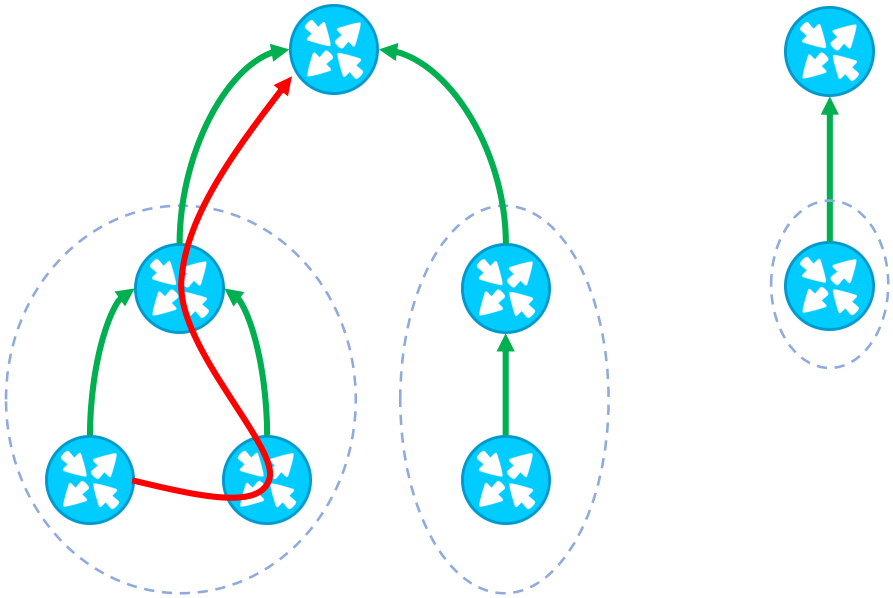
In ‘Ideal World’ AS-SETs = AS Cone

AS-SETs & AS Cone



In ‘Ideal World’ AS-SETs = AS Cone

AS-SETs & AS Cone



In an ‘Ideal World’ AS-SETs = AS Cone
But even then it has limitations.

What Do We Know?

- IRR filters doesn’t perform origin validation;
- AS-SET objects are not authorized (even in RIPE);
- Poorly maintained AS-SETs become less affective;
- There are ISPs does not use any IRR filters.

Investigation

How many filters have been already violated?

Methodology

- Route Object Aggregator (RIPE, APNIC, ARIN, AFRINIC, RADB… 27 sources);
- Analyze prefixes with unique asn in route objects;
- Detect c2p links through which route leaks were propagated;
- Check that origin doesn’t belong to customer cone.

Results

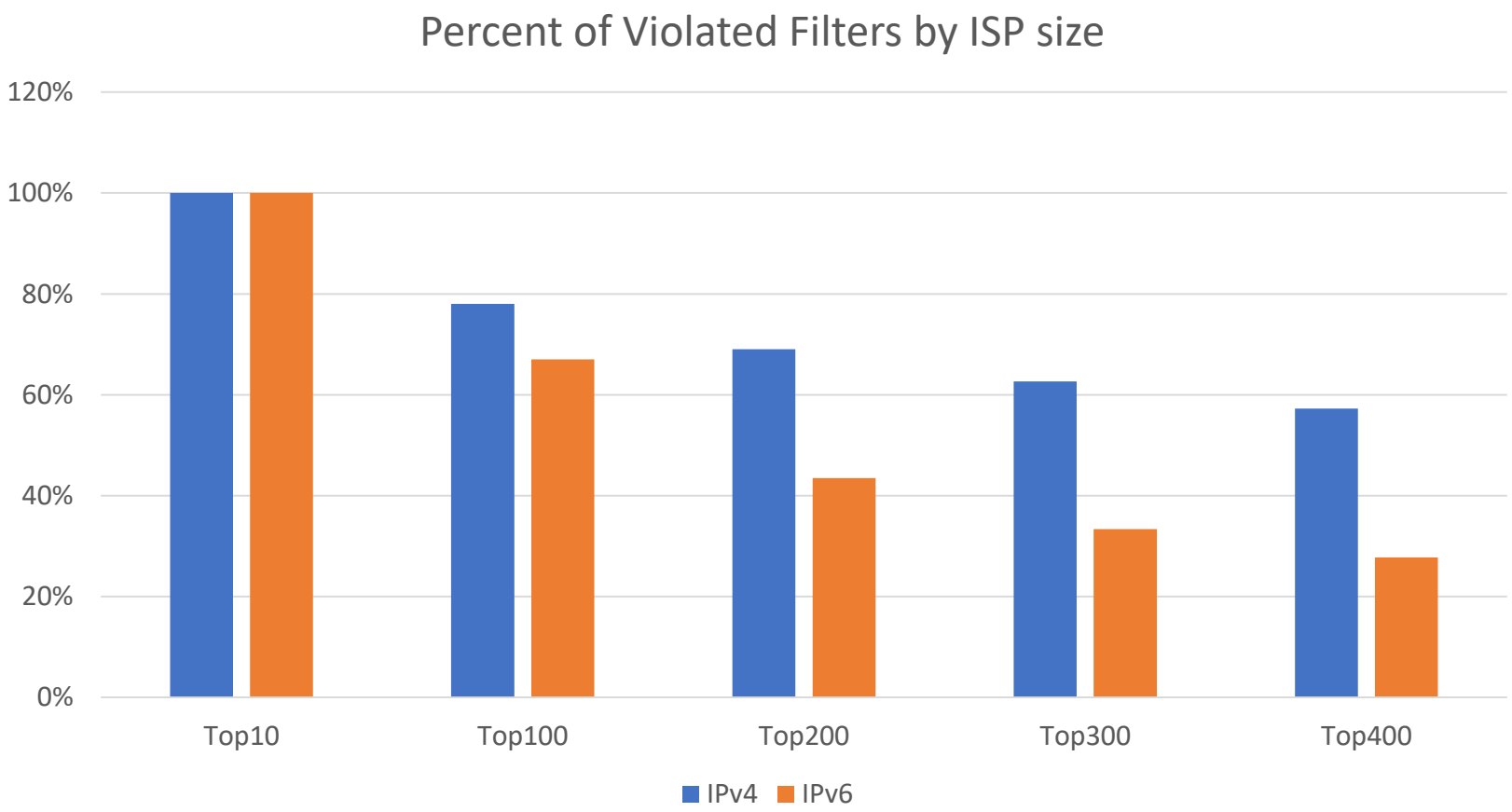
IPv4

At least 7% of ISPs have problems with filters

IPv6

At least 1% of ISPs have problems with filters

Results: Explained



Accepts Leaks originated by Tier1

Russia

IPv4

4809 - China Telecom
4837 - China Unicom
6695 - DECIX
6939 - HE
7363 - YOMURA
7552 - Viettel
7713 - Telkomnet
7843 - TWCABLE
8732 - Comcor
9583 - Sify
12389 - Rostelecom
12586 - GHOSTnet
13536 - TVC-AS1
20485 - TTK
20562 - Opentransit
22356 - Durand
22773 - CXA
31025 - GHOSTnet
35104 - Kaztranscom
40805 - JMFSOLUTIONS
48276 - LEVEL-AS
50384 - W-IX
53211 - ISPRJ

IPv6

6939 - HE
16735 - ALGAR
23106 - Cemig
49697 - Joey-Network
199524 - G-Core

Accepts Leaks originated by Tier1

China

IPv4

4809 - China Telecom
4837 - China Unicom
6695 - DECIX
6939 - HE
7363 - YOMURA
7552 - Viettel
7713 - Telkomnet
7843 - TWCABLE
8732 - Comcor
9583 - Sify
12389 - Rostelecom
12586 - GHOSTnet
13536 - TVC-AS1
20485 - TTK
20562 - Opentransit
22356 - Durand
22773 - CXA
31025 - GHOSTnet
35104 - Kaztranscom
40805 - JMFSOLUTIONS
48276 - LEVEL-AS
50384 - W-IX
53211 - ISPRJ

IPv6

6939 - HE
16735 - ALGAR
23106 - Cemig
49697 - Joey-Network
199524 - G-Core

Accepts Leaks originated by Tier1

IXes

IPv4

4809 - China Telecom
4837 - China Unicom
6695 - DECIX
6939 - HE
7363 - YOMURA
7552 - Viettel
7713 - Telkomnet
7843 - TWCABLE
8732 - Comcor
9583 - Sify
12389 - Rostelecom
12586 - GHOSTnet
13536 - TVC-AS1
20485 - TTK
20562 - Opentransit
22356 - Durand
22773 - CXA
31025 - GHOSTnet
35104 - Kaztranscom
40805 - JMFSOLUTIONS
48276 - LEVEL-AS
50384 - W-IX
53211 - ISPRJ

IPv6

6939 - HE
16735 - ALGAR
23106 - Cemig
49697 - Joey-Network
199524 - G-Core

Accepts Leaks originated by Tier1

Hurricane Electric!

IPv4

4809 - China Telecom
4837 - China Unicom
6695 - DECIX
6939 - HE
7363 - YOMURA
7552 - Viettel
7713 - Telkomnet
7843 - TWCABLE
8732 - Comcor
9583 - Sify
12389 - Rostelecom
12586 - GHOSTnet
13536 - TVC-AS1
20485 - TTK
20562 - Opentransit
22356 - Durand
22773 - CXA
31025 - GHOSTnet
35104 - Kaztranscom
40805 - JMFSOLUTIONS
48276 - LEVEL-AS
50384 - W-IX
53211 - ISPRJ

IPv6

6939 - HE
16735 - ALGAR
23106 - Cemig
49697 - Joey-Network
199524 - G-Core

Key Findings: AS-SETs

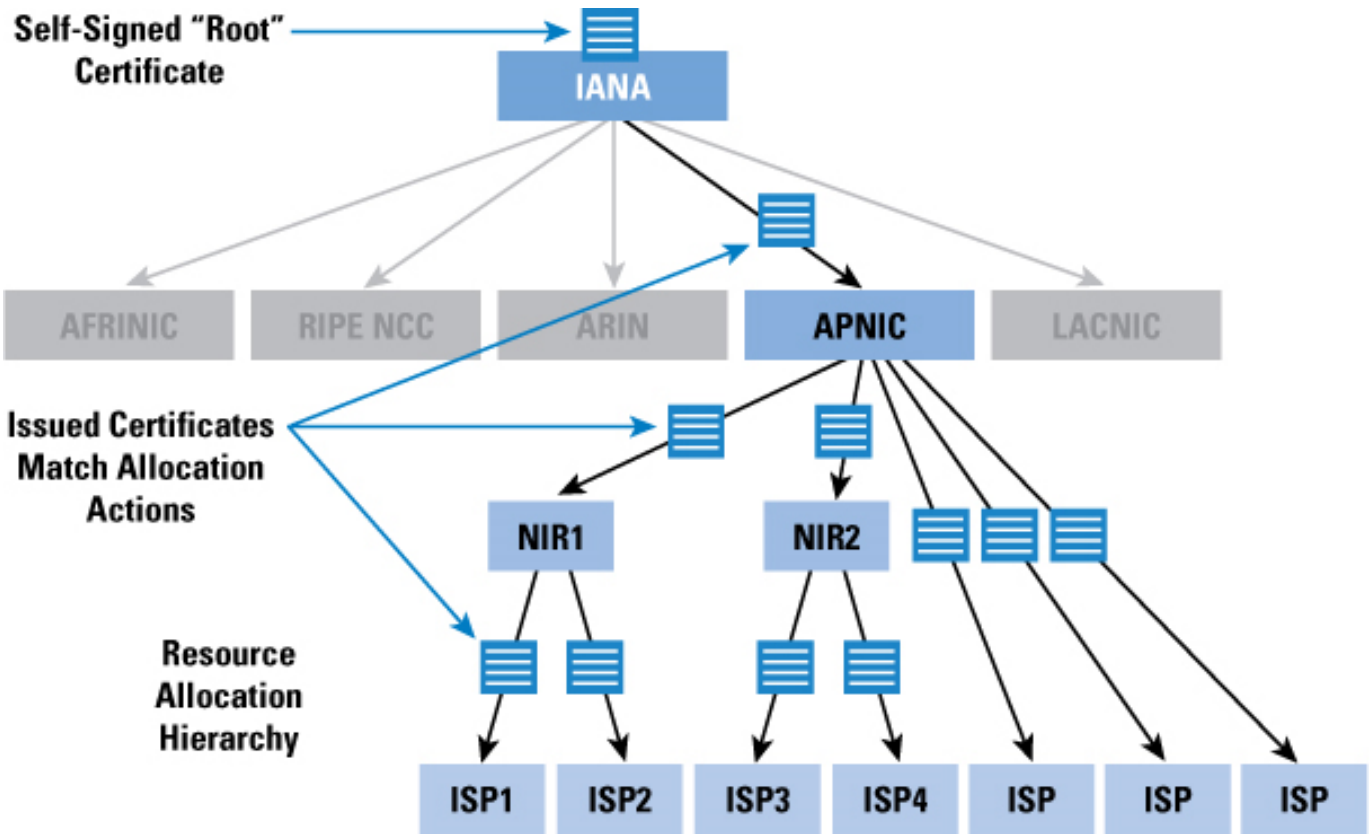
AS-SET Can be Used to:

- 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 exceeds *maximum length*;

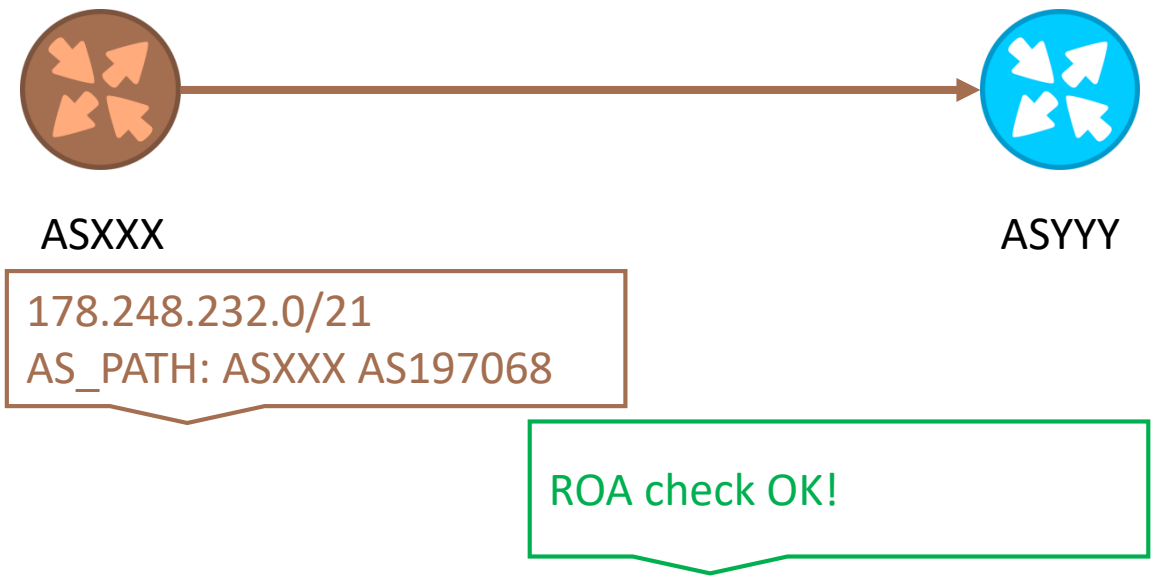
Unknown – ROA that covers *prefix* does not exist.

But you can’t retrieve all valid prefixes for an *asn*!

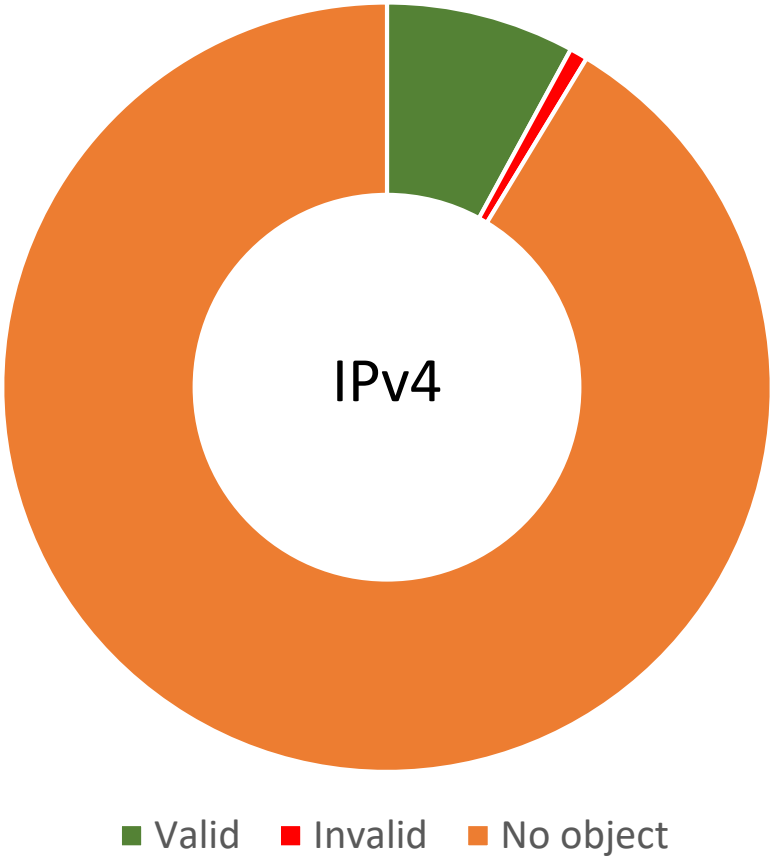
Integration with AS-SET? Ooops…

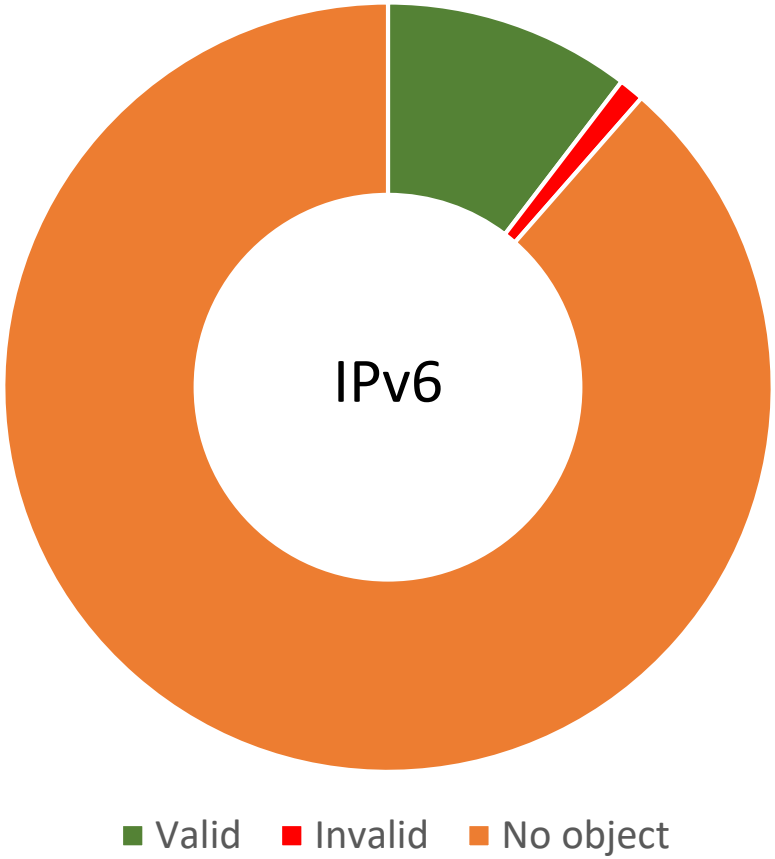
ROA Validation: AS_PATH Violation

ROA (178.248.232.0/21, 197068, 32)

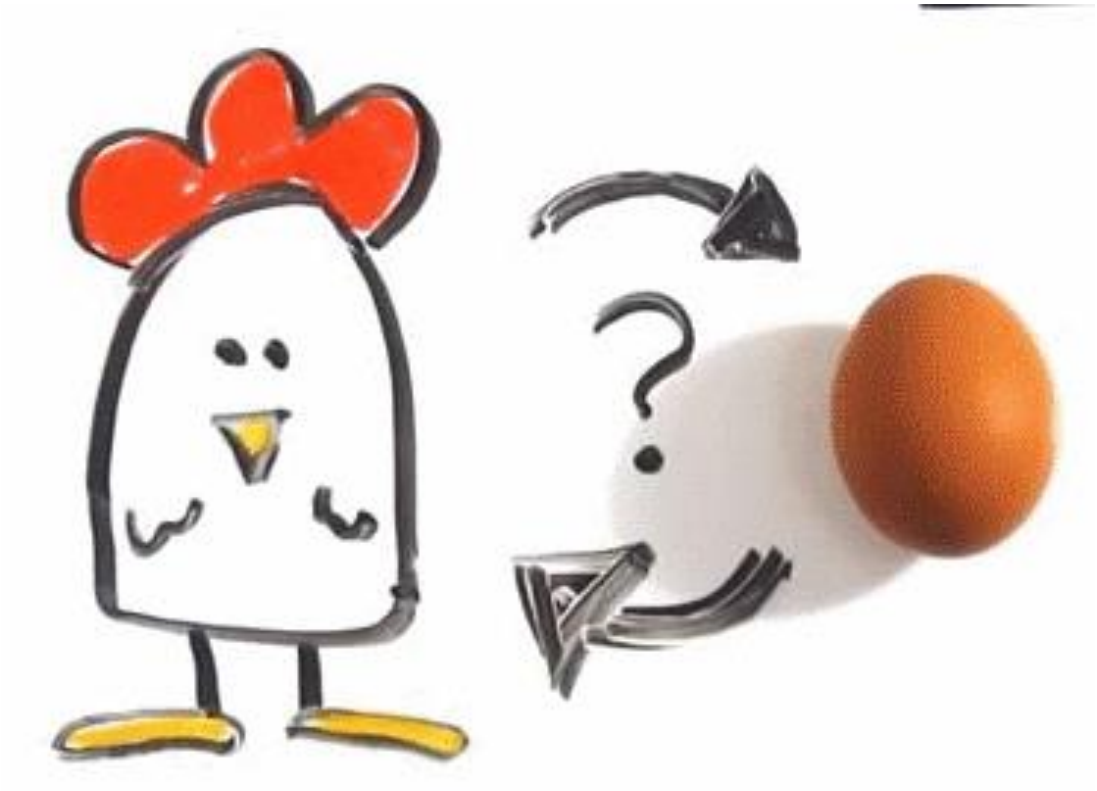


ROA Records





No ROA validation – no ROAs?



Key Findings: ROA validation

ROA Validation Can be Used to:

- filter mistake hijacks;

ROA Validation Can't:

- filter route leaks;
- filter malicious hijacks.

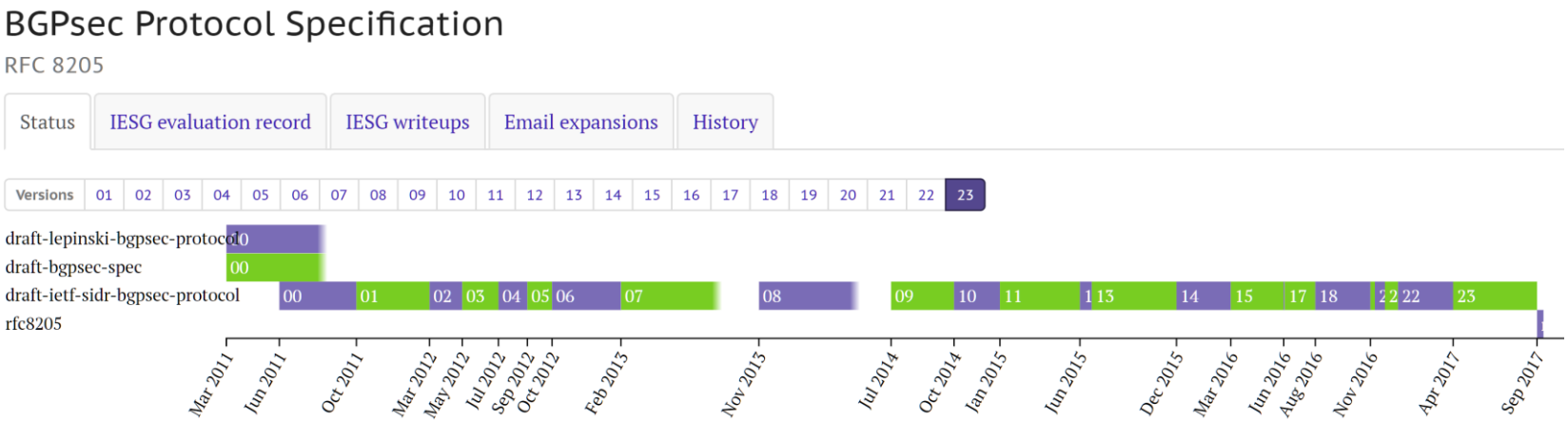
In reality:

- Only 10% of prefixes are signed;
- Transit ISPs doesn't perform origin validations.

BGP Quadrant

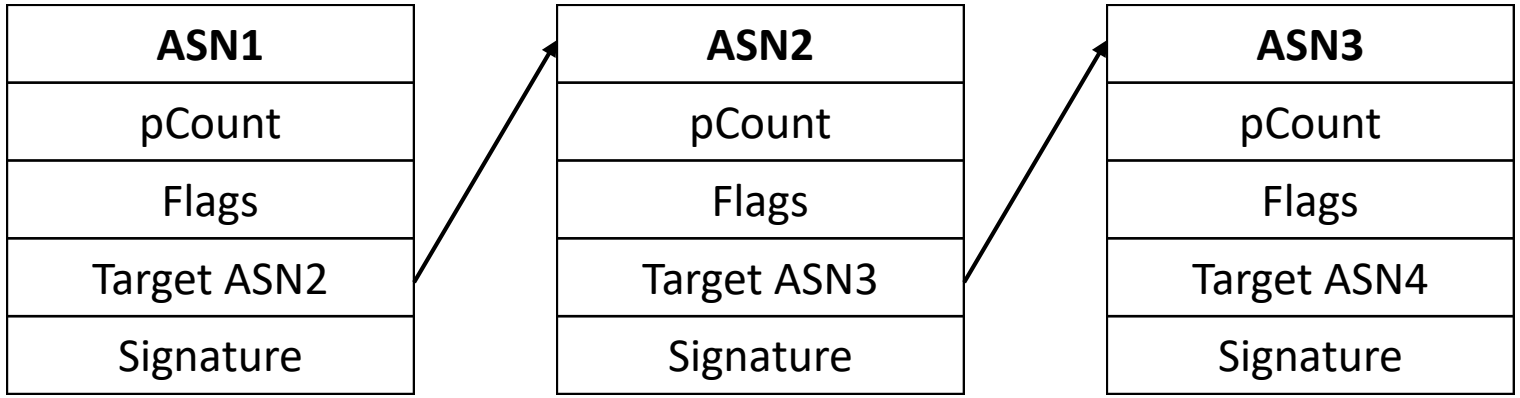
	Hijacks	Route Leaks
Mistake	IRR filters; ROA Validation.	IRR filters; draft-ietf-idr-bgp-open-policy draft-ymbk-idr-bgp-eotr-policy draft-ietf-idr-route-leak-detection-mitigation
Malicious	BGPSec	BGPSec

28.09.2017



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)

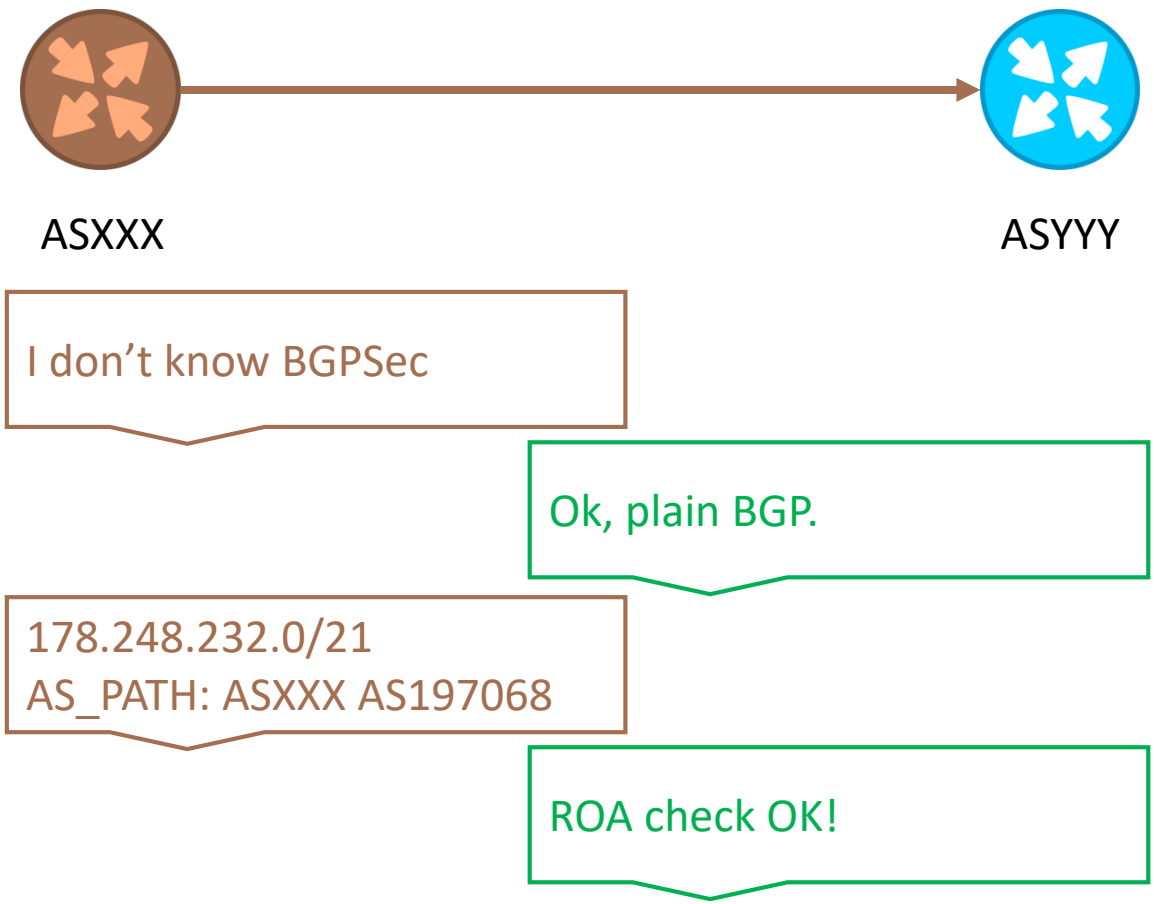
AS_PATH Validation



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

BGPSec: Backward Compatibility

ROA (178.248.232.0/21, 197068, 32)



Key Findings: BGPSec

BGPSec Can be Used to:

- make things more complicated.

In reality:

It seems that authors forgot the goal.

BGP Quadrant

	Hijacks	Route Leaks
Mistake	IRR filters; ROA validation.	IRR filters; draft-ietf-idr-bgp-open-policy draft-ymbk-idr-bgp-eotr-policy draft-ietf-idr-route-leak-detection-mitigation
Malicious	!	!

What can YOU do?

What Can Transit Do?

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

What Can IX Do?

- IRR filters at all links, no exceptions!
- Work with customers, that corrupt AS-SETs.
- Remove legacy filters (LOA, route-sets);
- 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 (RIPE Wizard);
- Perform constant BGP monitoring.