Stop, DROP, and ROA: Effectiveness of Routing Defenses through the lens of DROP

Leo Oliver **Gautam Akiwate** Matthew Luckie

Ben Du KC Claffy

NANOG 87 | Atlanta, Georgia
February 2023

Problem: Malicious use of address space

(Still vulnerable forty years later..)

Malicious actor can:

1) falsely assert ownership of someone else's addresses
2) use own address space for malicious activity
   a) obtain addresses fraudulently
   b) use address space of hosting companies who don't care

"There are no routing police!"

What do we do about it

(Cooperative architectures in adversarial landscape)

a) blocklists: timing/scalability/lack of ground truth

What do we do about it

(Cooperative architectures in adversarial landscape)

a) blocklists: timing/scalability/lack of ground truth

b) detect hijacks: complexity, lack of ground truth

What do we do about it

(Cooperative architectures in adversarial landscape)

a) blocklists: timing/scalability/lack of ground truth

b) detect hijacks: complexity, lack of ground truth

c) validate announcement ***origins*** (BGP vs IRR/RPKI)

Our focus here!
(Ground truthiness)

What do we do about it

(Cooperative architectures in adversarial landscape)

a) blocklists: timing/scalability/lack of ground truth

b) detect hijacks: complexity, lack of ground truth

c) validate announcement ***origins*** (BGP vs IRR/RPKI) ⬅ Our focus here! (Ground truthiness)

d) future: BGPSEC (crypixie-dust whole path): complexity/cost/incentive

What do we do about it

(Cooperative architectures in adversarial landscape)

a) blocklists: timing/scalability/lack of ground truth

Use this data
to identify hijacks

b) detect hijacks: complexity, lack of ground truth

c) validate announcement ***origins*** (BGP vs IRR/RPKI)

Our focus here!
(Ground truthiness)

d) future: BGPSEC (crypixie-dust whole path): complexity/cost/incentive

Goal

What can blacklists
(as a source of information about hijacked prefixes)
tell us about
*the **effectiveness of IRR/RPKI***
as “routing defenses”?

Caveat: "IRR/RPKI not a routing defense"

(It's just the basis of one..)

*In addition, this system is only able to provide limited protection against a determined attacker -- **the attacker need only prepend the "valid" source AS to a forged BGP route announcement** in order to defeat the protection provided by this system.*

*This mechanism **does not protect** against "**AS-in-the-middle attacks**" or provide any **path validation**. It only attempts to verify the origin. In general, this system should be thought of more as a protection against misconfiguration than as true "security" in the strong sense.*

"BGP Prefix Origin Validation" (Security Considerations - Page 7,8), RFC6811, 2013.

DROP: Don’t Route or Peer

(Spamhaus well-regarded public advisory blacklist)

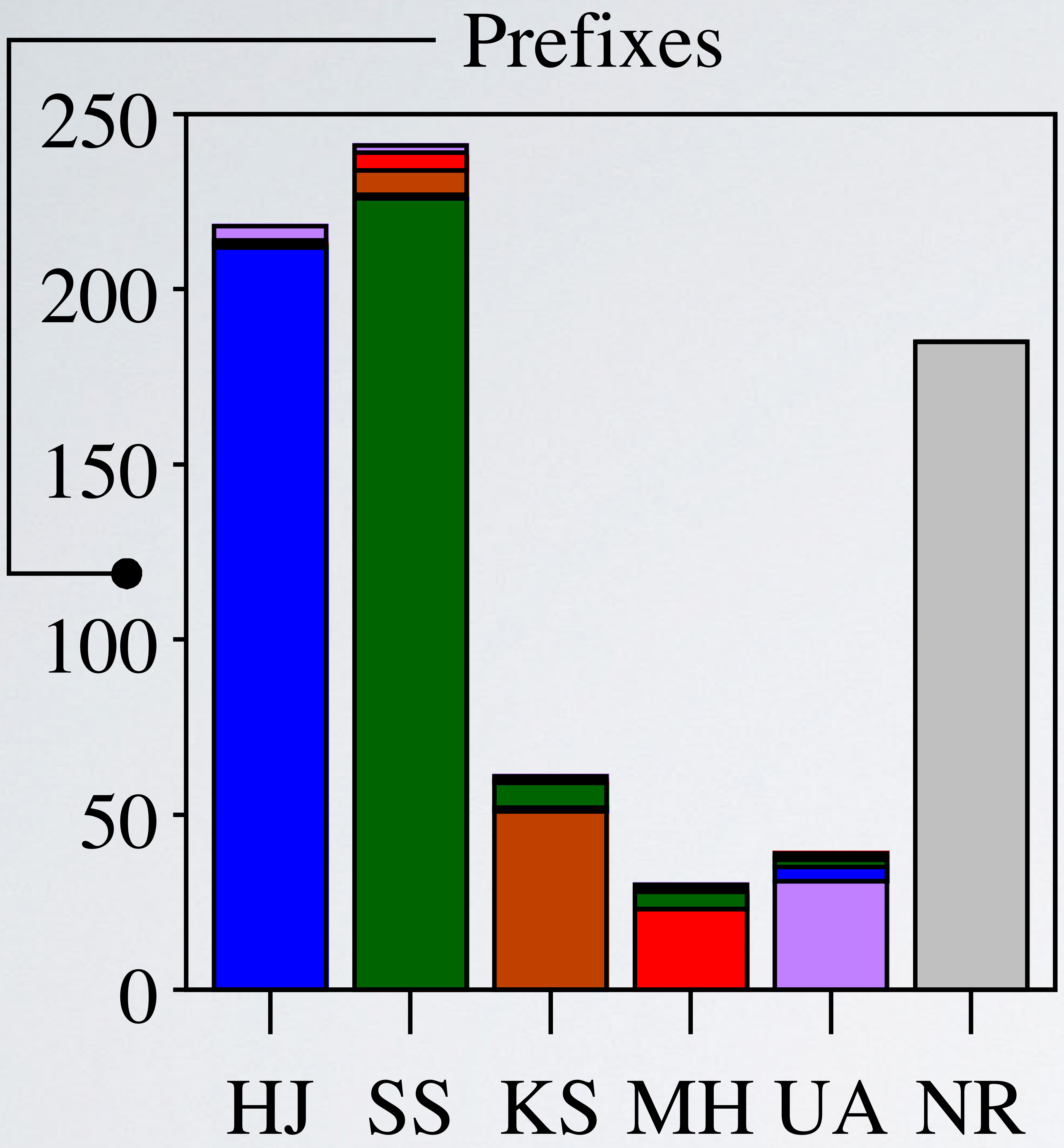
Strengths

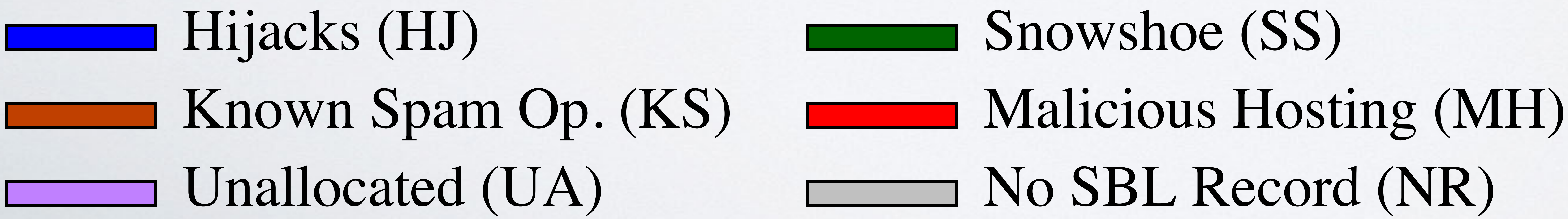
1. Well-documented: entry says why it’s on DROP
2. Seriously abused prefixes — w/hijack subcategory
3. Human vetting, try to be responsive to researchers
4. Public, thus easily reproducible

Limitations

1. Small
2. ?? Representative ??
3. Correlation, not causation

DROP list by category

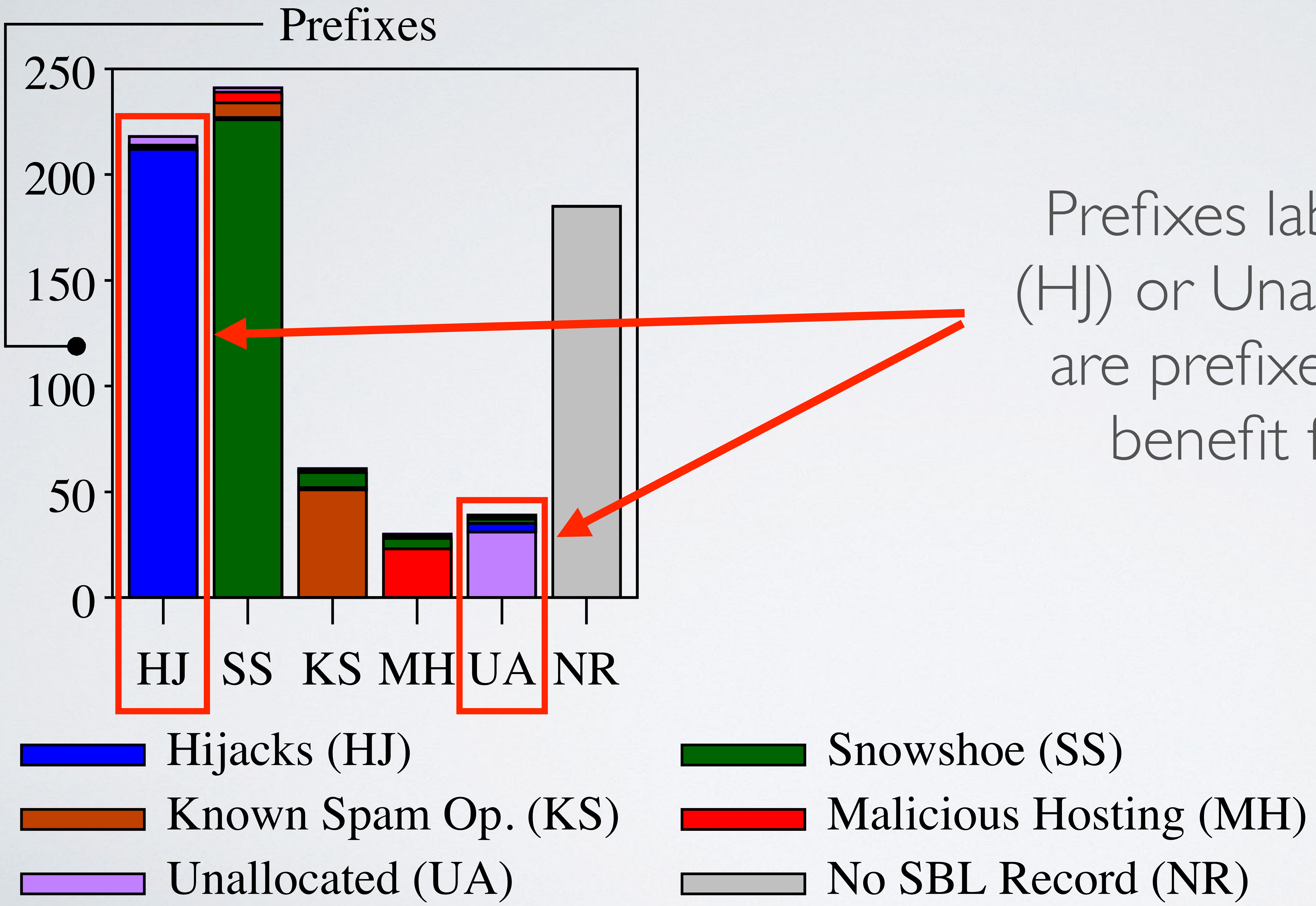




- **712 prefixes appeared in DROP from June 2019 to March 2022**

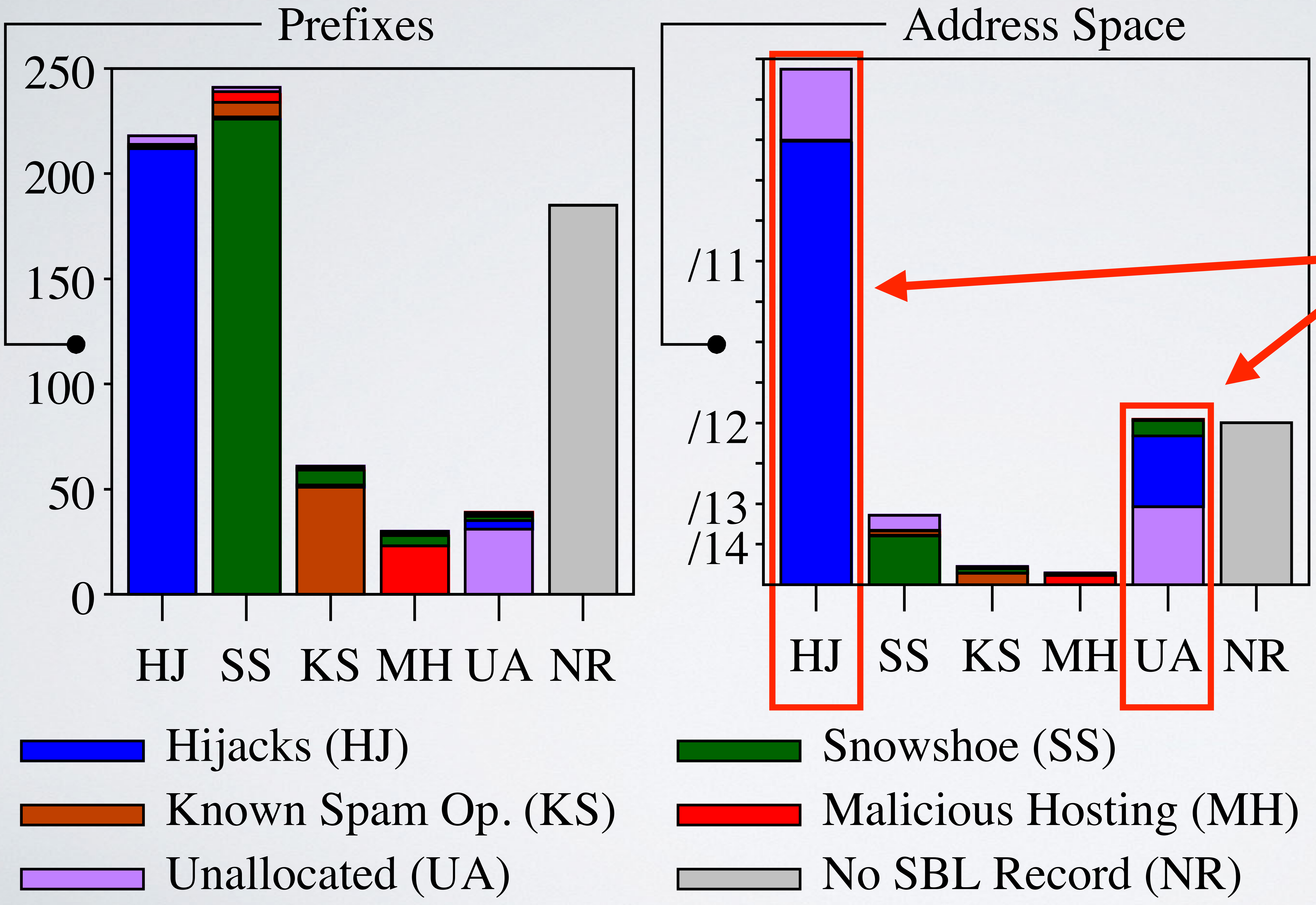
- We categorized all prefixes using six labels based on Spamhaus' description

What is DROP?



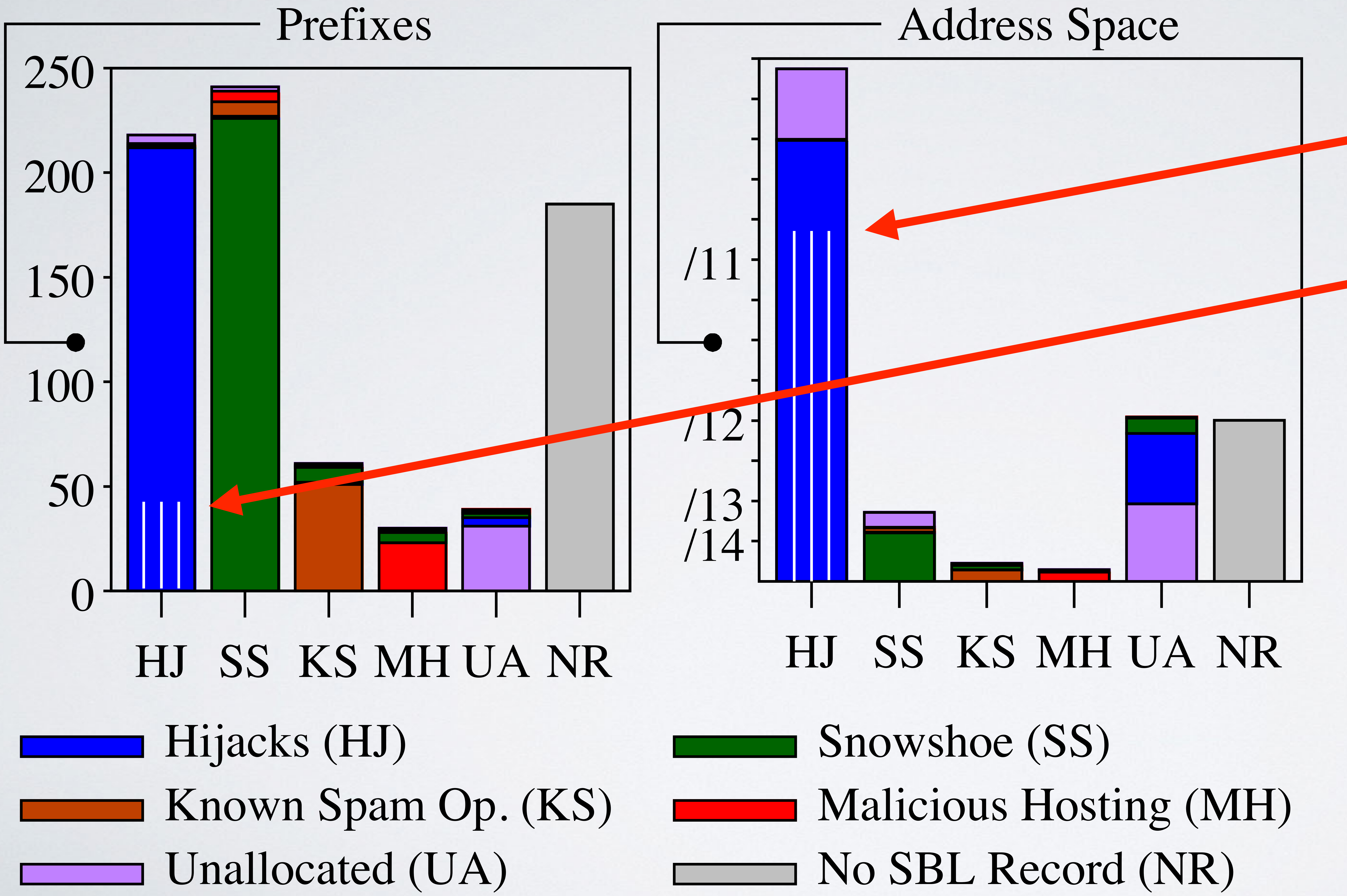
Prefixes labelled Hijack (HJ) or Unallocated (UA) are prefixes that could benefit from RPKI

What is DROP?



Prefixes labelled Hijack (HJ) or Unallocated (UA) cover most of the address space covered by DROP

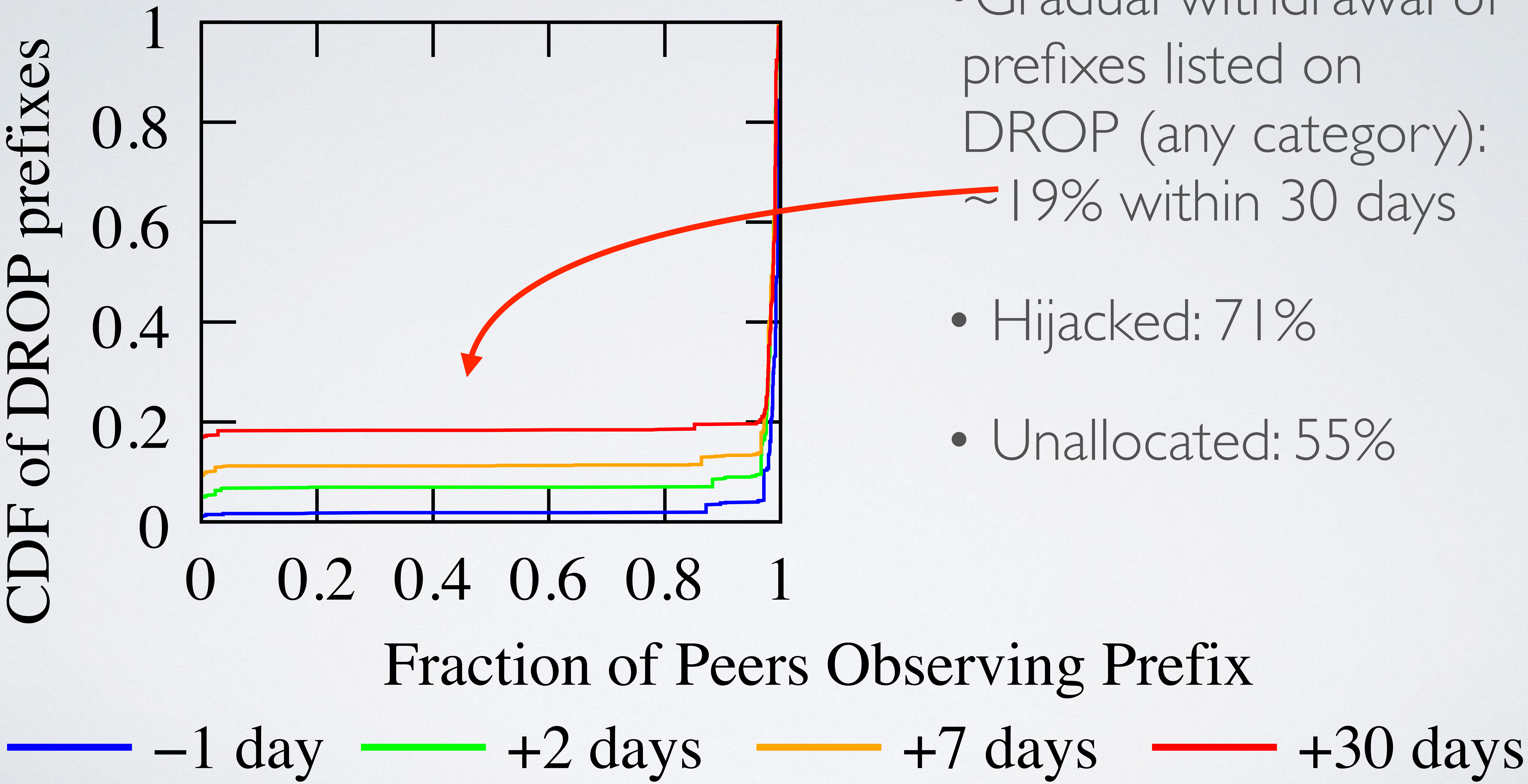
What is DROP?



48.8% of DROP address space from **45** prefixes were related to AFRINIC incidents described in the paper.

We excluded these from analysis.

Do DROP prefixes get dropped?

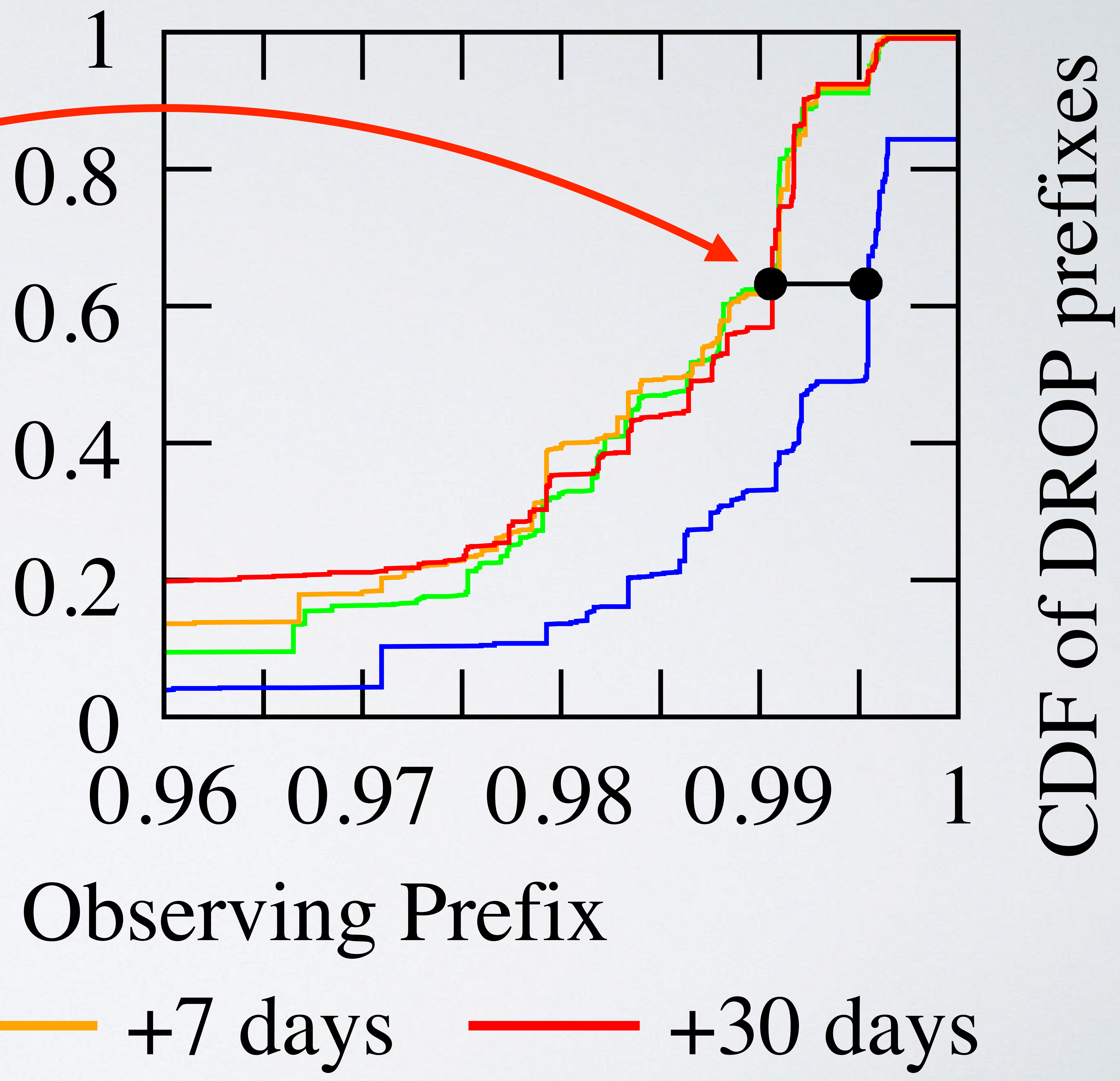


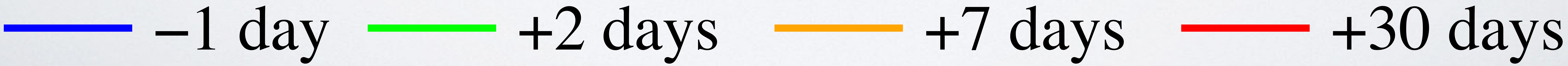
- Gradual withdrawal of prefixes listed on DROP (any category): ~19% within 30 days
- Hijacked: 71%
- Unallocated: 55%

What effect might DROP have on routing?

Three full-feed RouteViews peers BGP-filtered DROP prefixes

(validated by one of these peers)





What effect might DROP have on RPKI?

	Never on DROP	Removed from DROP	Not removed from DROP
AFRINIC			
APNIC			
ARIN			
LACNIC			
RIPE NCC			
Overall	**RPKI signing rate of prefixes**		

Population: Prefixes without a ROA on June 4th, 2019

What effect might DROP have on RPKI?

	Never on DROP	Removed from DROP	Not removed from DROP
AFRINIC			
APNIC			
ARIN			
LACNIC			
RIPE NCC			
Overall	**RPKI signing rate of prefixes**		

Not added to DROP between June 2019 and March 2022 (control)

Population: Prefixes without a ROA on June 4th, 2019

What effect might DROP have on RPKI?

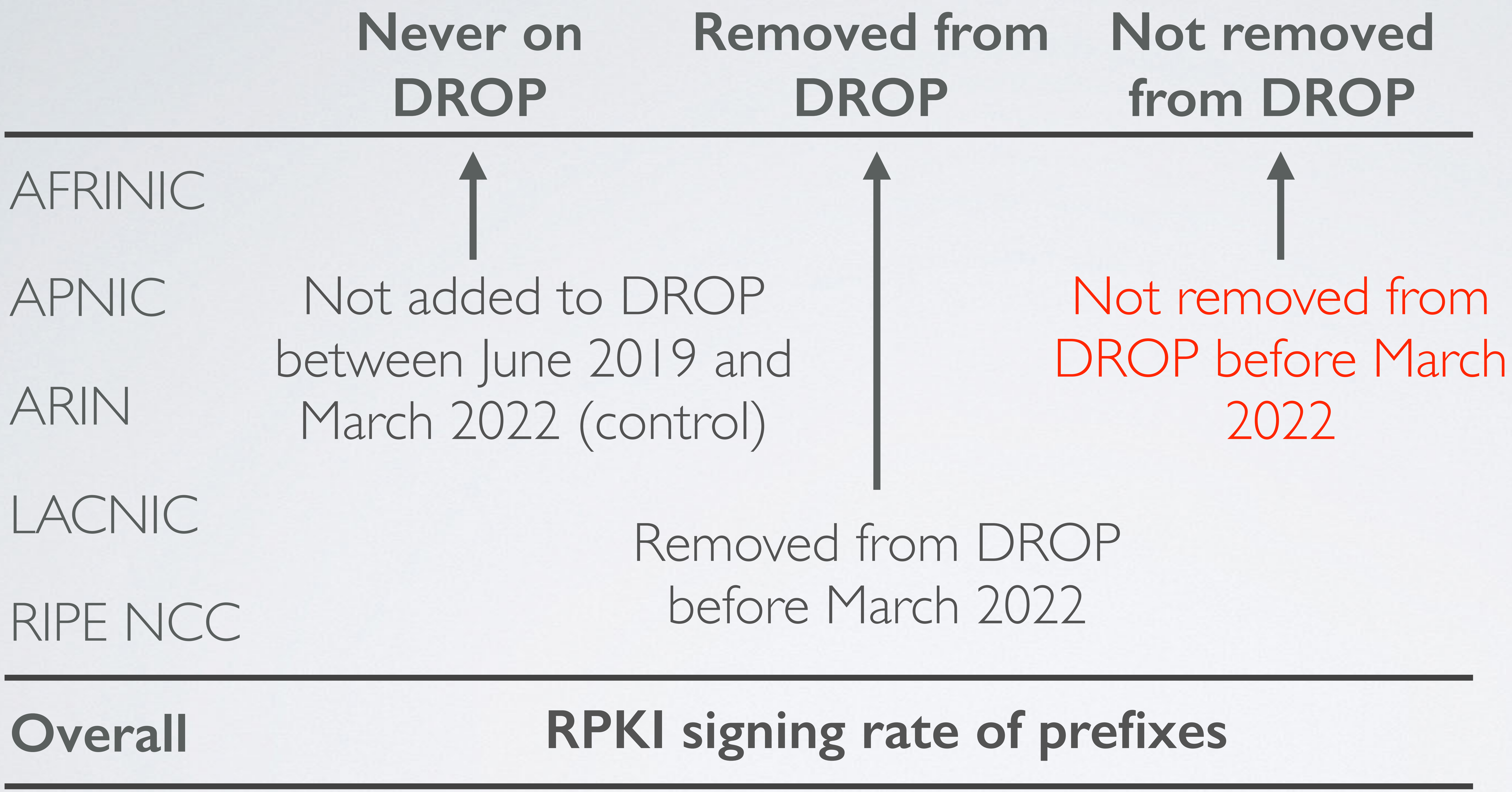
	Never on DROP	**Removed from DROP**	**Not removed from DROP**
AFRINIC			
APNIC			
ARIN			
LACNIC			
RIPE NCC			
Overall		**RPKI signing rate of prefixes**	

Not added to DROP between June 2019 and March 2022 (control)

Removed from DROP before March 2022

Population: Prefixes without a ROA on June 4th, 2019

What effect might DROP have on RPKI?



	Never on DROP	Removed from DROP	Not removed from DROP
AFRINIC			
APNIC			
ARIN			
LACNIC			
RIPE NCC			
Overall			

RPKI signing rate of prefixes

Not added to DROP between June 2019 and March 2022 (control)

Removed from DROP before March 2022

Not removed from DROP before March 2022

Population: Prefixes without a ROA on June 4th, 2019

What effect might DROP have on RPKI?

	Never on DROP	**Removed from DROP**	**Not removed from DROP**
AFRINIC	11.8% of 3901		
APNIC	26.3% of 42.2K		
ARIN	8.5% of 65.2K		
LACNIC	25.5% of 15.1K		
RIPE NCC	33.0% of 68.2K		
Overall	**22.3% of 195.6K**		

Different regions have different background RPKI-signing activity

Population: Prefixes without a ROA on June 4th, 2019

What effect might DROP have on RPKI?

	Never on DROP	Removed from DROP	Not removed from DROP
AFRINIC	11.8% of 3901	14.3% of 7	
APNIC	26.3% of 42.2K	44.4% of 18	
ARIN	8.5% of 65.2K	25.0% of 40	
LACNIC	25.5% of 15.1K	35.1% of 37	
RIPE NCC	33.0% of 68.2K	54.2% of 83	
Overall	**22.3% of 195.6K**	**42.5% of 186**	

Prefixes removed from DROP were RPKI-signed at a higher rate than this background activity

Only 6.3% were signed with the same ASN as the DROP-labelled attacker

Population: Prefixes without a ROA on June 4th, 2019

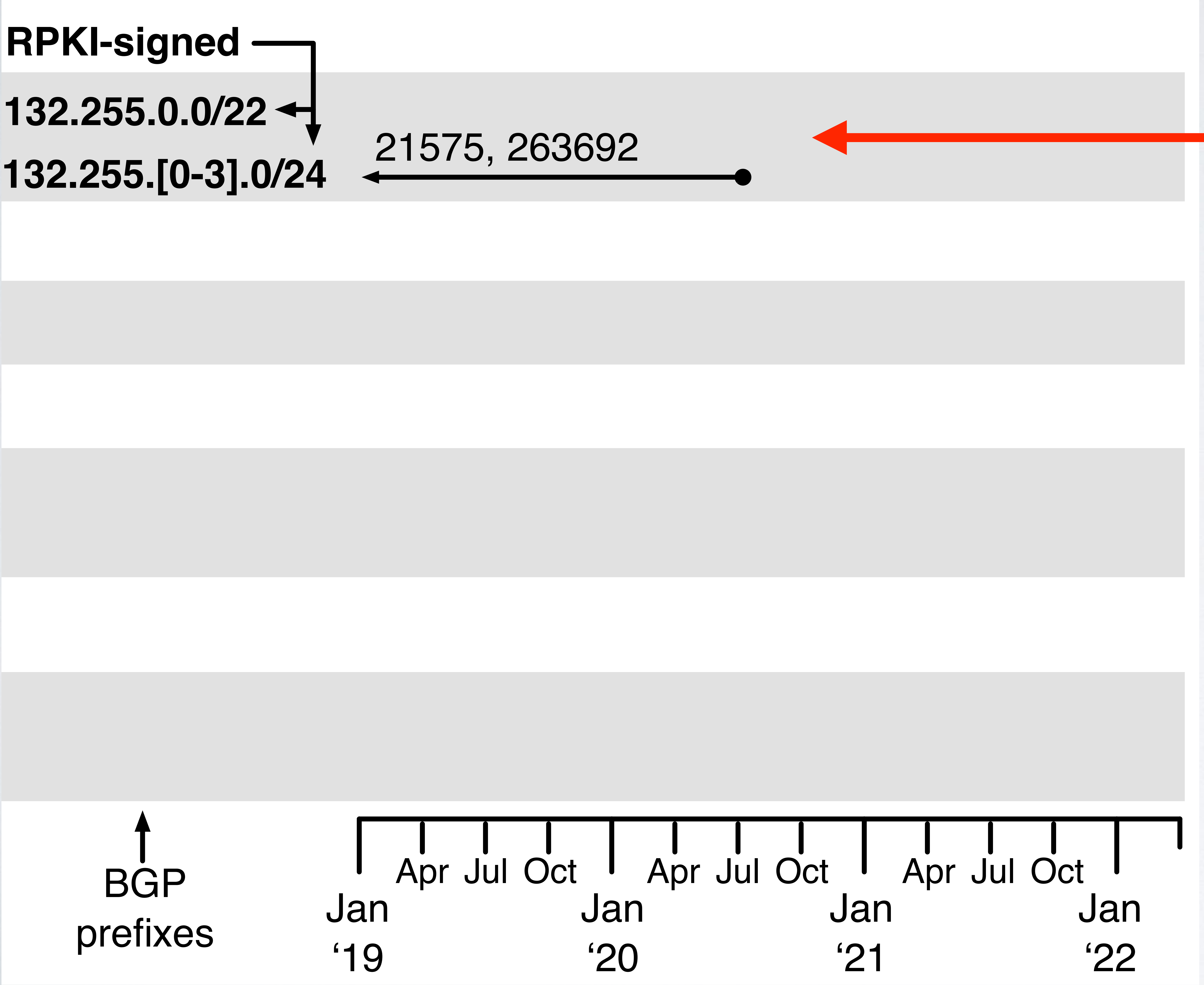
What effect might DROP have on RPKI?

	Never on DROP	Removed from DROP	Not removed from DROP
AFRINIC	11.8% of 3901	14.3% of 7	0.0% of 11
APNIC	26.3% of 42.2K	44.4% of 18	21.6% of 37
ARIN	8.5% of 65.2K	25.0% of 40	0.6% of 169
LACNIC	25.5% of 15.1K	35.1% of 37	0% of 9
RIPE NCC	33.0% of 68.2K	54.2% of 83	19.8% of 172
Overall	**22.3% of 195.6K**	**42.5% of 186**	**13.8% of 420**

Prefixes remaining on DROP were RPKI-signed at a lower rate.

Population: Prefixes without a ROA on June 4th, 2019

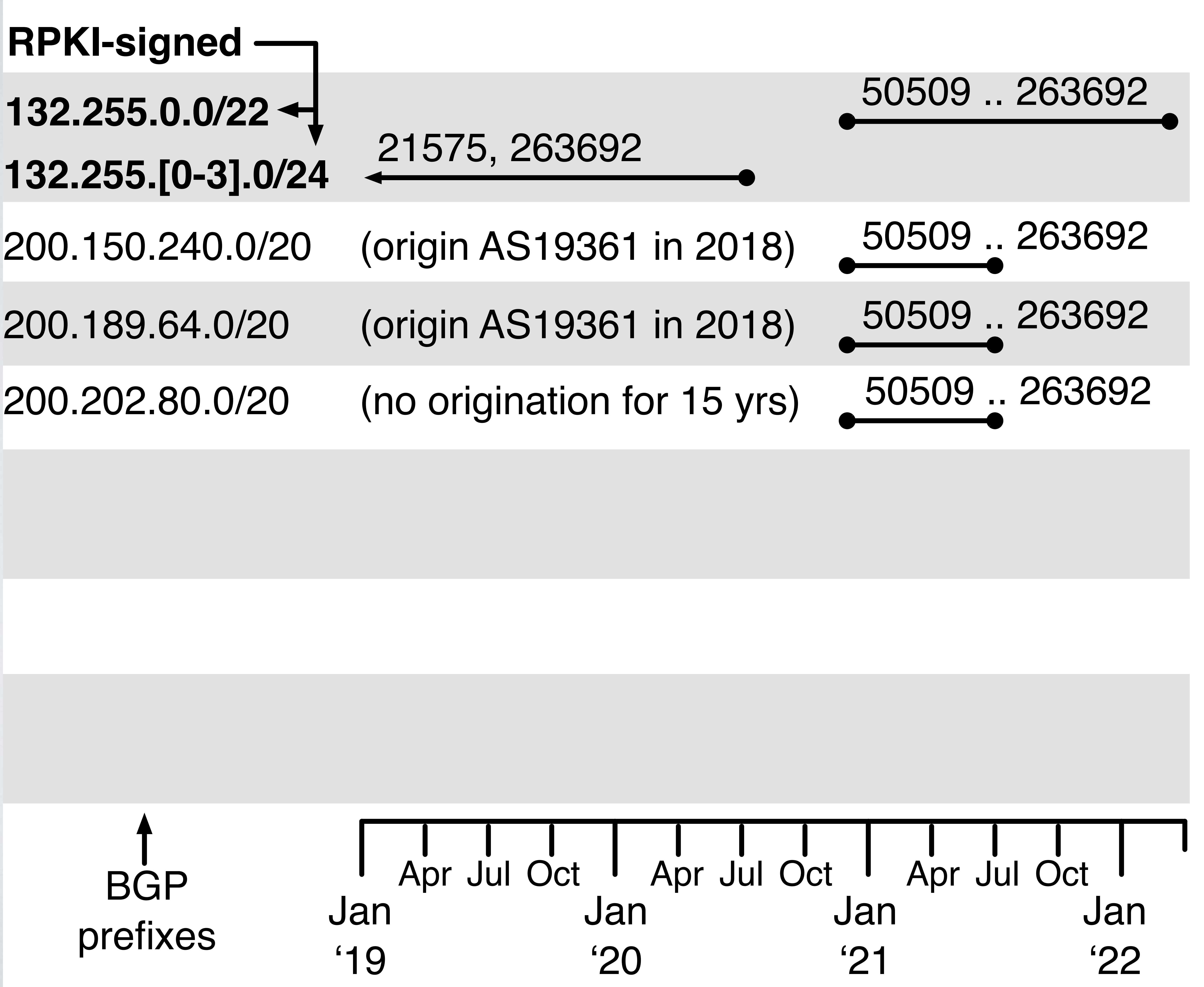
Hijack of RPKI-signed prefix



132.255.0.0/22 RPKI-signed by AS263692, abandoned July 2020

(RFC6811 warning vivified)

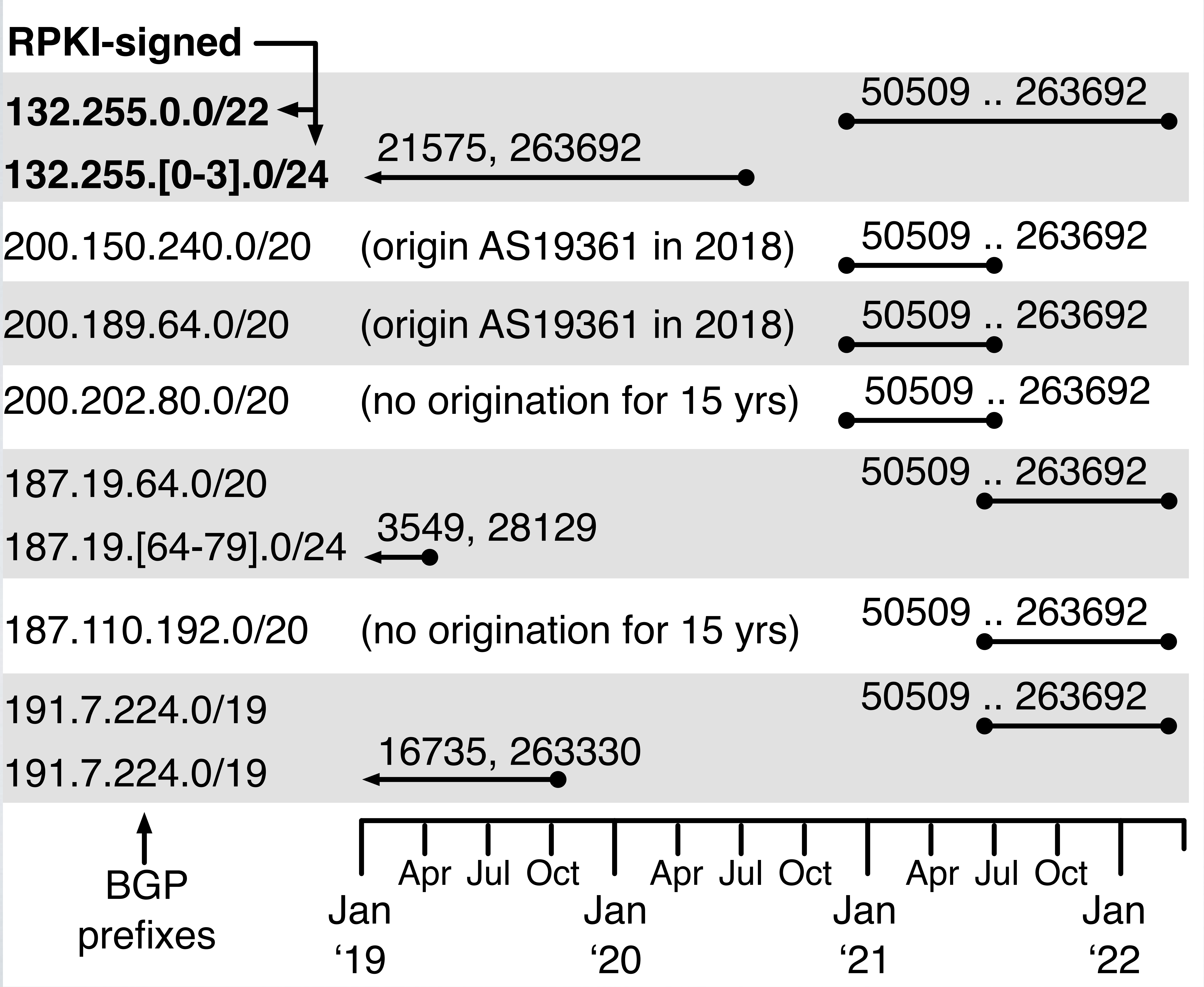
Hijack of RPKI-signed prefix



Attacker announces prefix and 3 others, spoofing origin as AS263692 in Dec 2020.

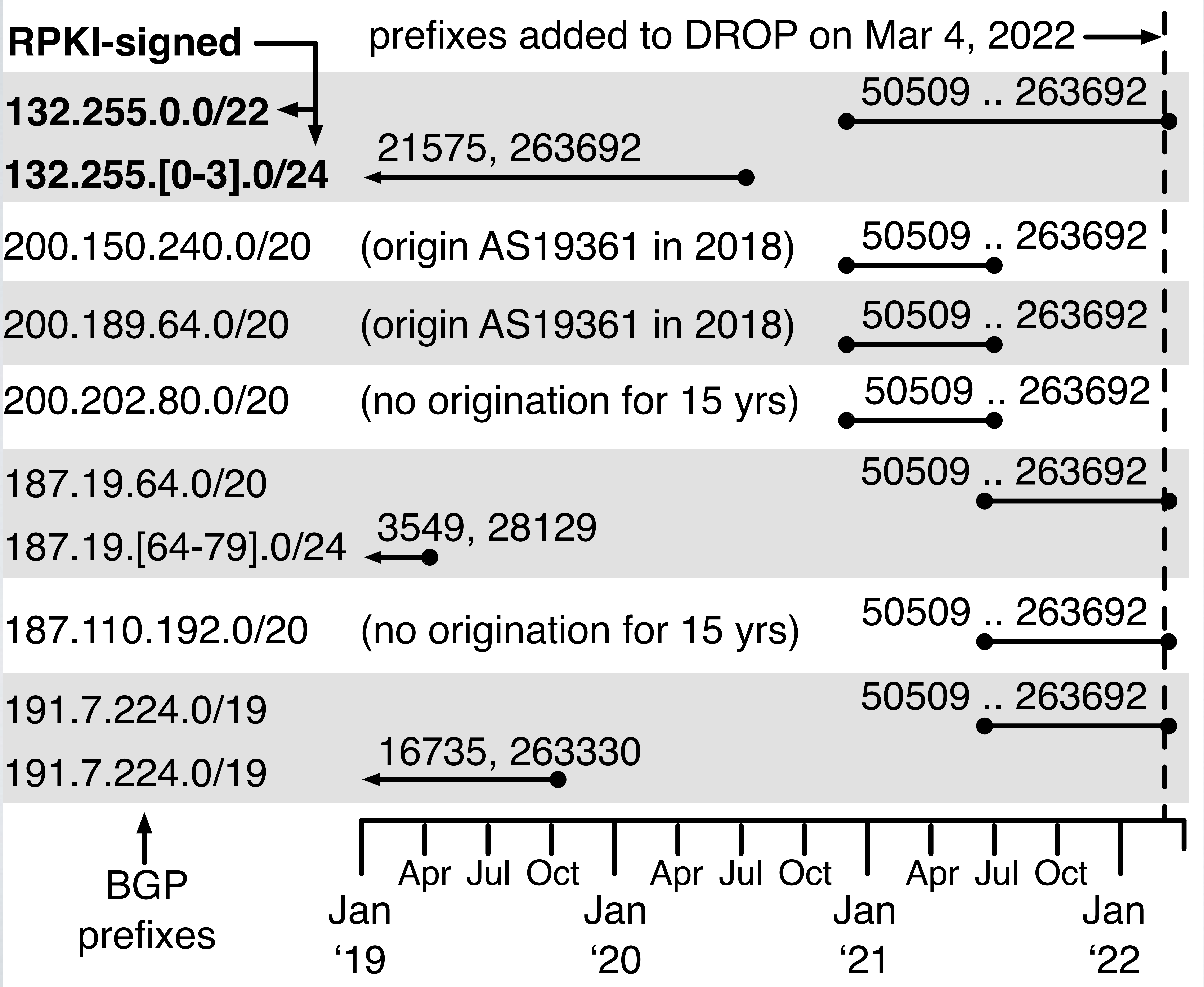
Attacker halts announcements for 3 prefixes in Jul 2021.

Hijack of RPKI-signed prefix



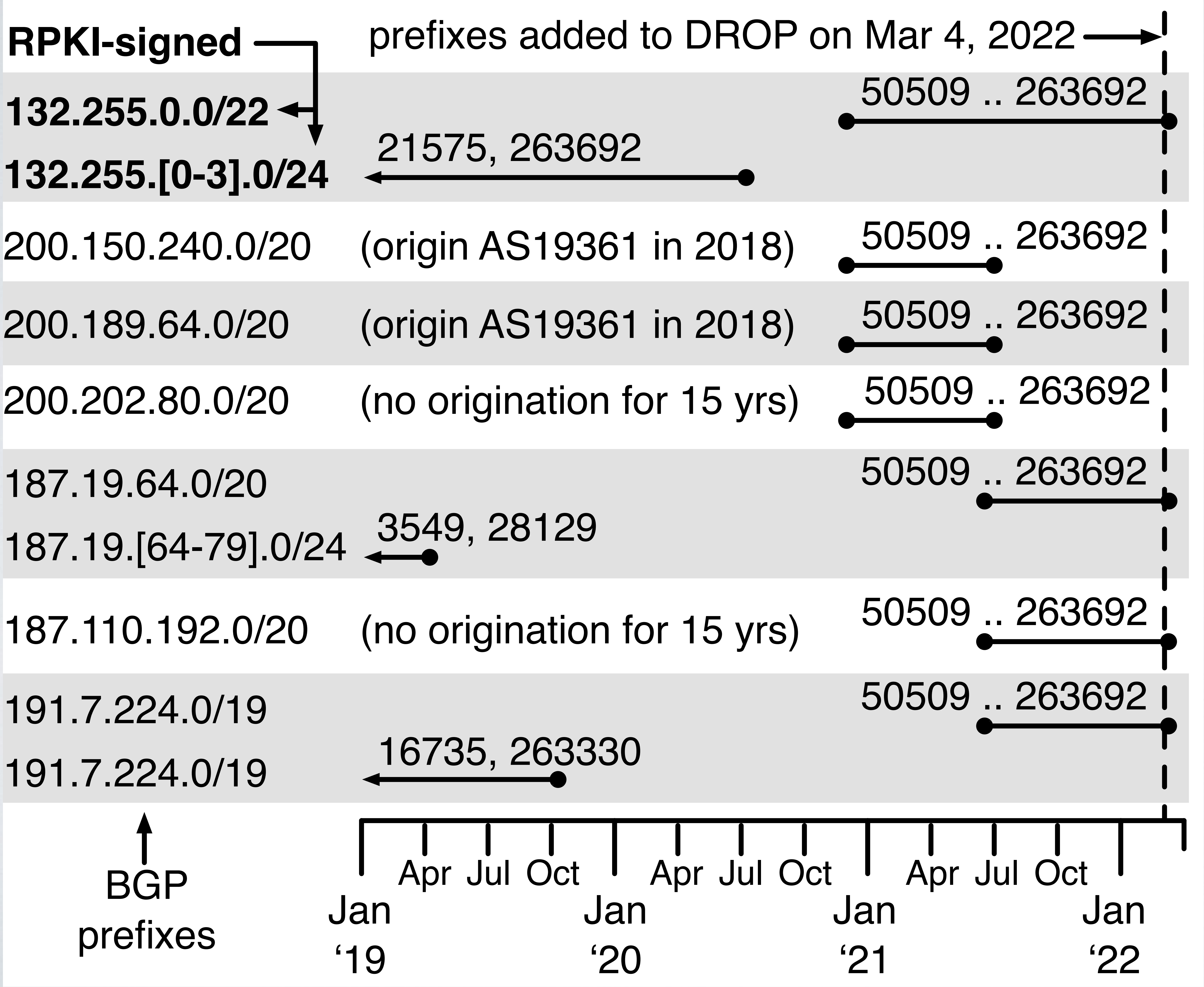
Attacker announces 3 other abandoned prefixes in Jun 2021.

Hijack of RPKI-signed prefix



Attacker withdraws prefixes after Spamhaus adds them to DROP

Hijack of RPKI-signed prefix



Key issue: RPKI-signed prefix is no more protected than any other abandoned prefix, as attacker can spoof origin ASN.

[AS RFC6811 warned]

AS0: prevent rogue announcement of prefix

Reduce attack surface of unrouted space

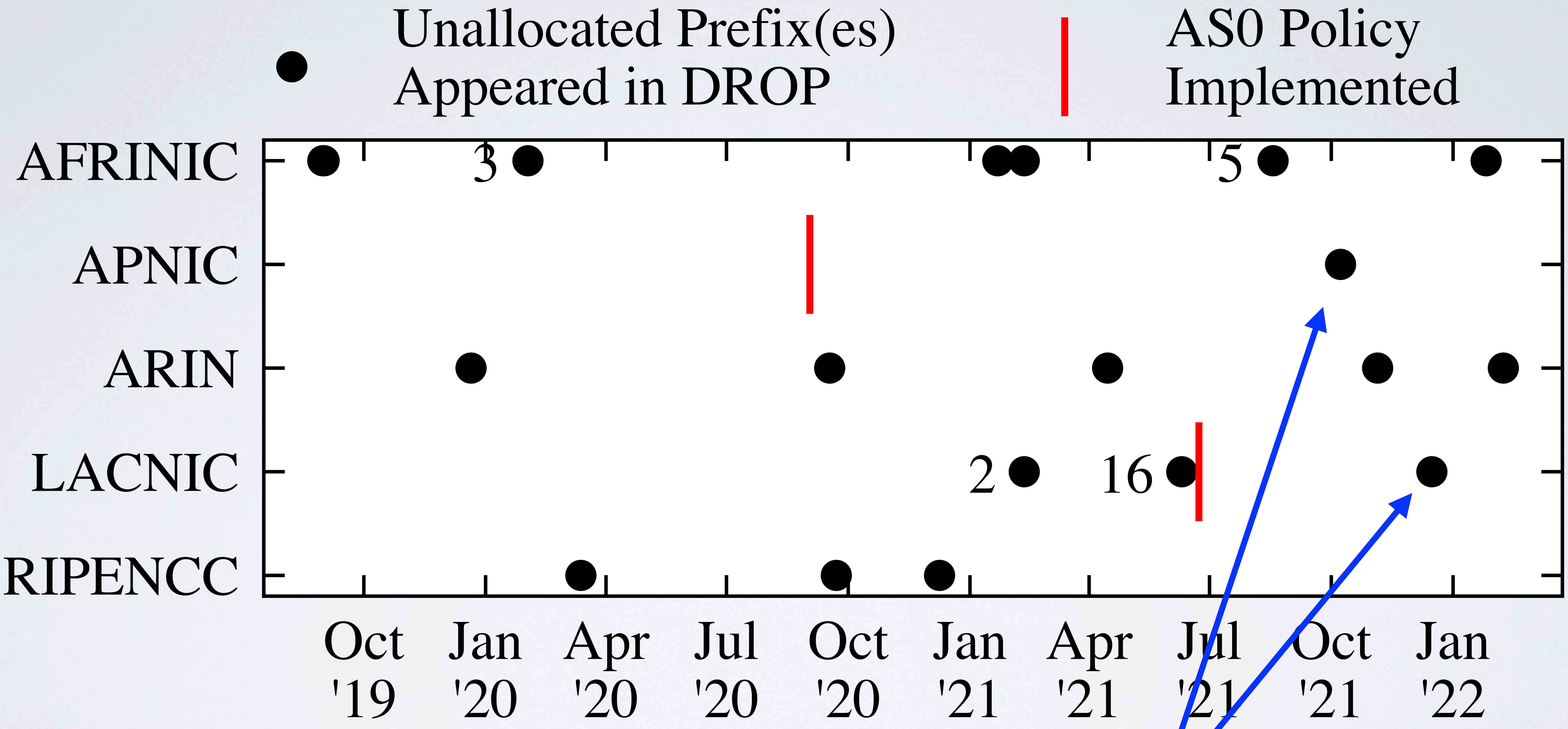
- An AS0 ROA asserts that a prefix (and more specifics) should not be routed
- Two types, both problematic
  - **RIR:** an RIR may issue AS0 ROAs for ***unallocated*** prefixes
  - **Operator:** an operator may issue AS0 ROAs for ***unrouted*** prefixes

AS0 policies are *politically* sensitive

Much debate landed differently in different regions

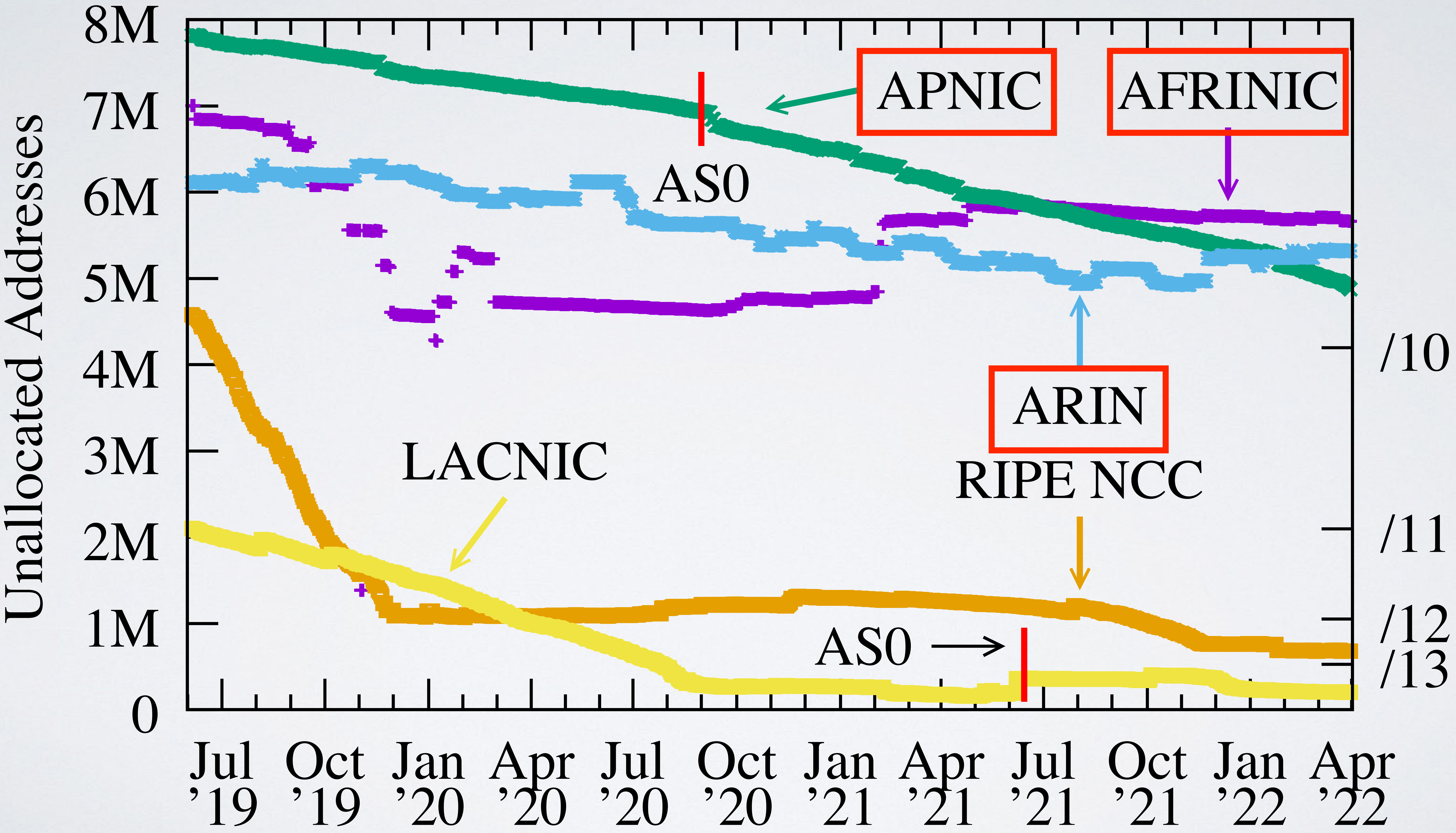
- AS0 policies are *politically sensitive*
  - **RIR**-executed: slippery slope of power to blacklist address space by non-profit, non-government, not heavily capitalized organizations
    - *Only APNIC and LACNIC support: different TAL, do not advise filtering*
  - **Operator**-executed: networks not using address space are "supposed to" return it to RIR for subsequent allocation based on need.

Current RIR AS0 policies have limited effect

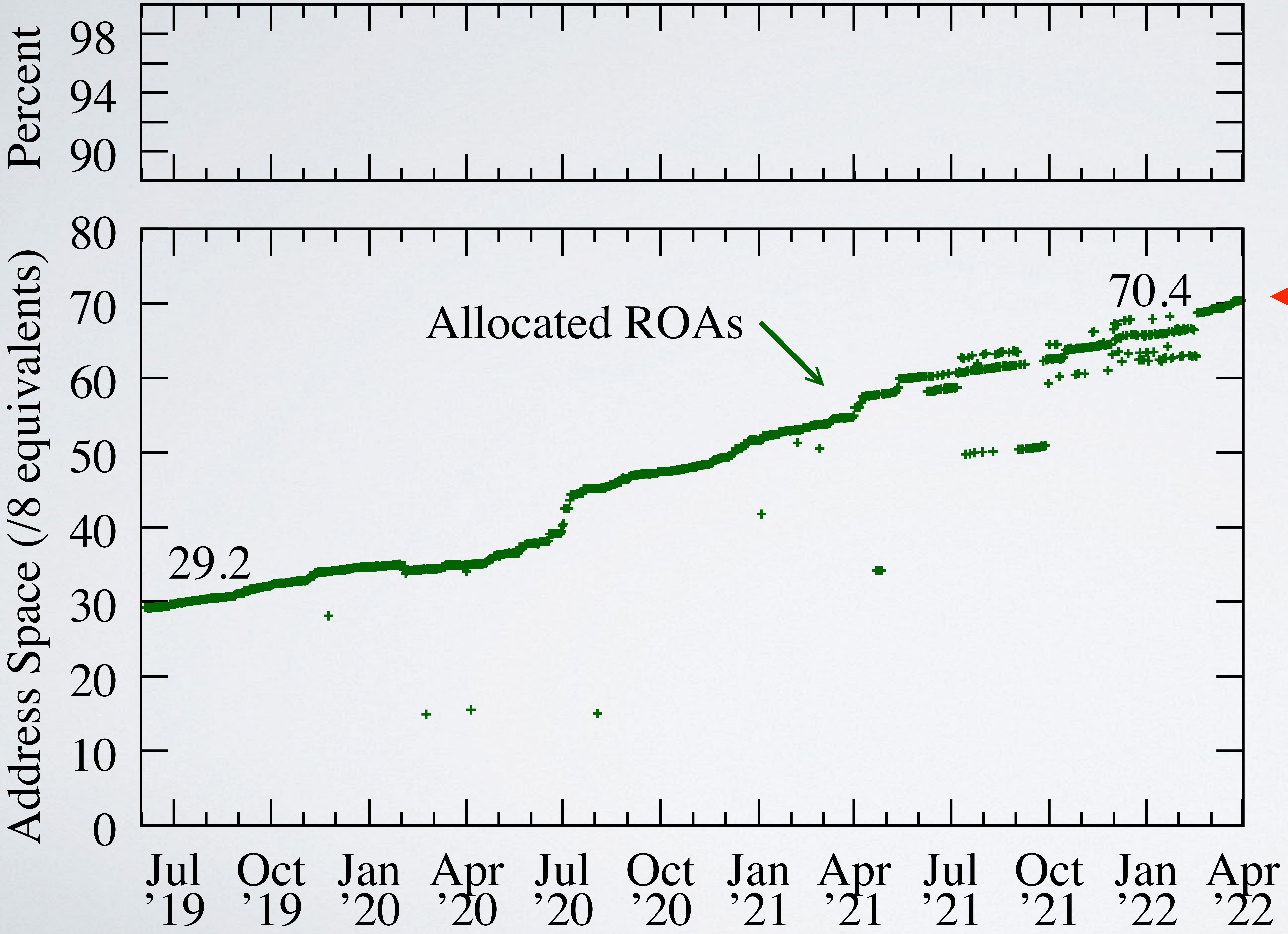


Unallocated prefixes continue to be added to DROP after RIR AS0 policy implemented

Still unallocated space in three RIRs..



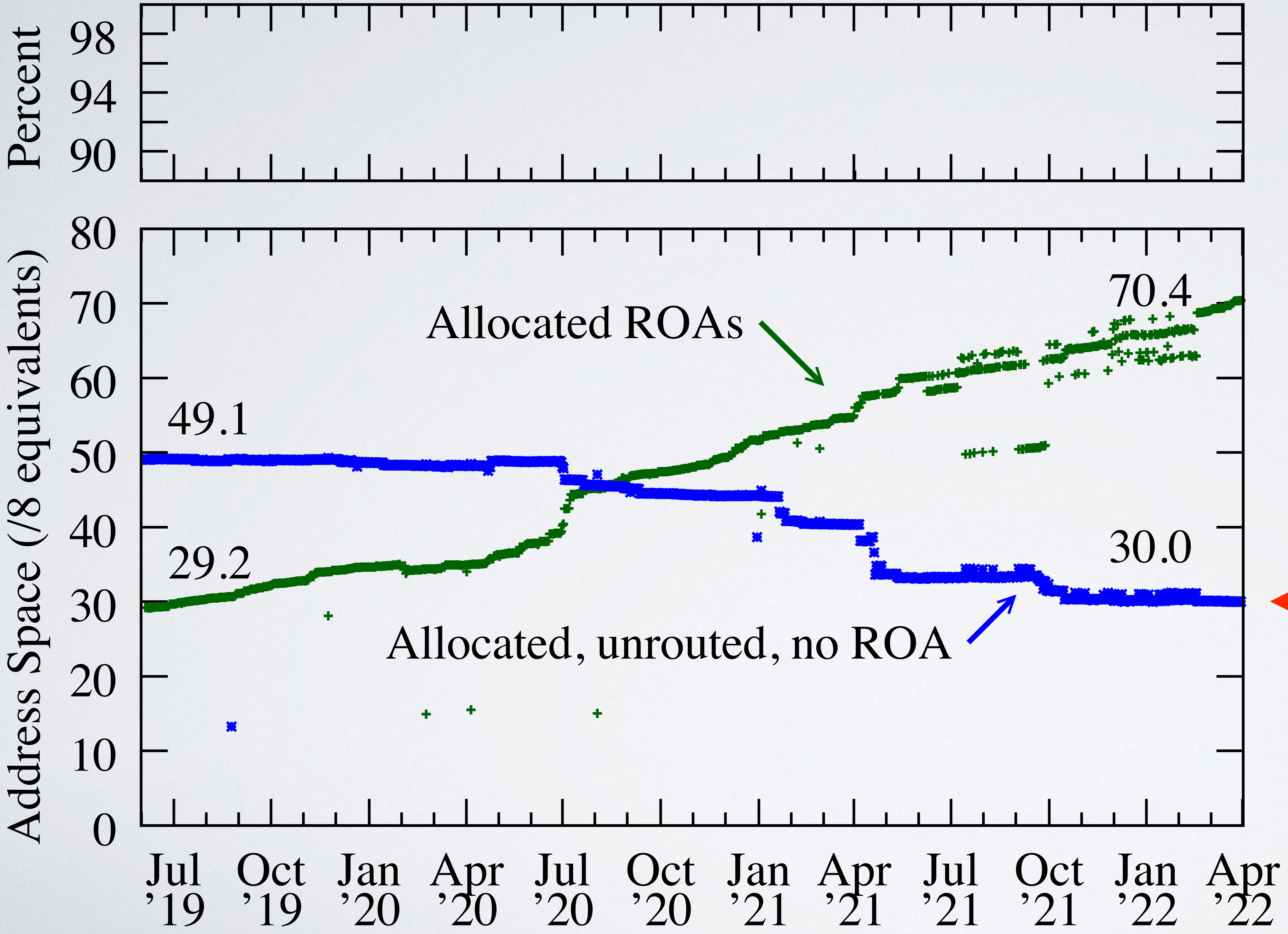
Dynamics of ROAs and their implication



Continued growth in address space covered by a ROA to **70.4 /8s**

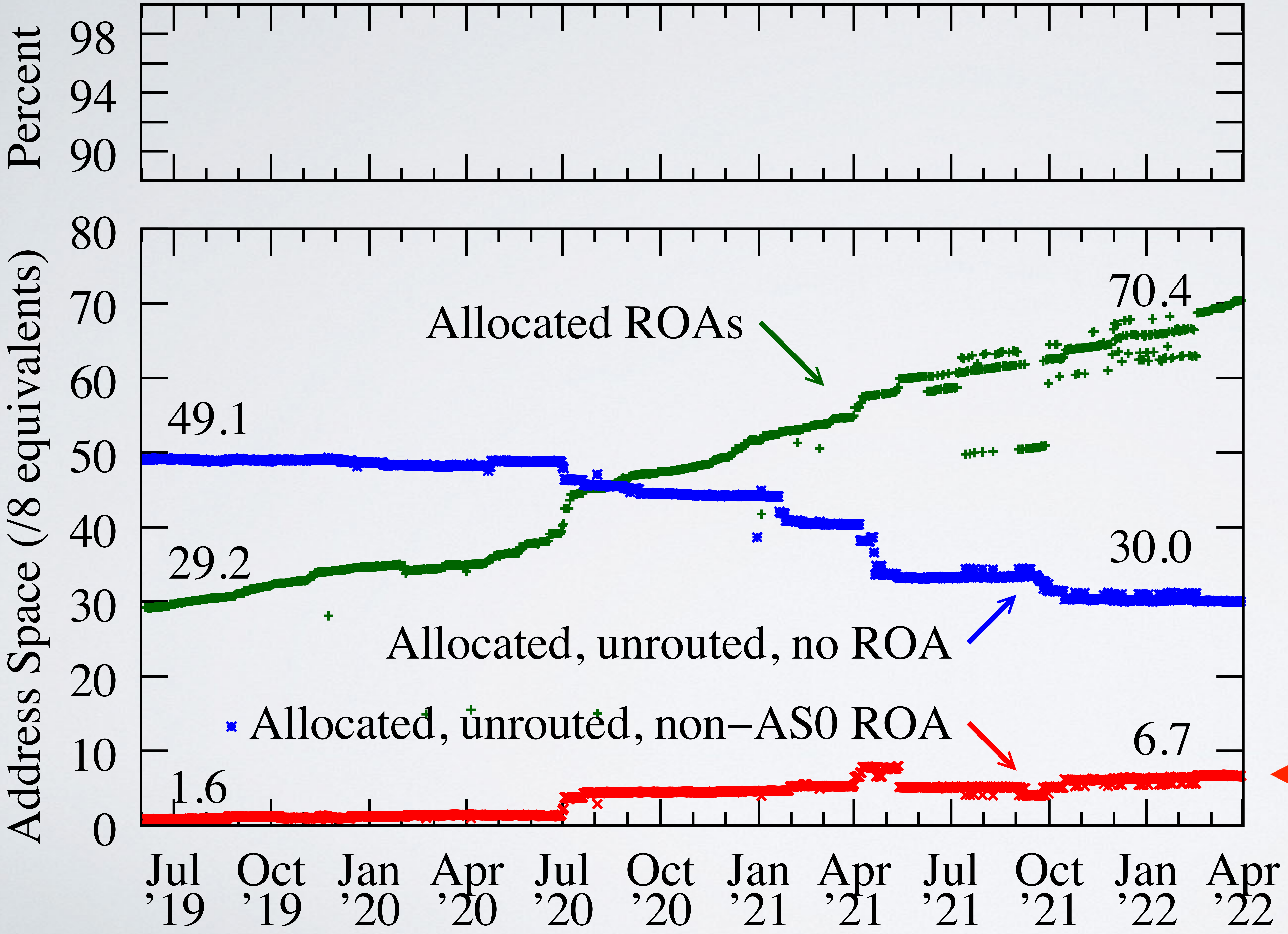
More than double in <3 years

Dynamics of ROAs and their implication



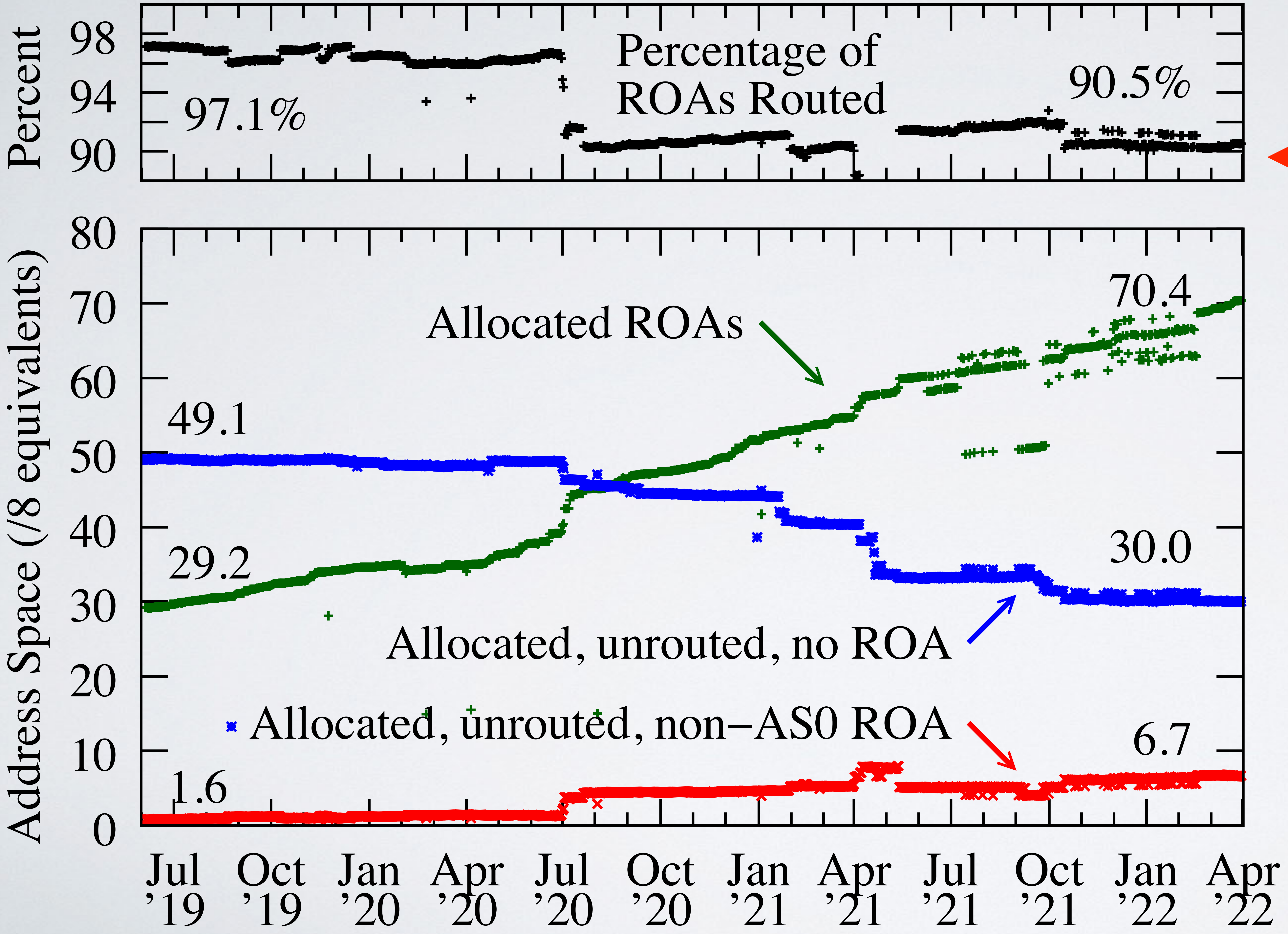
Gradual reduction in unrouted address space not covered by a ROA to **30.0 /8s**

Dynamics of ROAs and their implication



However, gradual growth in unrouted address space covered by a non-AS0 ROA to **6.7 /8s**

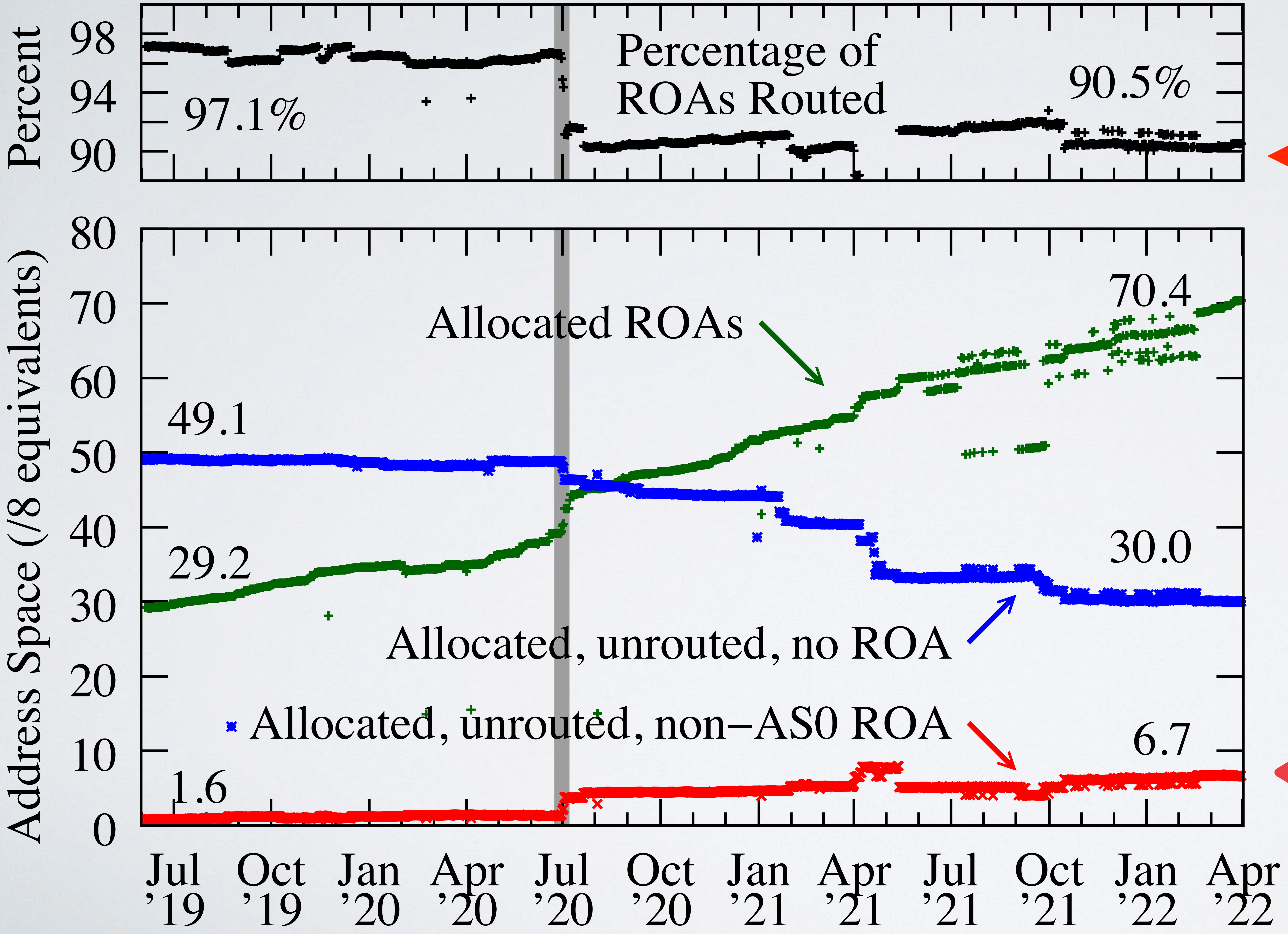
Dynamics of ROAs and their implication



The effect is a reduction in ROAs covered by a routed prefix.

Increase in hijack attack surface.

Dynamics of ROAs and their implication



(3 orgs: Amazon, Prudential, Alibaba are 70%)

Key findings

- Good news: DROP seems to improve incentives: prefixes removed from DROP were RPKI-signed at ~2X rate (42%) of prefixes not removed (22%)

- Bad news: Attackers subverting defenses against malicious use of address space

  a) Obtaining fraudulent IRR records for prefixes before using them
  b) Spoofing origin AS consistent w/ historic route announcements
  c) Announcing with ASN in Route Origin Authorization

- Attack surface: 6.7 /8 equivalents are RPKI-signed (with non-AS0) but unrouted: Another 30 /8 equivalents are unrouted, no ROA. All 600M IPs(v4) hijackable.

Parting Thoughts

- Hunt for routing security solutions continues (now feat. U.S. FCC)
- Need more transparency and accountability than we have today
- Prediction: "zones of trust" will emerge to provide/enable it