

Measuring RPKI adoption and impact

Cecilia Testart
06.11.2023

About Me

Assistant Professor

School of Cybersecurity and Privacy & School of Computer Science

Georgia Institute of Technology

Email: ctestart@gatech.edu

Research Area: Internet Security and Policy, Internet Measurements

Teaching: Computer Networks, Internet Security

Motivation: Internet for Society

Previously: PhD@MIT, MS Technology and Policy, BSc in Industrial Engineering

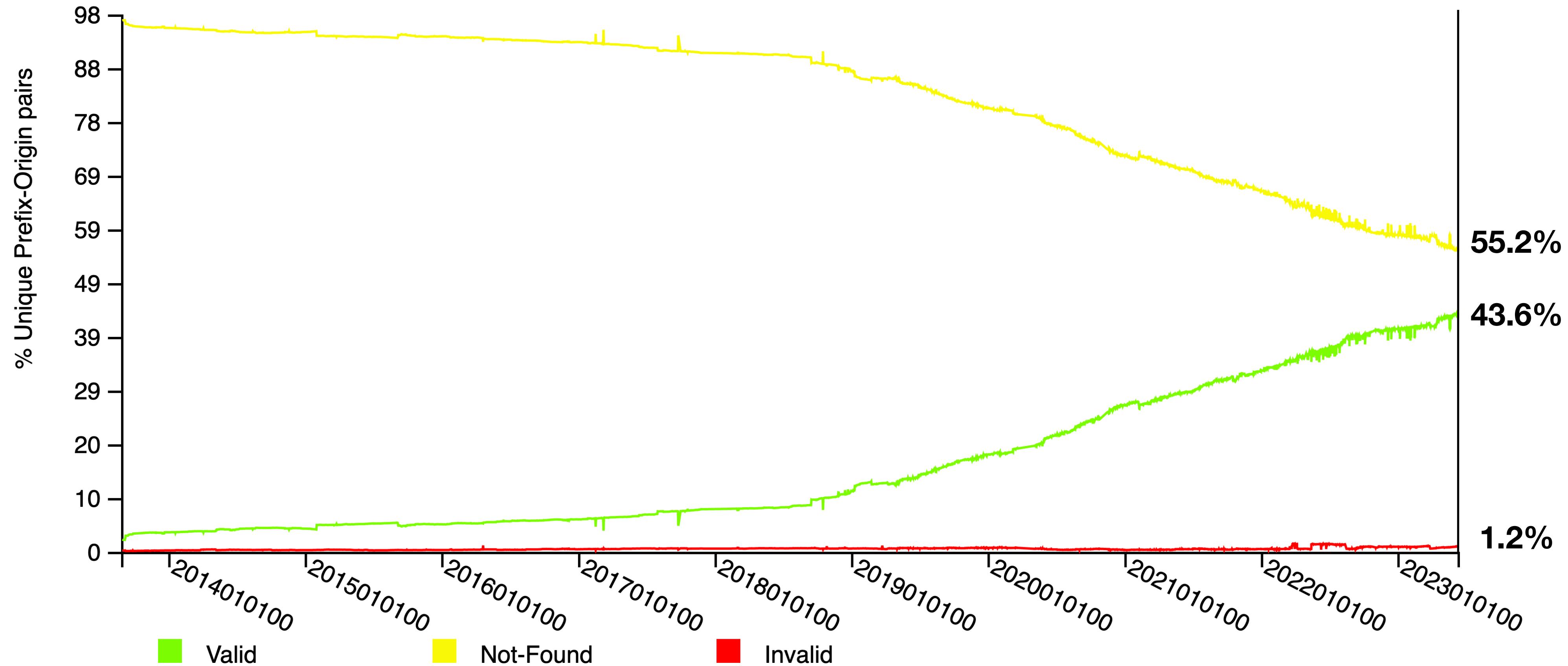
Research questions

- How is RPKI adoption evolving over time?
 - Coverage of routed prefixes by ROAs
 - Deployment of ROV
- What is the impact of RPKI adoption?
 - Spread of RPKI-invalid BGP updates
 - BGP hijacking

Coverage of Routed Prefixes

BGP prefixes covered by ROA over time from NIST

RPKI-ROV History of Unique Prefix-Origin Pairs (IPv4)



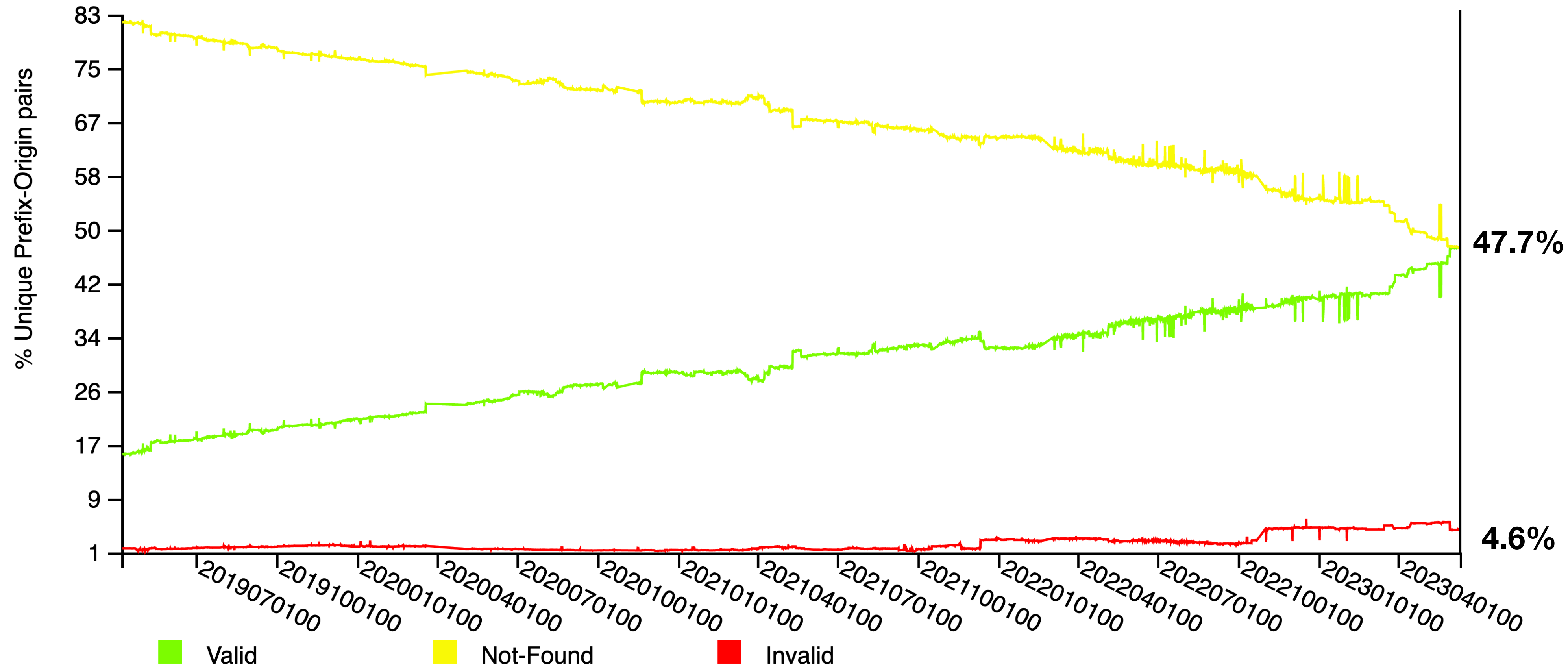
NIST RPKI Monitor: RPKI-ROV Analysis

Protocol: IPv4

RIR: All

BGP prefixes covered by ROA over time from NIST

RPKI-ROV History of Unique Prefix-Origin Pairs (IPv6)



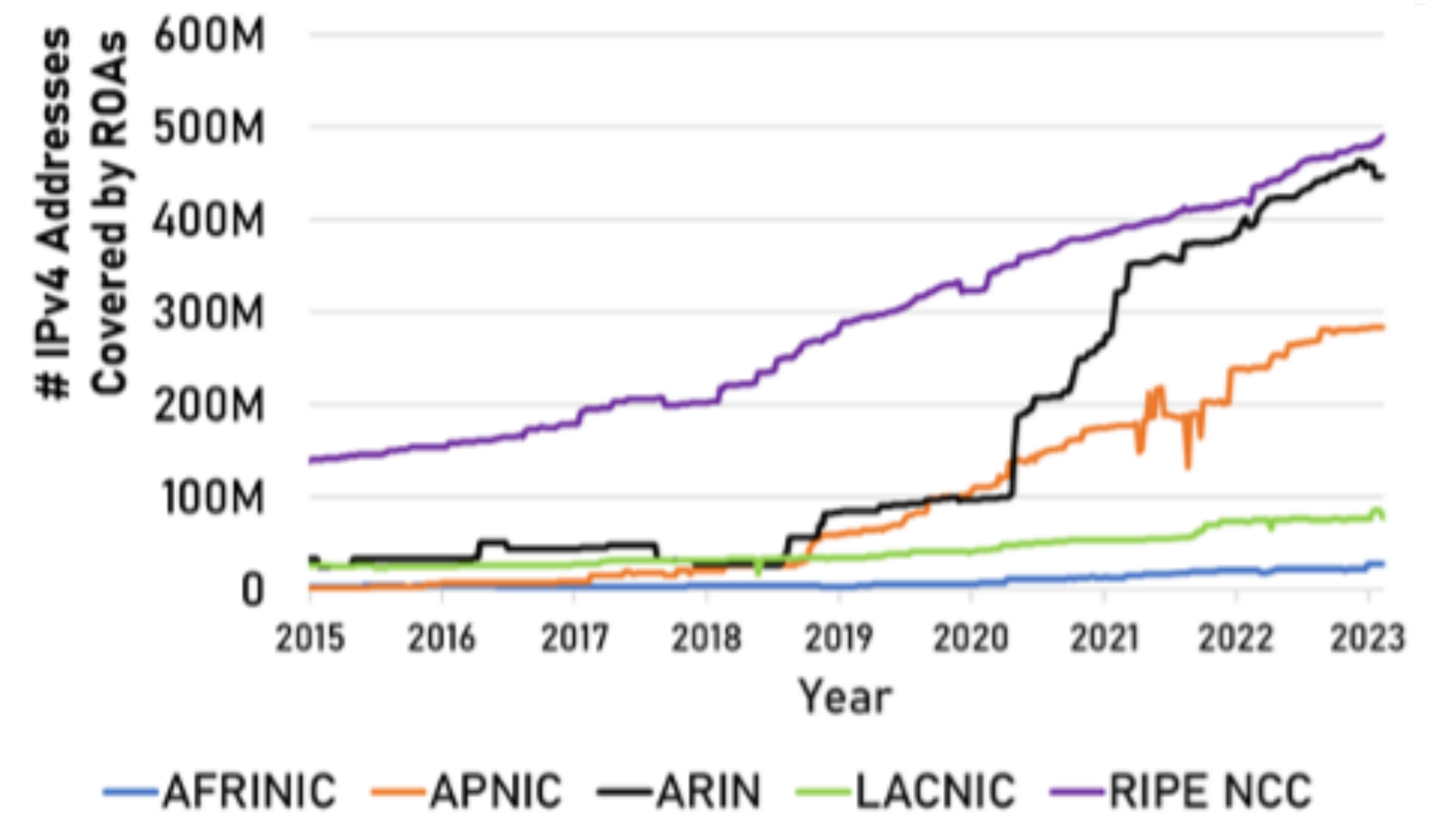
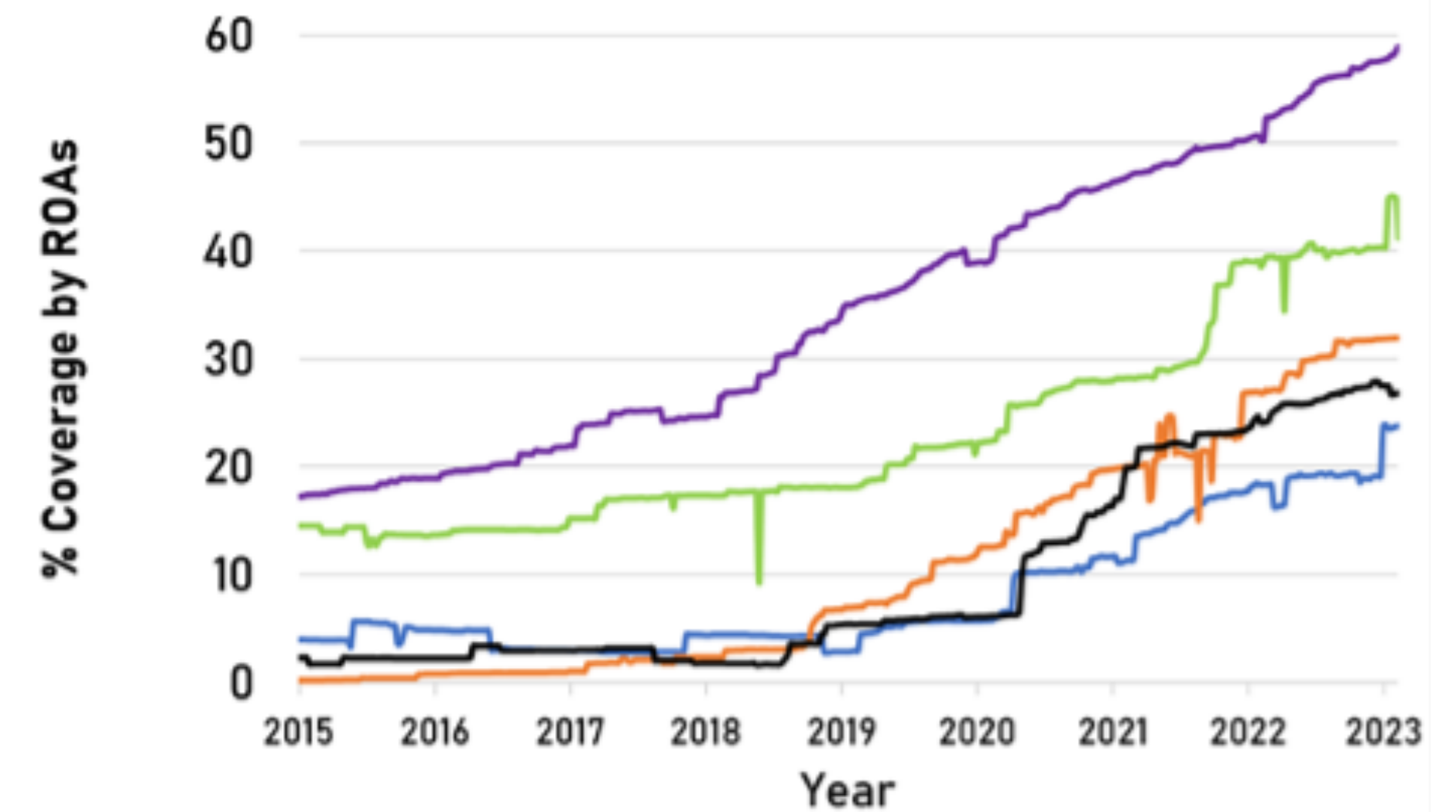
NIST RPKI Monitor: RPKI-ROV Analysis

Protocol: IPv6

RIR: All

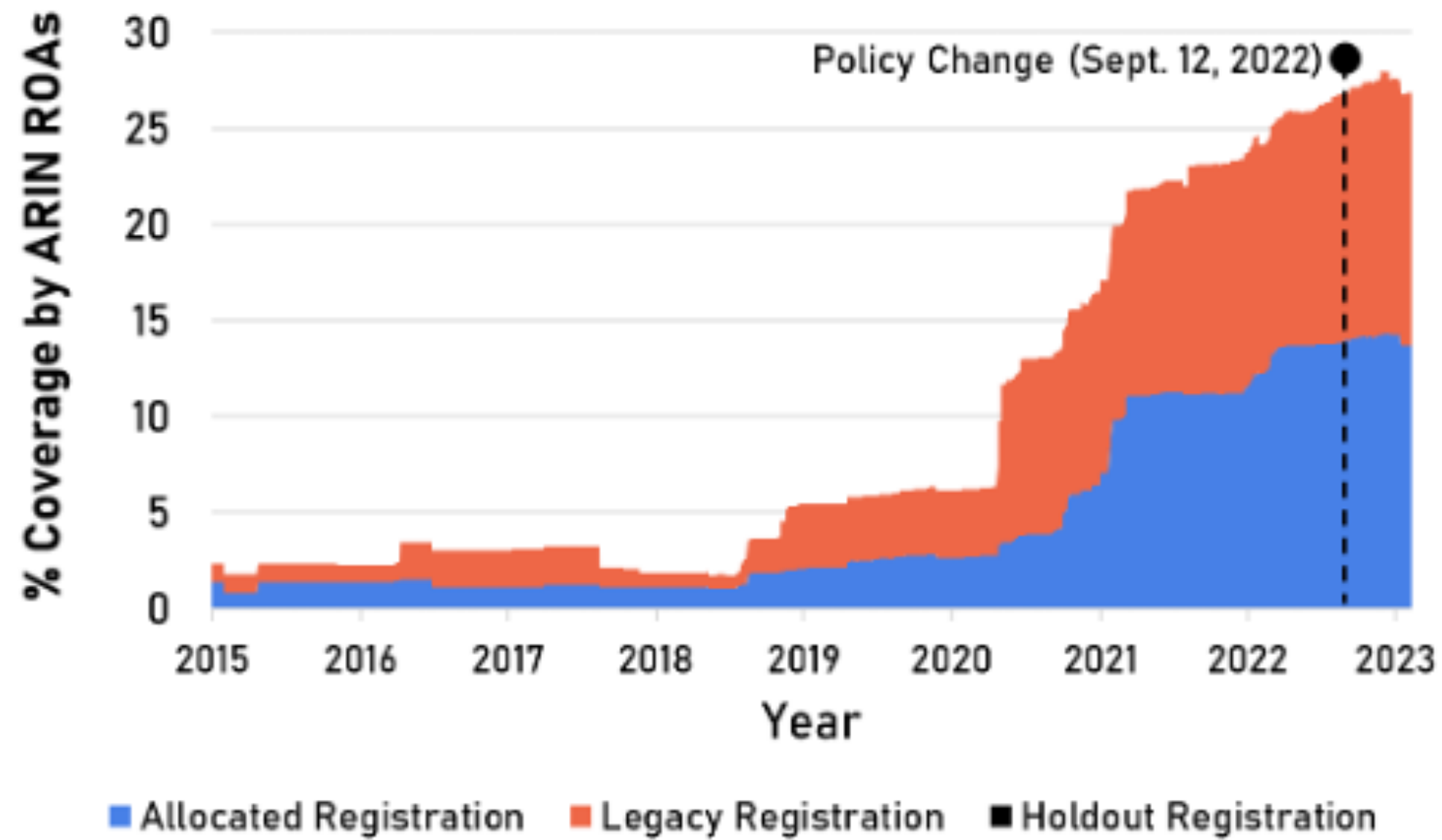
ARIN singularity

- ARIN required legal agreements to:
 - issue ROAs,
 - access ROAs (RPKI TAL),
 - publish ROAs in machine readable way.
- Legacy addresses treated differently.
- Requirements changed in Sept 2022.



Based on work by Noah Craft (MSc Student)

Legacy IP addresses

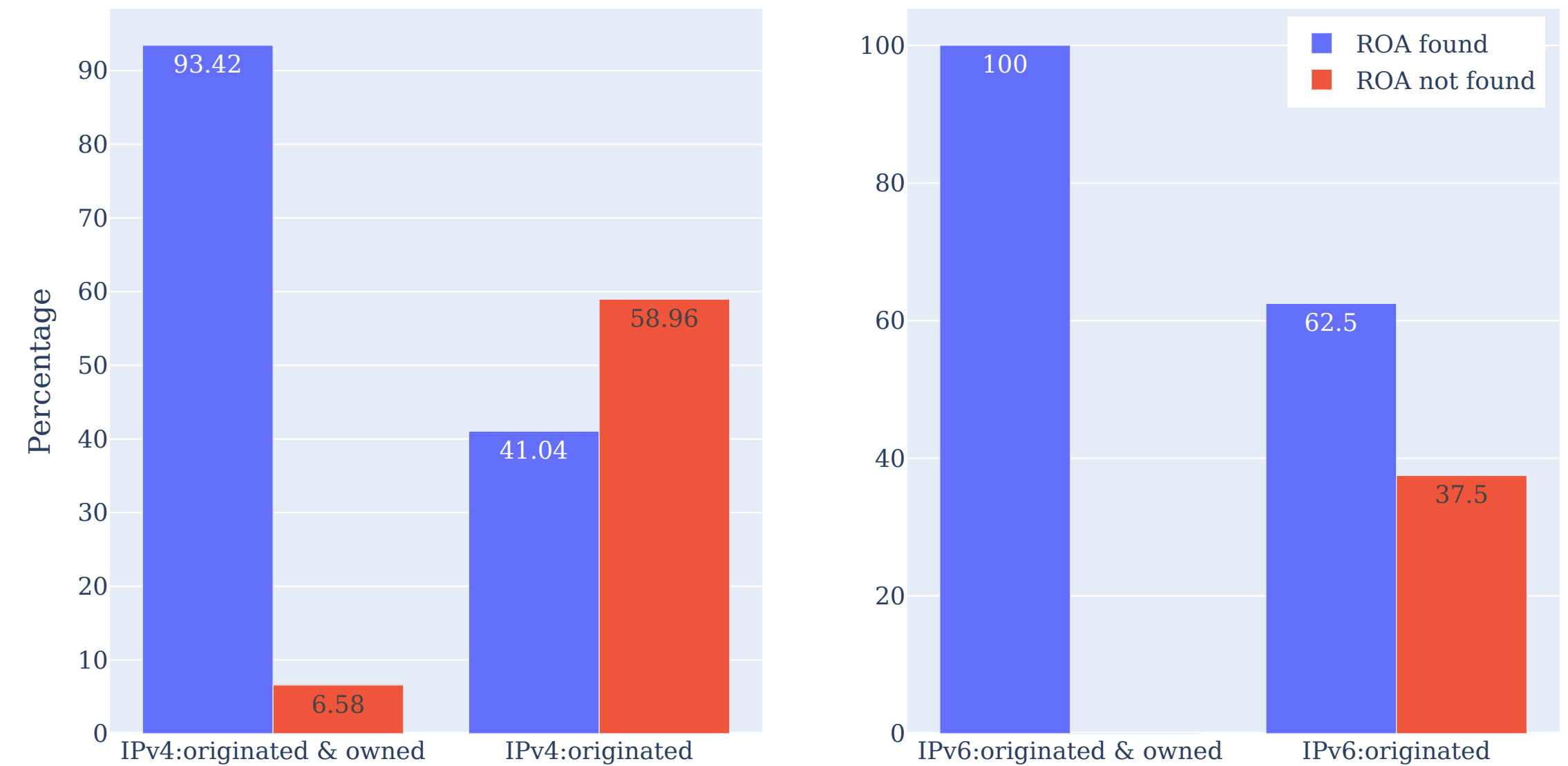


Organization	/8 legacy holdout count	Other Prefixes covered by ROAs
Apple	1	No
AT&T	1	Yes
Cogent	1	Yes
DISA	12	No
Ford	1	No

ROA coverage by organization vs. by ASN

Case study of IJ ROA Coverage

- Originated prefixes ~ 41%
- Originates & Owned ~ 93%



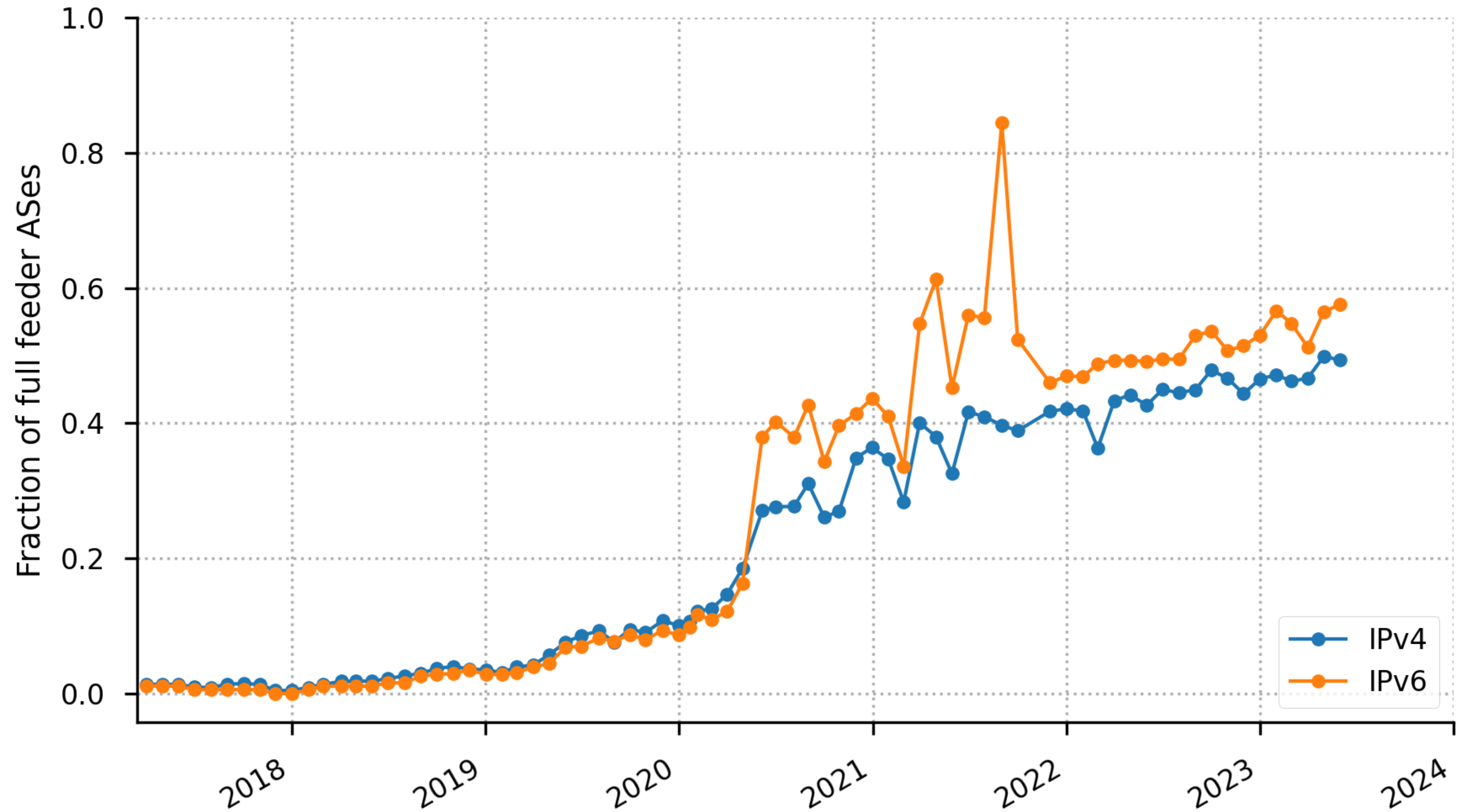
ROA coverage by organization vs. by ASN

Org by prefix origination	% Prefixes	# Orgs	ROA Coverage (%)		
No AS	13.53	29765	47.23	←	Should be easy but org. challenges
Originates only by own AS	10.12	23737	35.28	←	Should be easy but org. challenges (?)
Originates by self & others	10.61	8906	33.65	←	Afraid of mess
Originates self & others	12.38	10641	50.58	←	Less afraid of mess
Originates self & others by self & others	53.36	5594	42.98	←	Messy but large orgs

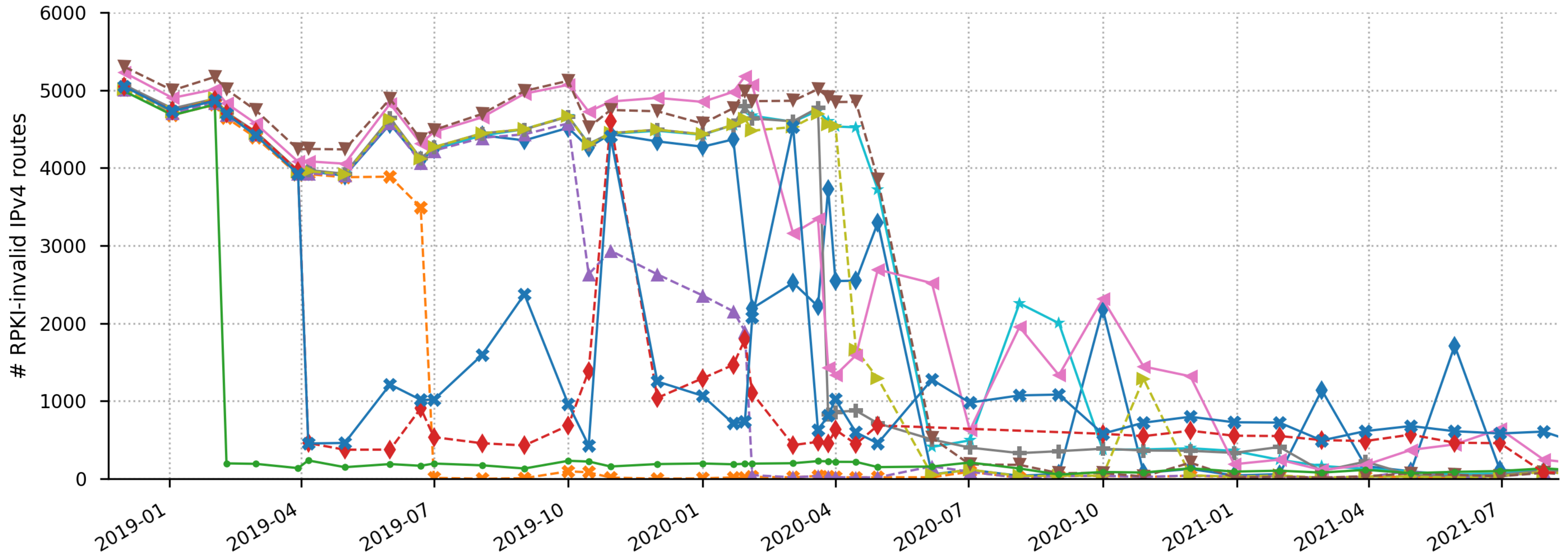
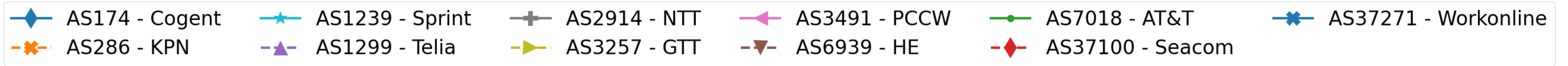
ROV Deployment

ROV deployment in ASes peering with BGP collectors

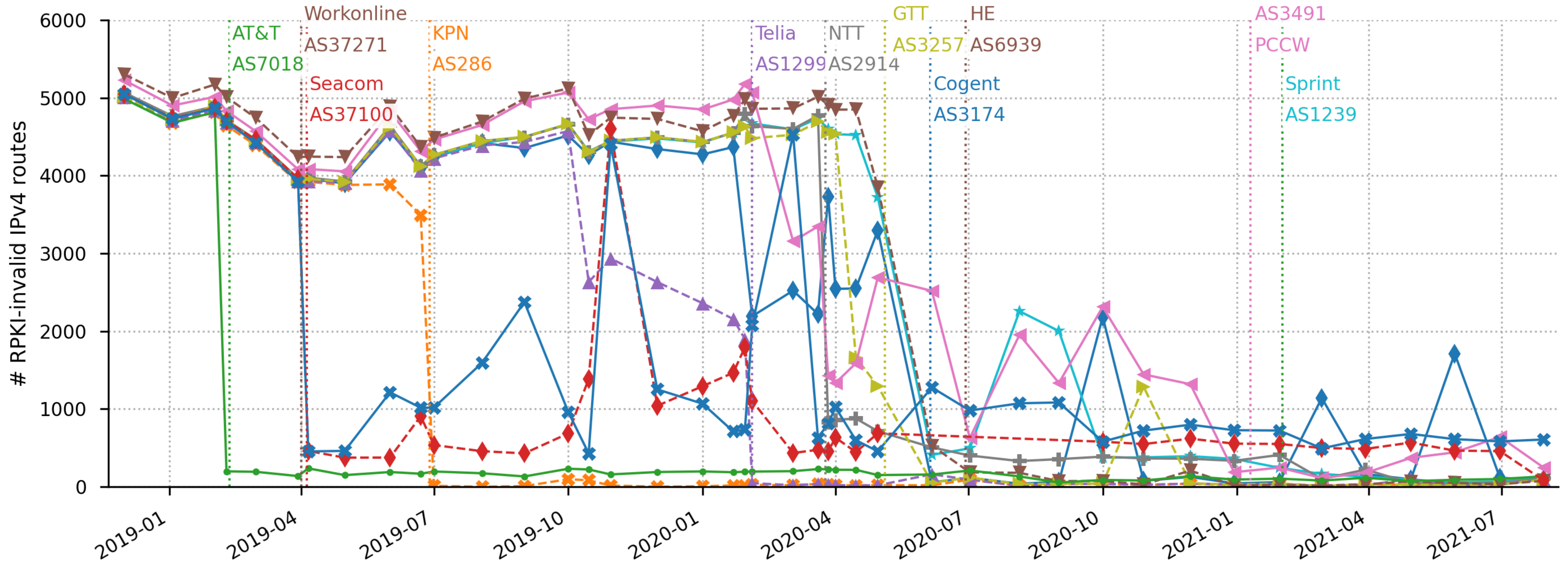
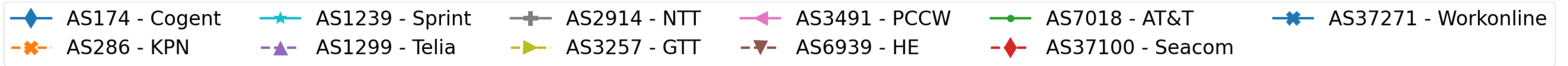
- BGP collectors peers in 2023:
 - IPv4: 315-320 ASNs
 - IPv6: 280-290 ASNs
- ROV ASNs 06/2023
 - IPv4: 155
 - IPv6: 163
- Unique ROV ASNs: 303



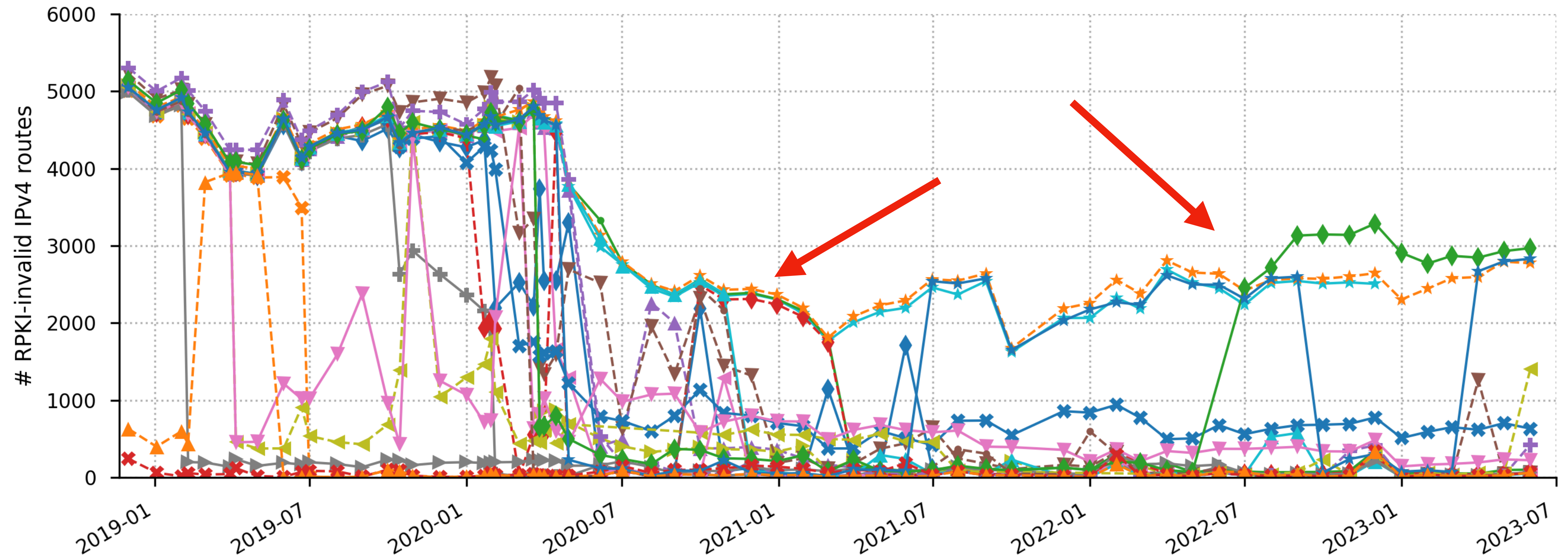
RPKI-invalid prefix count over time 2019-2021



RPKI-invalid prefix count over time 2019-2021



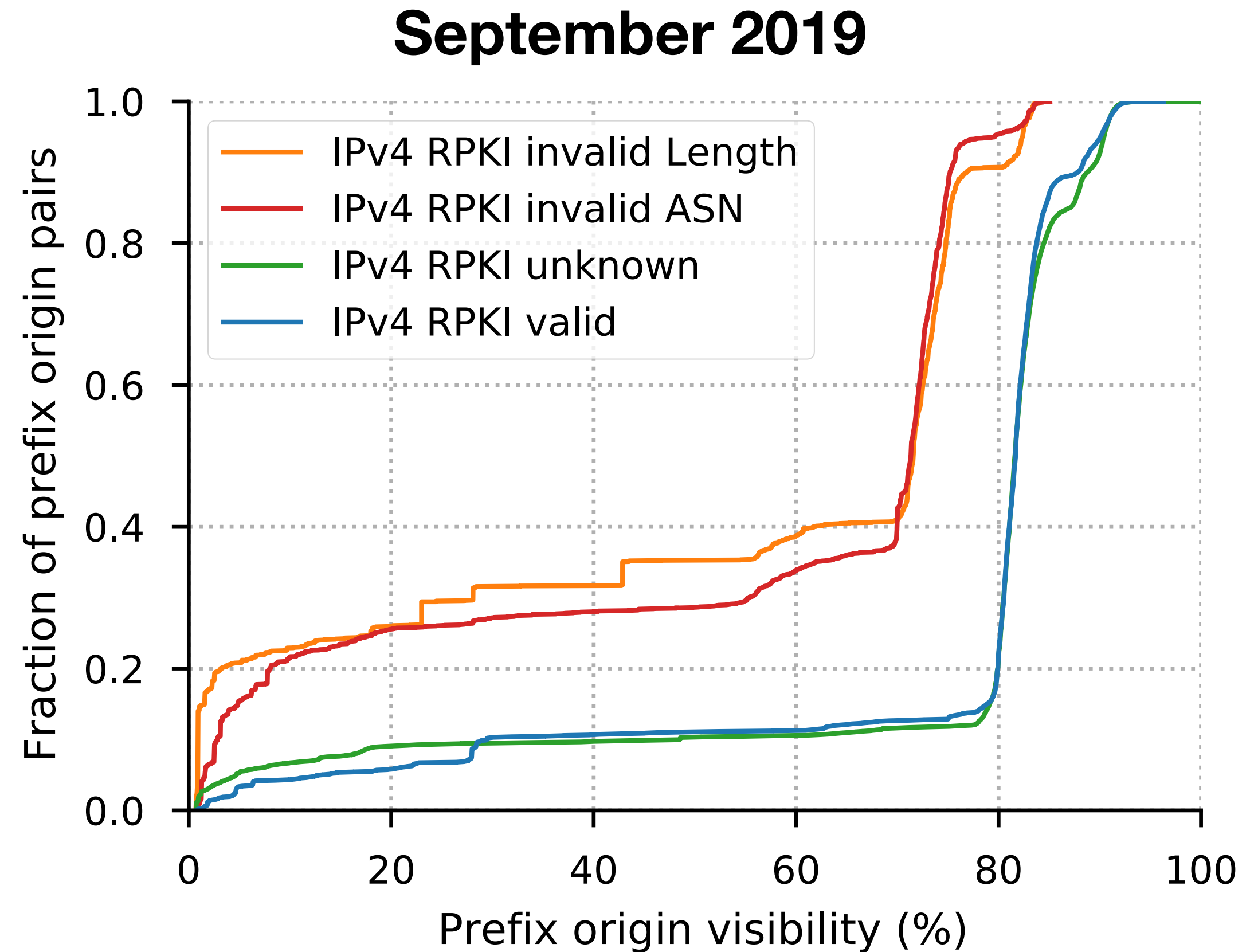
RPKI-invalid prefix count over time 2019-2023



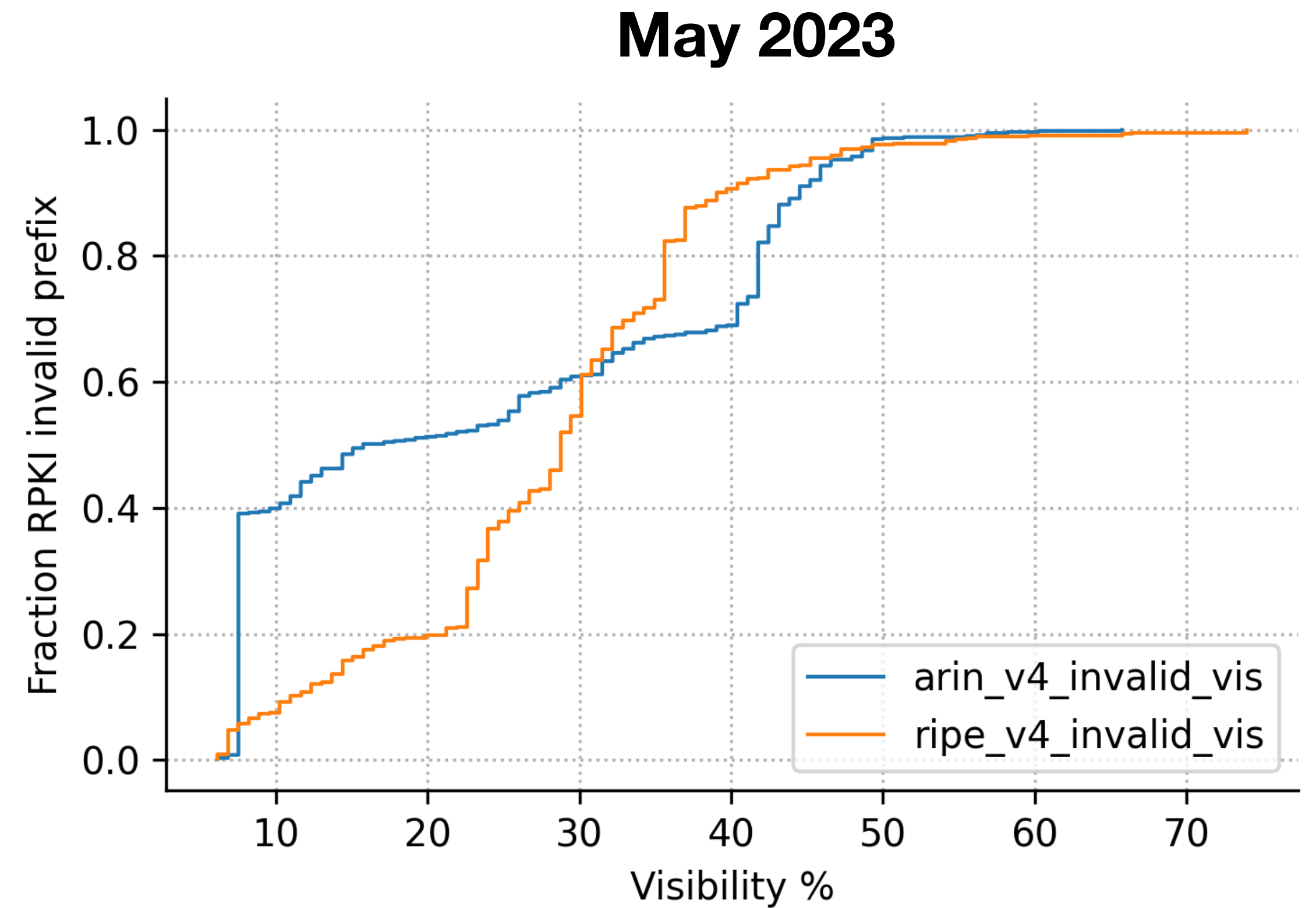
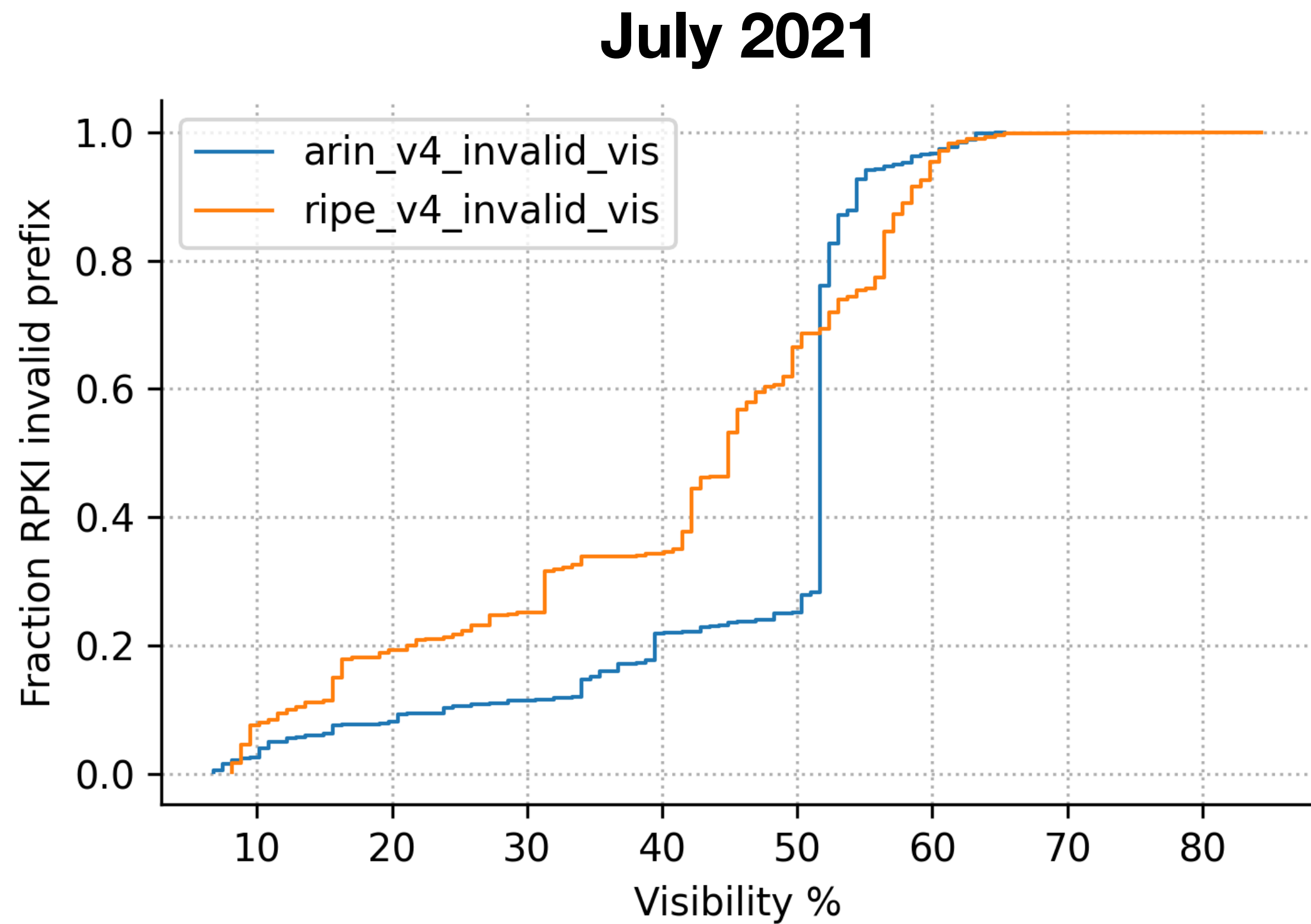
ROV Impact - RPKI Invalid visibility

ROV impact in prefix visibility

- ROAs impact prefix visibility.
- Most prefixes are either high visibility or low visibility
- Natural experiment option: each RIR defines its own RPKI-related policies.



ROV impact in RPKI invalid prefix visibility ARIN & RIPE



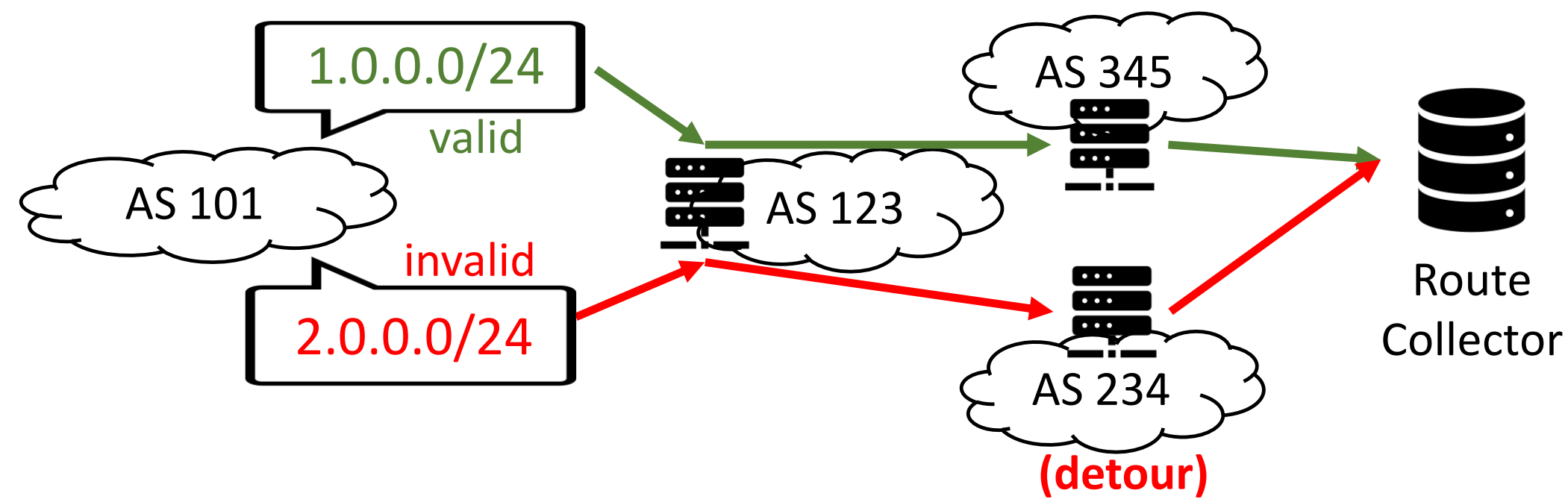
- Arin still has more high-visibility RPKI-invalid prefixes

ARIN RPA

Validator	Auto download ARIN repo	Date of ARIN Update
FORT Validator	No, requires agreement	N/A
Routinator	Yes	11/10/22
RPKI Prover	Yes	11/22/22
Octo RPKI	Yes	4/5/23
RPSTIR2	Yes	3/4/21

ROV Impact - RPKI Invalid detour

Detour of RPKI invalid BGP announcements



- 160 detour ASNs
- Limitations: ROV depends on AS relationships (Hegemony score may help)

Transit ASN	Company	# AS	# Invalid Pfx
AS 6762	Telecom Italia	301	1,125
AS 6461	Zayo	59	147
AS 7473	Singapore Telecom	54	135
AS 6453	TATA America	38	78
AS 1273	Vodafone	13	18

BGP Hijacks

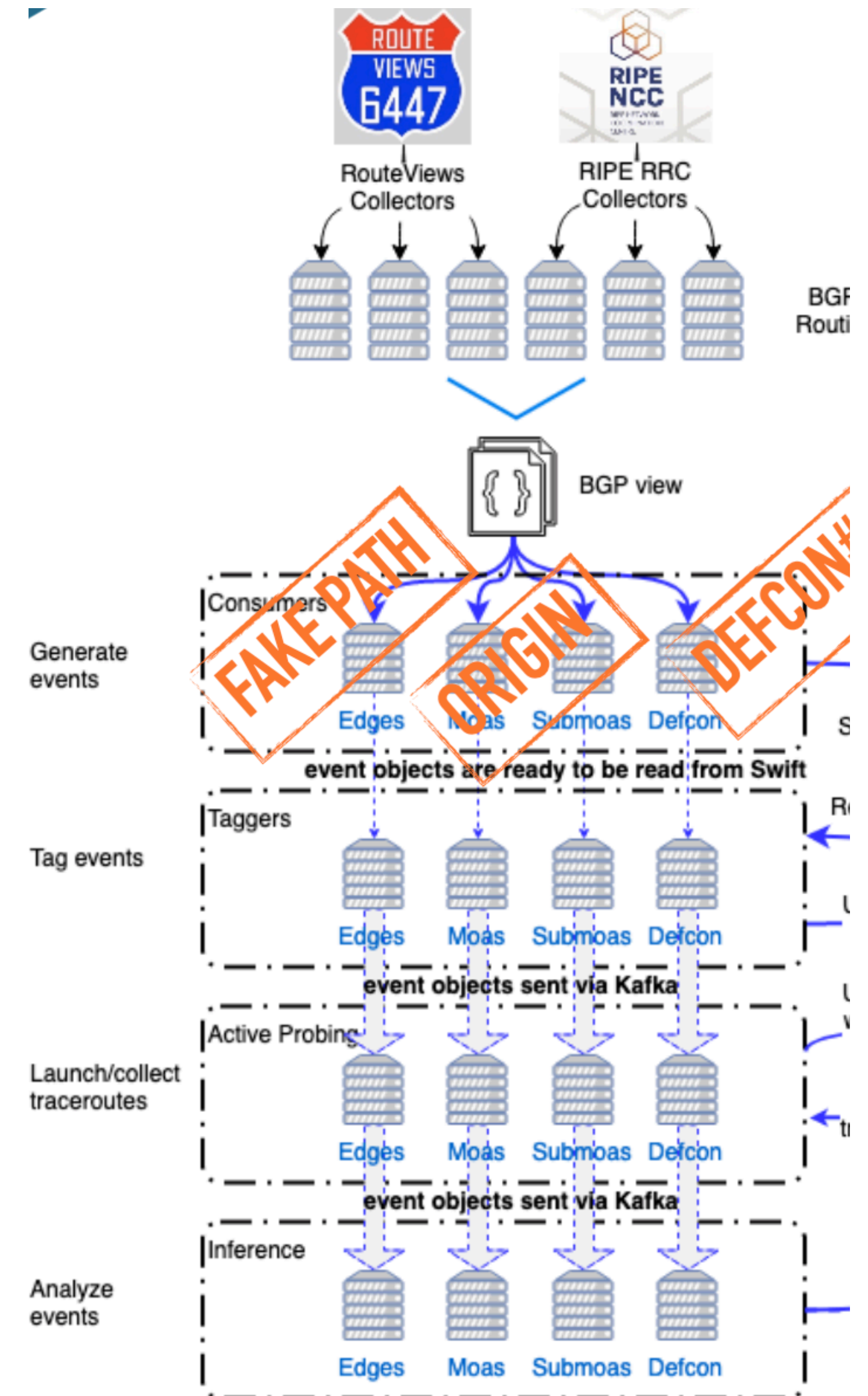
Global Routing Internet Platform (GRIP)

- All types of hijacks:
 - Origin
 - Fake path
 - Not preferred path (Defcon #16)
- In use by MANRS Observatory

Events	Code Repos	Acknowledgements	Methodology	Contacts				
Global Routing Intelligence Platform Select an event type: All MOAS Sub-MOAS New Edge Defcon Select an event suspicion level: All Suspicious Grey Benign Select time period (UTC now: Jun 11, 2023 4:42 PM): Jun 10, 2023 4:40 PM - Jun 11, 2023 4:40 PM Search for events by prefix/ASN/tags: Search by prefix/ASN/tags Search								
Events List								
Potential Victims	Potential Attackers	Largest (Sub)Prefix	# Prefix Events	Start Time	Duration	Suspicion	Category	Type
AS46887 Lighttower Fib...], LLC	AS400855	160.72.161.0/24	1	2023-06-11 15:20	ongoing	High	Default Tr Worthy	moas
AS396569 AS20172 VeriSign Glob...rvices ...	AS211369 VeriSign Inc. AS25485 VeriSign Inc.	192.35.51.0/24	4	2023-06-11 14:40	ongoing	High	Default Tr Worthy	moas
AS200406 Javid Berbid ...ny PJS	AS42440 Rayaneh Danes...S. Co.	185.231.112.0/24	1	2023-06-11 10:15	5 min	High	Default Tr Worthy	moas
AS13649 Flexential Co... Corp.	AS400856	192.67.157.0/24	1	2023-06-11 07:25	ongoing	High	Default Tr Worthy	moas
AS262535 Flash Net Bra... - EPP	AS273681 FLASH NET TEL...O LTDA	201.159.118.0/24	1	2023-06-11 04:40	60 min	High	Default Tr Worthy	moas
AS262535 Flash Net Bra... - EPP	AS273681 FLASH NET TEL...O LTDA	201.159.117.0/24	2	2023-06-11 03:00	60 min	High	Default Tr Worthy	moas
AS207281 Matrix Privat...bility	AS203811 AL-MARAJ AL-A...IYA Co	185.63.85.0/24	1	2023-06-11 01:00	25 min	High	Default Tr Worthy	moas
AS268519 master net ltda-me	AS28598 MOB SERVICOS ...S S.A.	45.161.158.0/24	1	2023-06-10 23:10	30 min	High	Default Tr Worthy	moas
AS328838 AIM Firms Limited	AS327859 Capital Techn...logies	102.220.72.0/22	1	2023-06-10 21:40	ongoing	High	Default Tr Worthy	moas
AS46186 Gilead Sciences	AS198949 DC PROTECTION LTD	8.20.113.0/24	1	2023-06-10 20:45	5 min	High	Default Tr Worthy	moas

GRIP Infrastructure

- Gathers all potential events
- Tags based on routing behavior and additional data (RPKI, IRR, AS type, etc)
- Inference engine to weed out false positive cases
- Allows to gather feedback



Thanks