Routing Security Landscape

Doug Madory (Kentik)

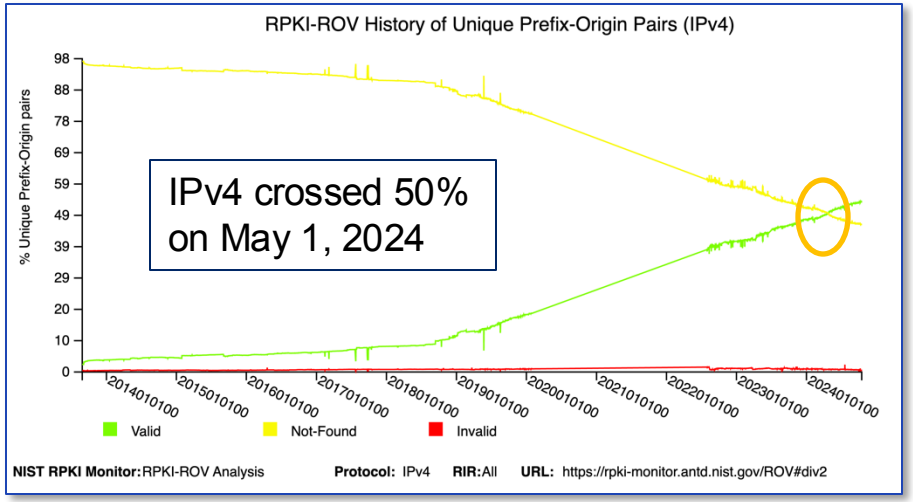
kentik®

The network observability company

Update on RPKI ROV Adoption

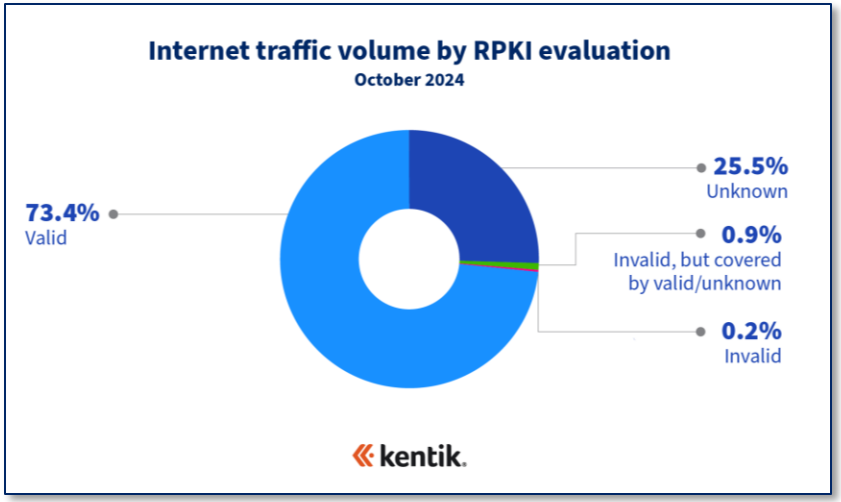
ROA growth continues!

BGP (IPv4:53.3%, IPv6:55.2%)



https://rpki-monitor.antd.nist.gov/

Traffic (73.4% bits/sec)



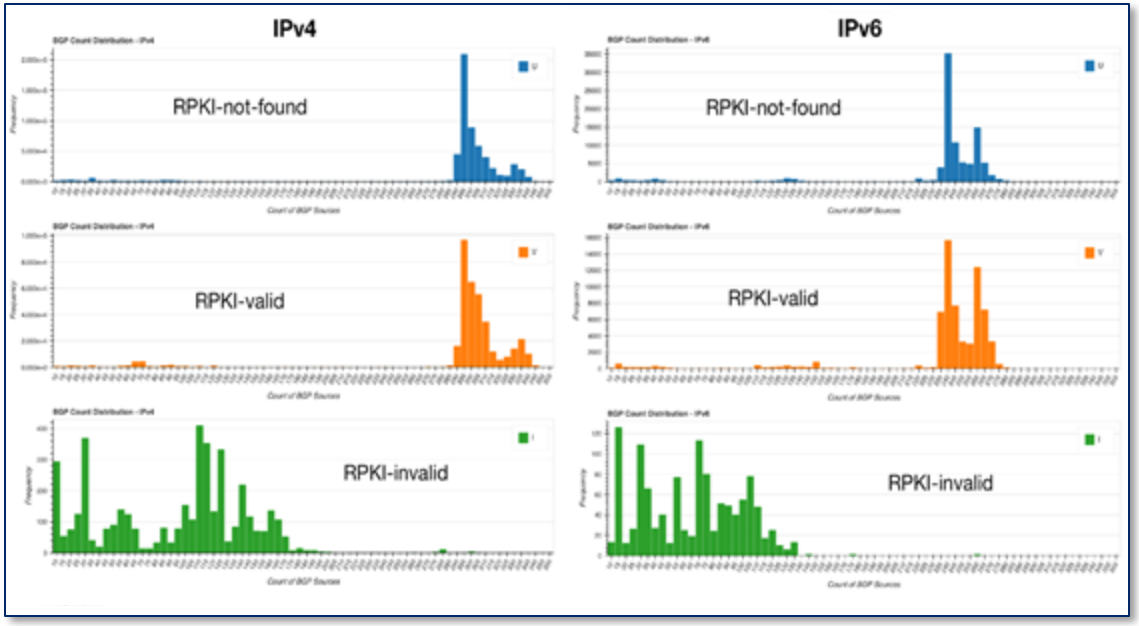
https://www.kentik.com/blog/rpki-rov-deployment-reaches-major-milestone/

Update on RPKI ROV Adoption

RPKI-invalid propagation is low

2022 analysis showed propagation of invalid routes is half or less than other types.

An RPKI-invalid routes cannot be globally routed.



Update on RPKI ROV Adoption

RPKI-invalid propagation is low ***and declining***

Invalid routes from beacons all experienced an overall decline in propagation while the control routes saw increased propagation.

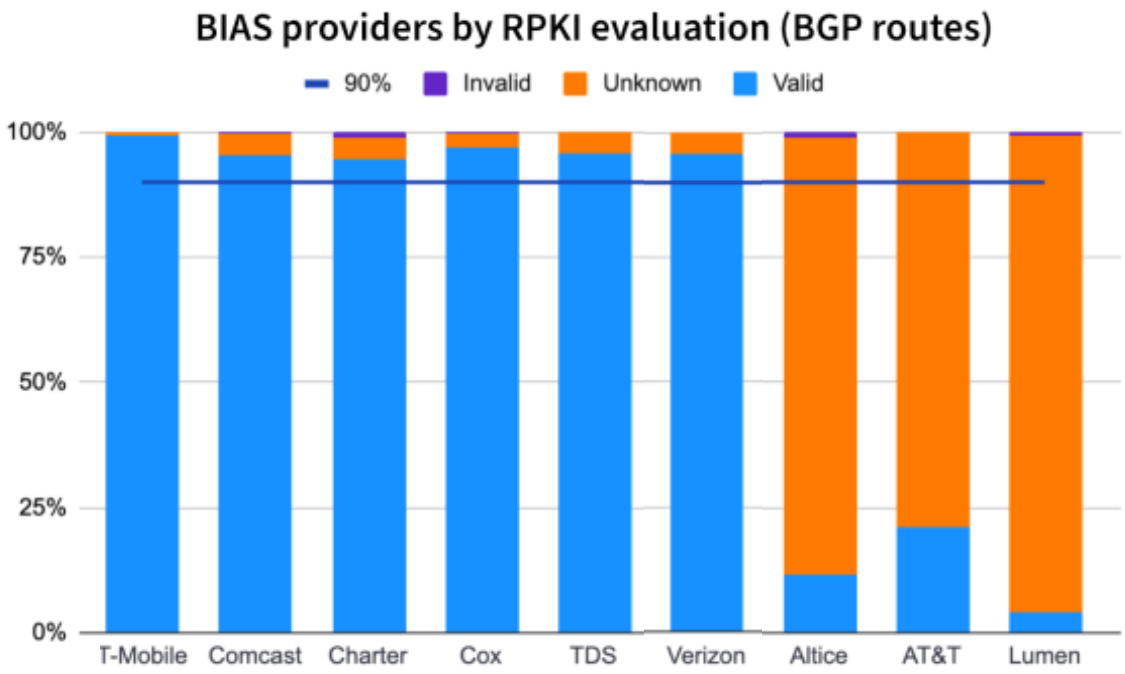
Zayo began rejecting RPKI-invalid routes from customers in April 2024

In July, the FCC published a proposal to require nine major US internet service providers to deploy RPKI Route Origin Validation (ROV).

> Describe the specific efforts made to create and maintain Route Origin Authorizations (ROAs) for **at least 90% of the routes under its control**. [¶ 37, 54]
> Describe the extent to which it has implemented ROV filtering at its interconnection points. [¶ 50]

In July we asked, where do these nine providers stand?

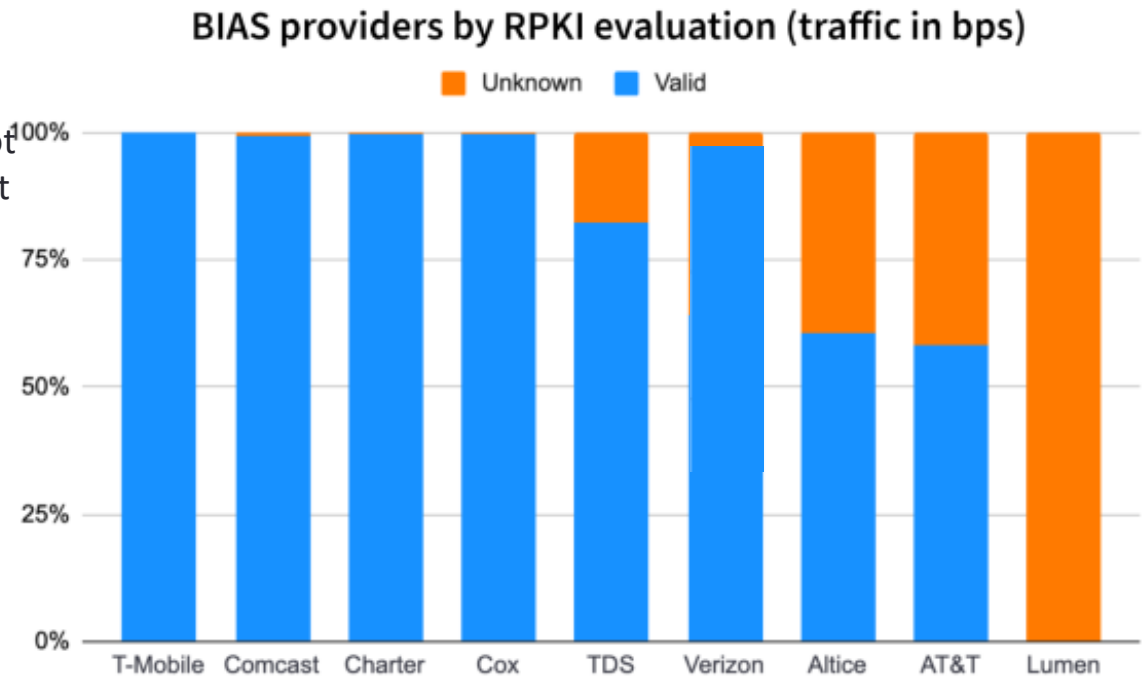
This metric could be gamed by providers who could de-aggregate space covered by ROAs and aggregate routes containing address space not covered by ROAs.



https://www.kentik.com/blog/dissecting-the-fccs-proposal-to-improve-bgp-security/

In July we asked, where do these nine providers stand?

One way to focus on risk is to not treat each BGP route equally but instead focus on *where traffic is going.*



https://www.kentik.com/blog/dissecting-the-fccs-proposal-to-improve-bgp-security/

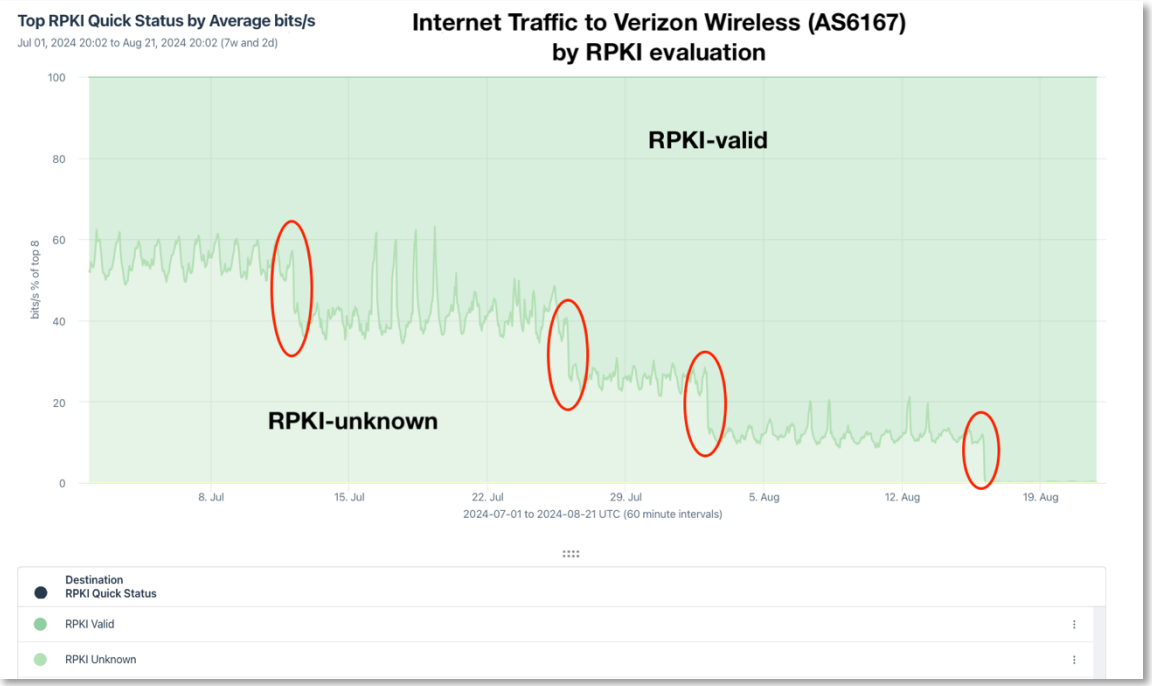
UPDATE: Verizon Wireless (AS6167) created a lot of ROAs this summer!

Verizon on the move!

ASNs: 701, 6167, 22394

Routes with ROAs:	56%	**95%**
Traffic %:	64%	**88%**

New ROAs put Verizon over the 90% threshold.



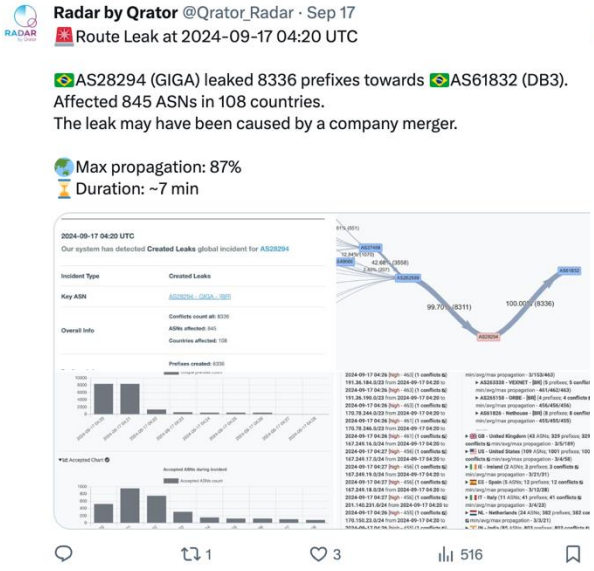
Measuring Success is Challenging

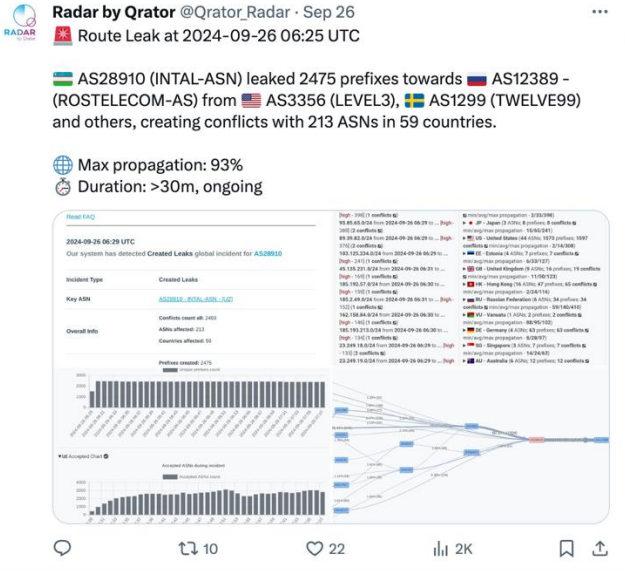
Classic security metrics challenge: how to measure non-events?

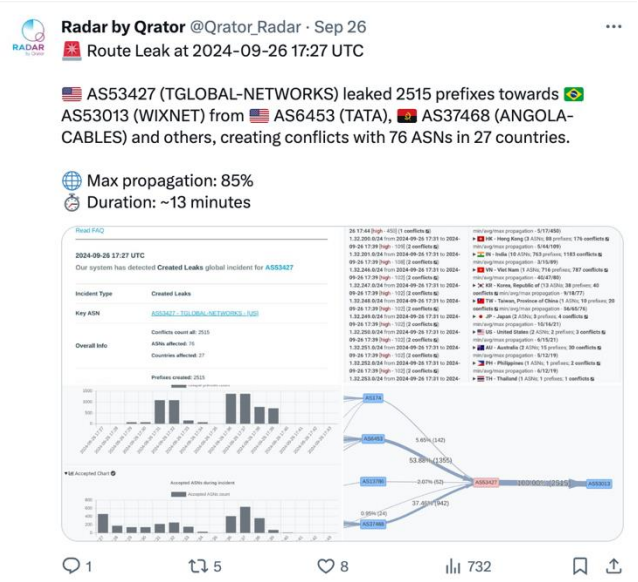
did not happen

Measuring Success is Challenging

Did you know?: Routing leaks are still occurring with some regularity!







Improvements in route hygiene are containing these leaks.

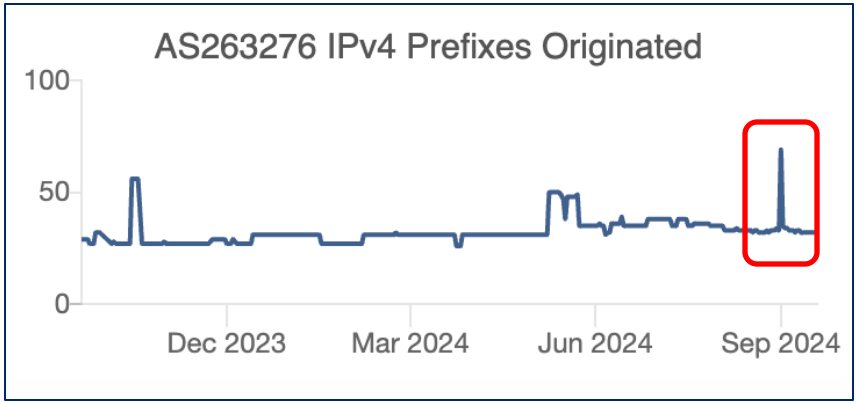
Measuring Success is Challenging

In September, Brazil ordered X (Twitter) to be blocked.

Some ISPs used BGP to hijack/blockhole X.

But the only hijacked X routes that appeared in public data were those without ROAs.

- Likely explanation: RPKI-invalids were rejected.
- No disruption of X outside of Brazil.
- RPKI-ROV did its job and no one knew.



Times have changed

Imagine if YouTube/Pakistan happened today would anyone notice?

Origination would be filtered by ROV (or another mechanism).

-events!

	119.159.255.0/24	Pakistan Telecommunication Company Limited
	154.198.13.0/24	Telenor Microfinance Bank Ltd
	172.40.52.0/24	
	182.176.0.0/24	Pakistan Telecommuication company limited

Conclusion

The system is working as designed!

Progress due to the dedicated efforts of hundreds of engineers at dozens of companies.

- 1/2 of BGP routes have ROAs, >2/3 of traffic (bps) went to routes with ROAs
- Propagation of RPKI-invalids continues to decline, Zayo now rejecting invalids

- scenarios best characterized by the recent attacks against cryptocurrency services.

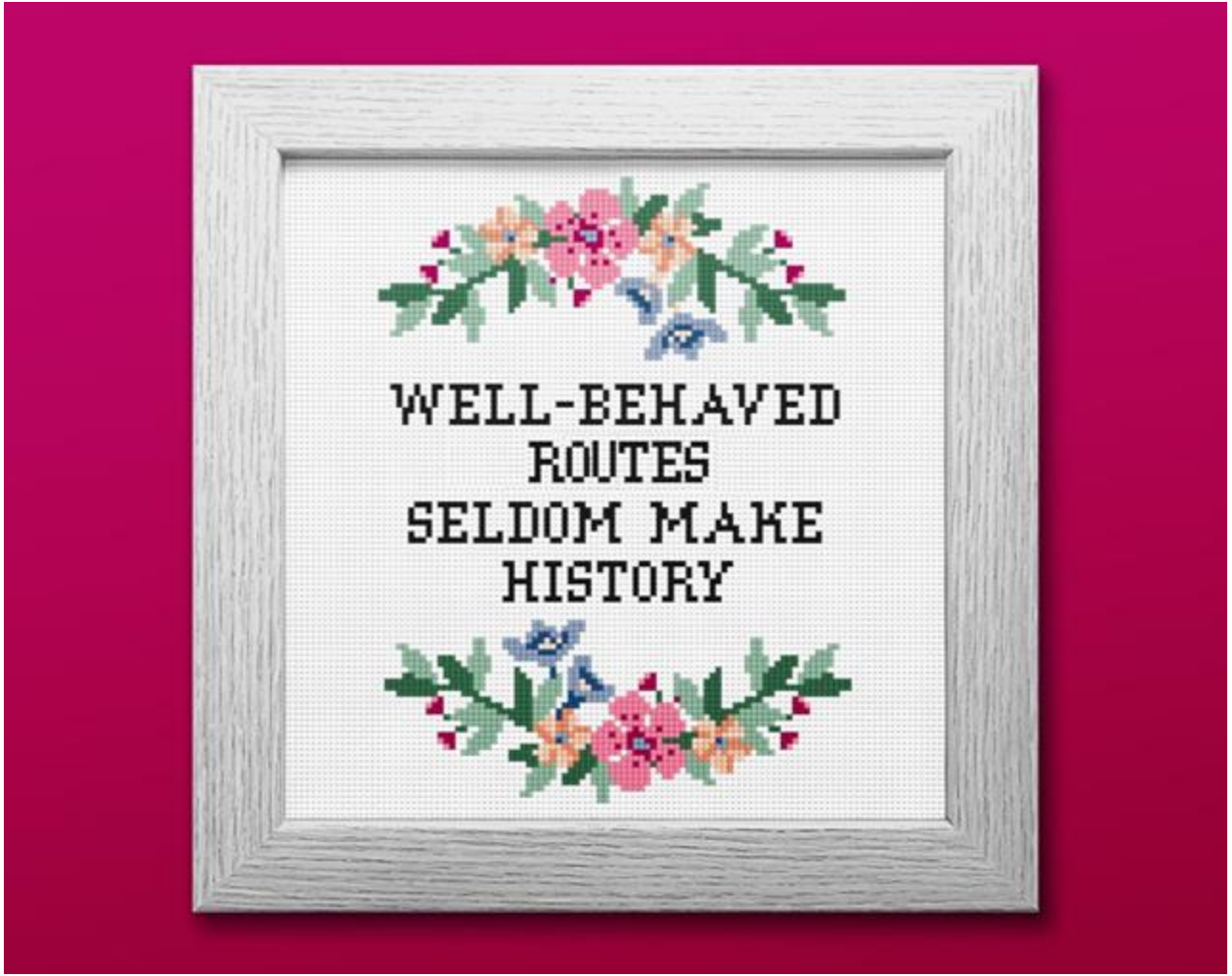
Need to build off the progress made by RPKI ROV to address more difficult scenarios.

Thank you!

Doug Madory
dmadory@kentik.com

@DougMadory

in/DougMadory



Internet Intelligence Lab

Observing trends in Internet routing security

NANOG 92, Toronto

Alberto Dainotti
dainotti@gatech.edu

October 23rd, 2024

Internet Intelligence Lab

GRIP — https://bgp.live (grip.inetintel.cc.gatech.edu)

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 22, 2023 3:16 AM): Jun 20, 2023 9:41 PM - Jun 21, 2023 9:41 PM

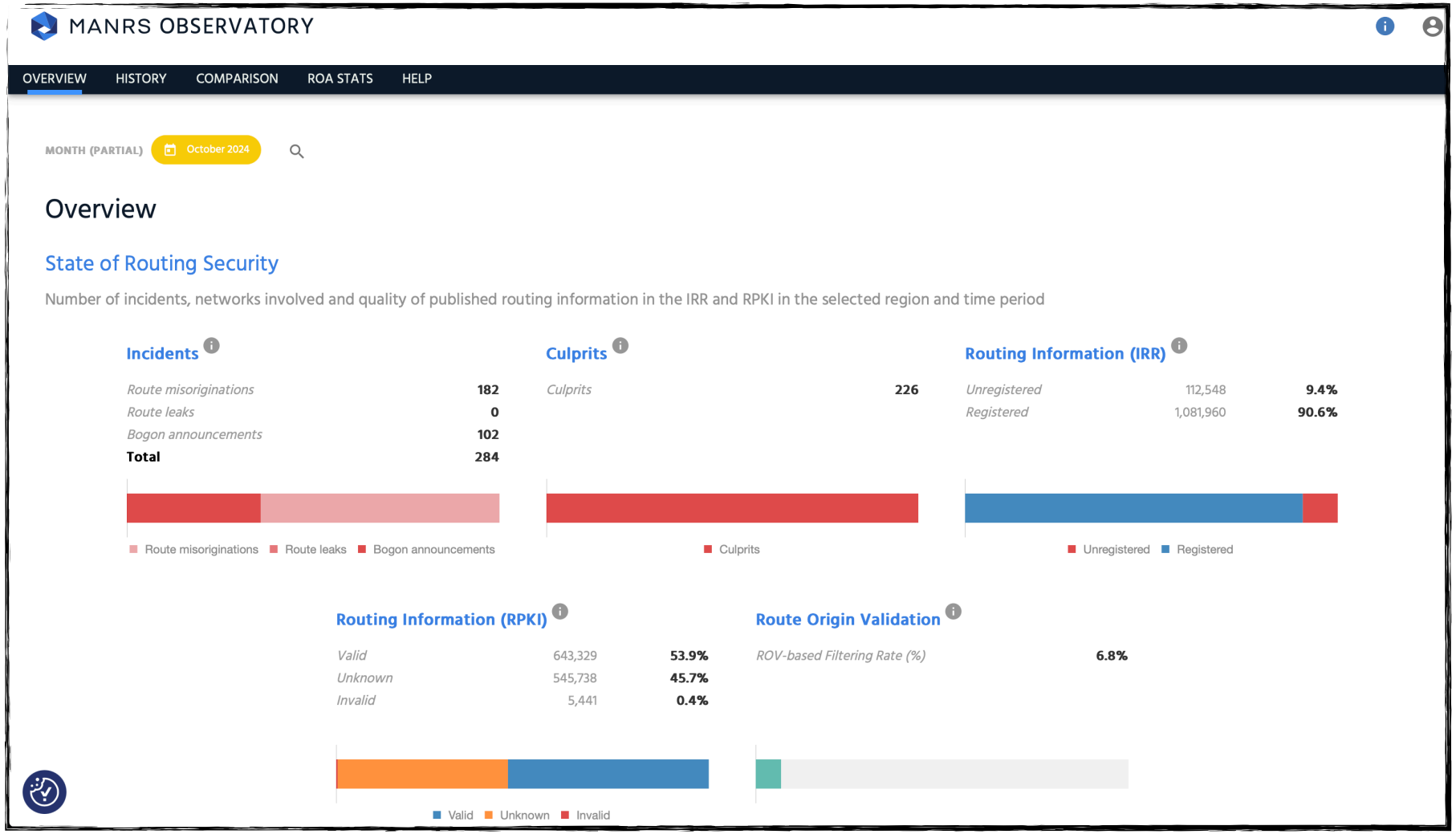
Search for events by prefix/ASN/tags: Search by prefix/ASN/tags | Search

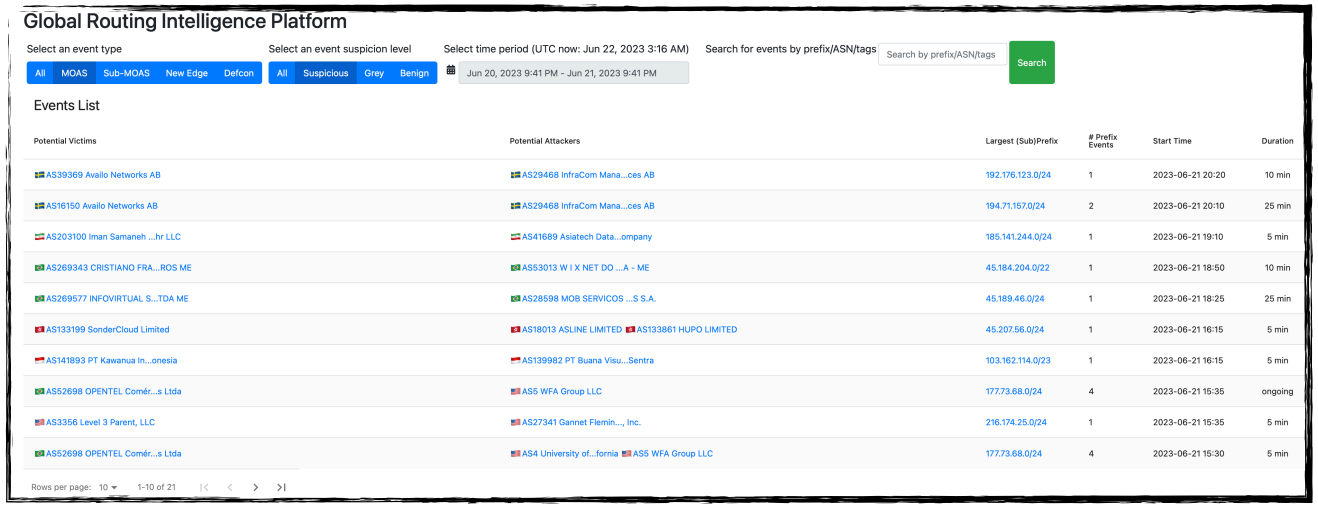
Events List

Potential Victims	Potential Attackers	Largest (Sub)Prefix	# Prefix Events	Start Time	Duration
AS39369 Availo Networks AB	AS29468 InfraCom Mana...ces AB	192.176.123.0/24	1	2023-06-21 20:20	10 min
AS16150 Availo Networks AB	AS29468 InfraCom Mana...ces AB	194.71.157.0/24	2	2023-06-21 20:10	25 min
AS203100 Iman Samaneh ...hr LLC	AS41689 Asiatech Data...ompany	185.141.244.0/24	1	2023-06-21 19:10	5 min
AS269343 CRISTIANO FRA...ROS ME	AS53013 W I X NET DO ...A - ME	45.184.204.0/22	1	2023-06-21 18:50	10 min
AS269577 INFOVIRTUAL S...TDA ME	AS28598 MOB SERVICOS ...S S.A.	45.189.46.0/24	1	2023-06-21 18:25	25 min
AS133199 SonderCloud Limited	AS18013 ASLINE LIMITED AS133861 HUPO LIMITED	45.207.56.0/24	1	2023-06-21 16:15	5 min
AS141893 PT Kawanua In...onesia	AS139982 PT Buana Visu...Sentra	103.162.114.0/23	1	2023-06-21 16:15	5 min
AS52698 OPENTEL Comér...s Ltda	AS5 WFA Group LLC	177.73.68.0/24	4	2023-06-21 15:35	ongoing
AS3356 Level 3 Parent, LLC	AS27341 Gannet Flemin..., Inc.	216.174.25.0/24	1	2023-06-21 15:35	5 min
AS52698 OPENTEL Comér...s Ltda	AS4 University of...fornia AS5 WFA Group LLC	177.73.68.0/24	4	2023-06-21 15:30	5 min

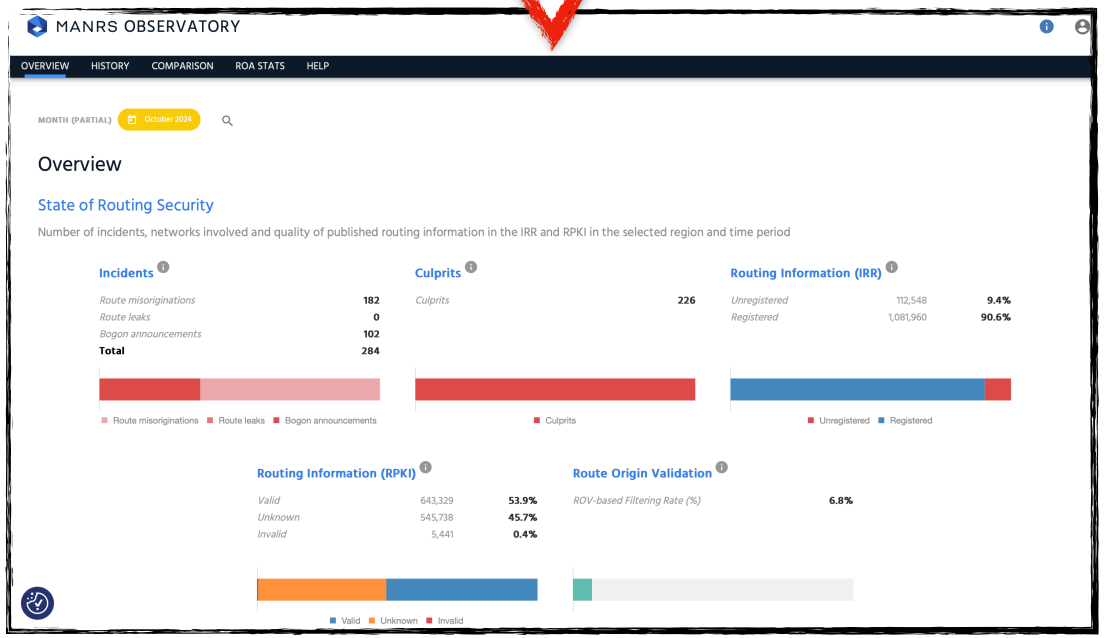
Rows per page: 10 1-10 of 21

MANRS Observatory





GRIP



MANRS Observatory

BGP Incident Monitoring & Analysis in the 2020s

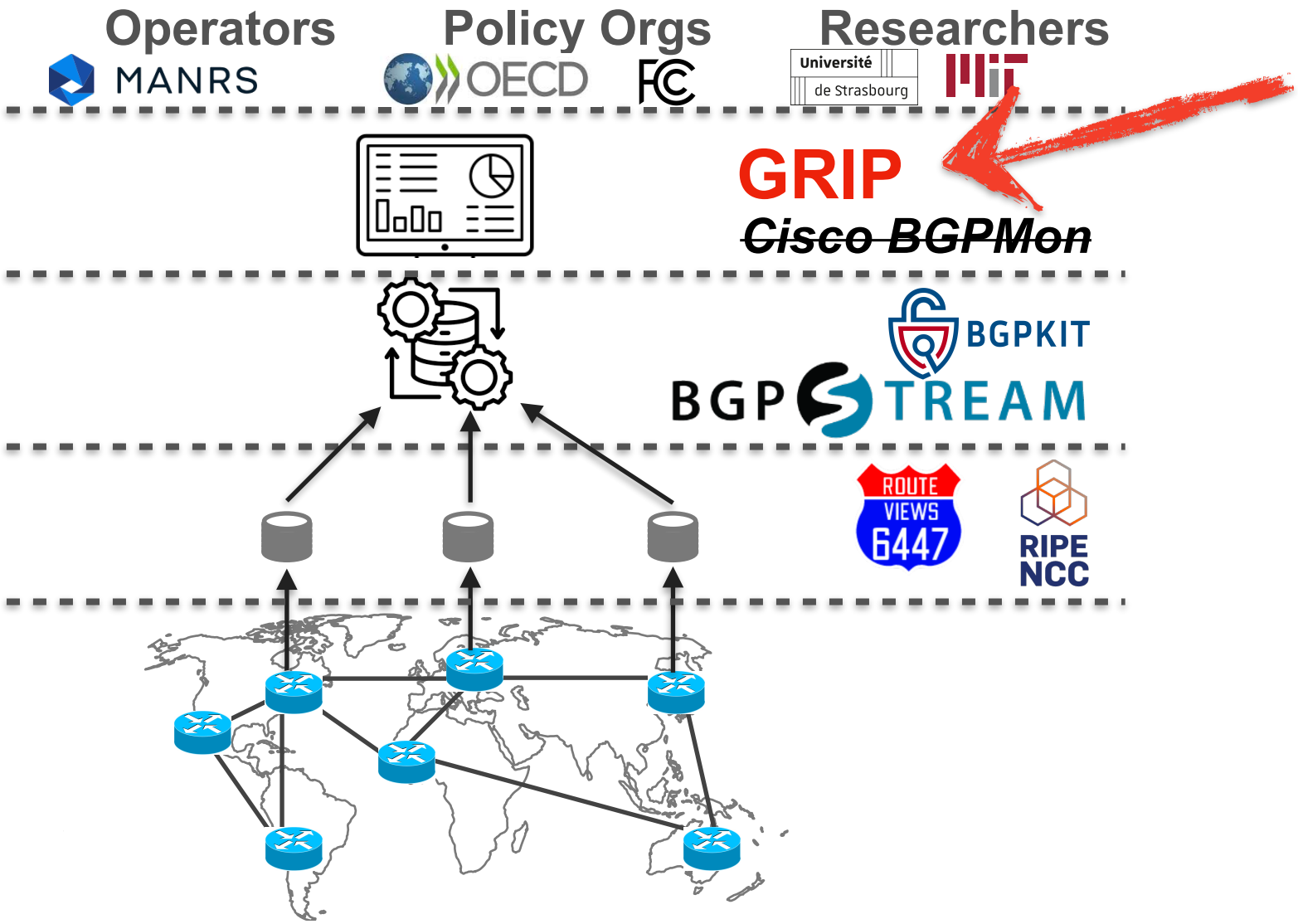
BGP Incident Study & Analysis

BGP Incident Detection & Monitoring

BGP Data Processing Software

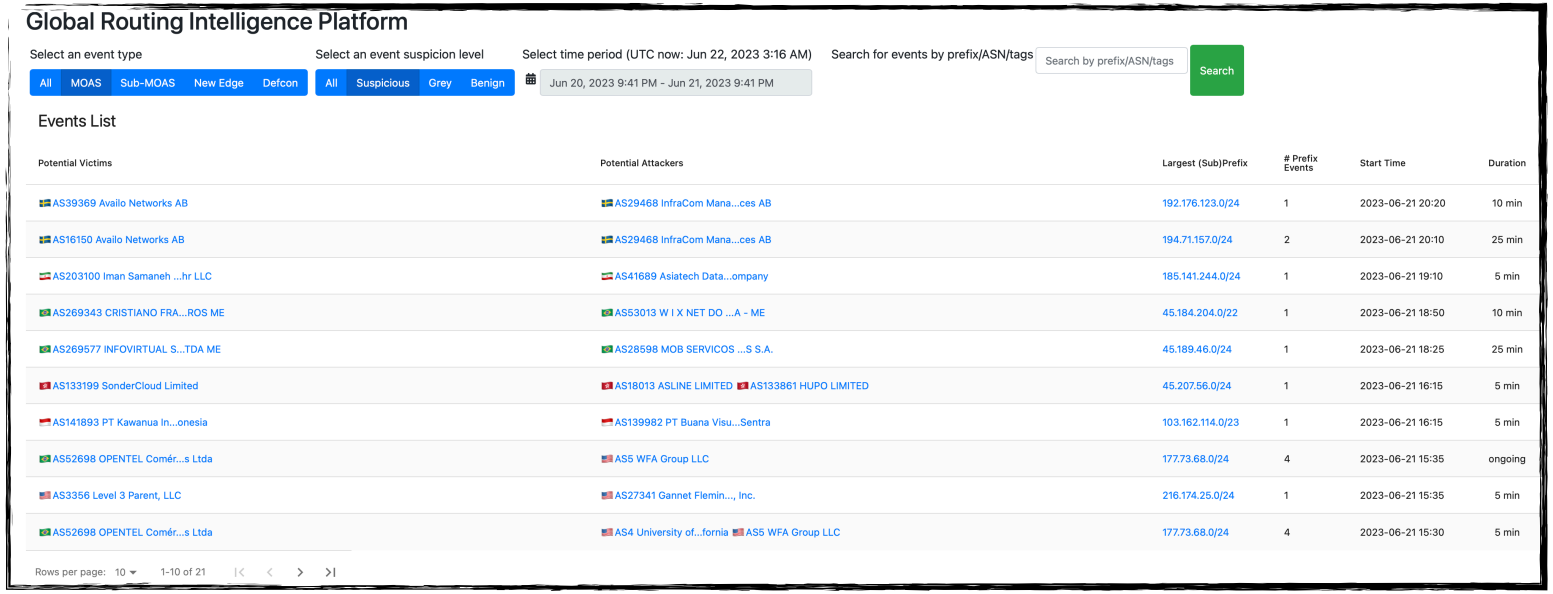
BGP Data Collection Projects

Internet Routing



GRIP and NANOG 92

- Been around since ~2018 (CAIDA); running @ GATech since 2021
- Public dashboard + API; Open source
- Annotation and inference methods constantly improving
- NANOG 92: We reprocessed the last 5 years to uncover trends

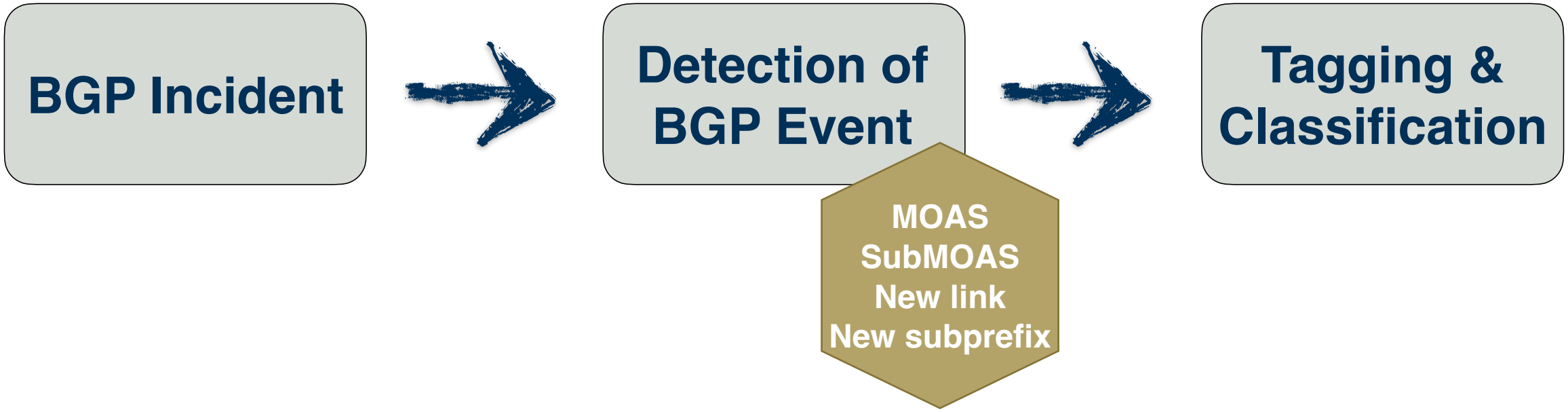


https://bgp.live

What do we know about routing incidents actually happening?

How does GRIP work?

- Target: *All* types of hijacking attacks and hijacking misconfigurations



Classification of events — where we are now

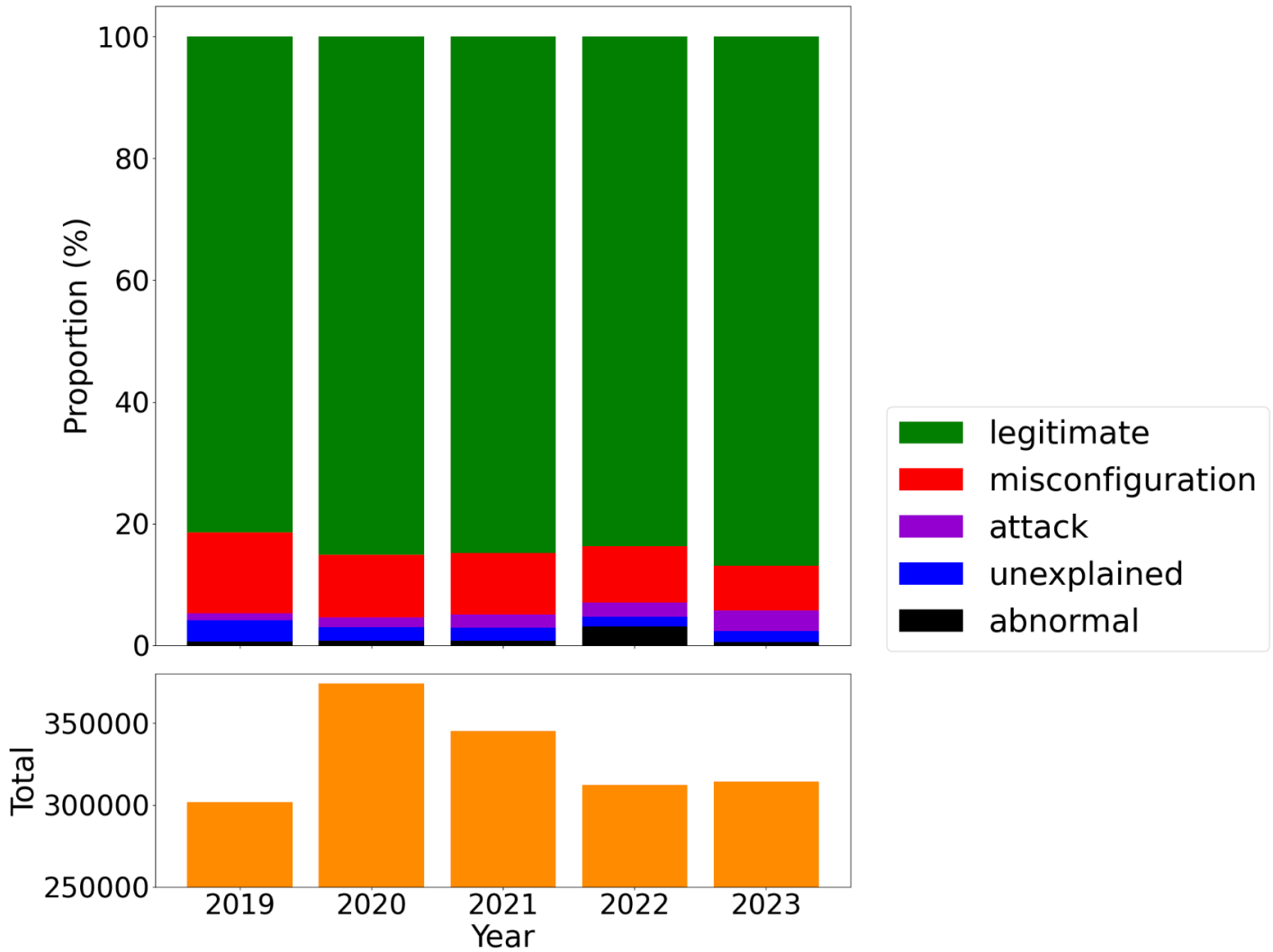
MOAS
SubMOAS
~~New link~~
~~New subprefix~~

- We mark most of the events as legitimate [85%]
- Most incidents show misconfiguration patterns [10%]
  - Fat finger of prefix/ASN
  - Path prepending gone wrong
  - Related ASes but RPKI invalid …
- Many events w/ patterns of attacks [2%]
  - or misconfigs hard to diagnose → *E.g., RPKI invalid but owners failed to publish correct ROAs*
- Unable to explain several events [2%]

- **Legitimate 85%; ~280k/yr**
- **Incidents 15%; ~50k/yr**
  - Misconfigs 10%; 33k/yr
  - Attacks 2%; 7k/yr
  - Unexplained 2%; 7k/yr
  - Abnormal 1%; 3k/yr

data from GRIP (https://bgp.live)

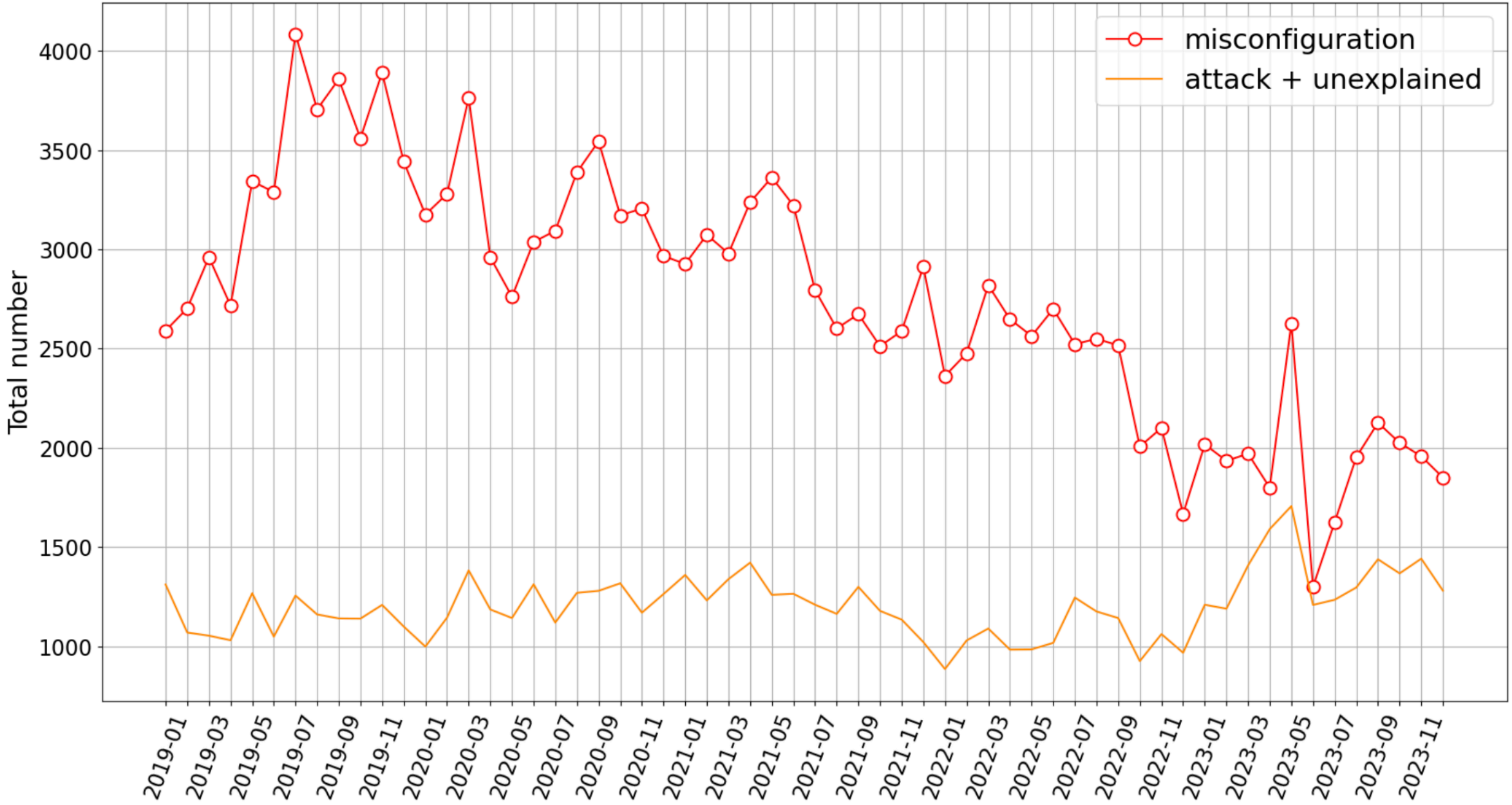
Classification of events: trend by year



- **Legitimate 85%; ~280k/yr**
- **Incidents 15%; ~50k/yr**
  - Misconfigs 10%; 33k/yr
  - Attacks 2%; 7k/yr
  - Unexplained 2%; 7k/yr
  - Abnormal 1%; 3k/yr

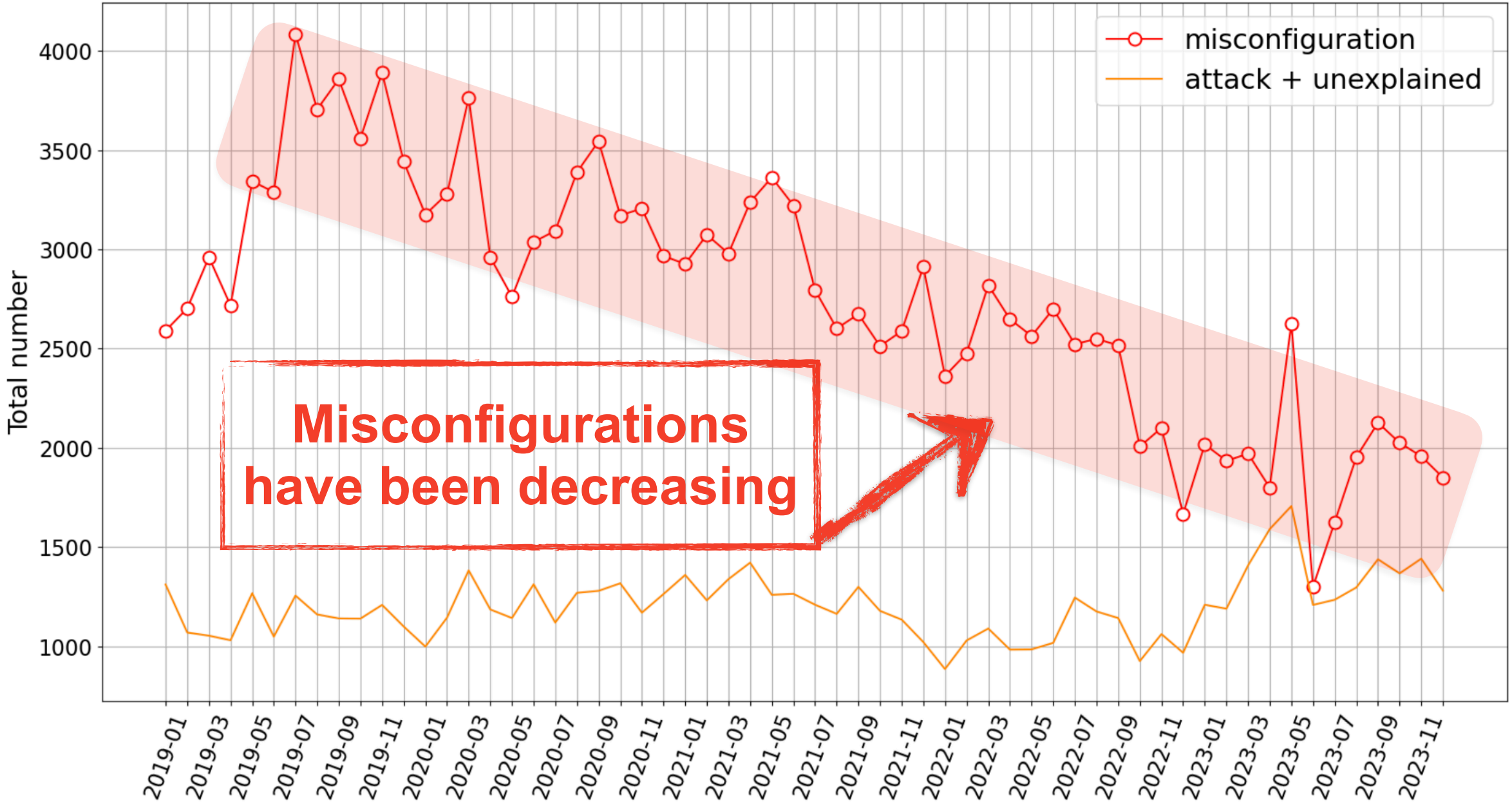
data from GRIP (https://bgp.live)

Incidents



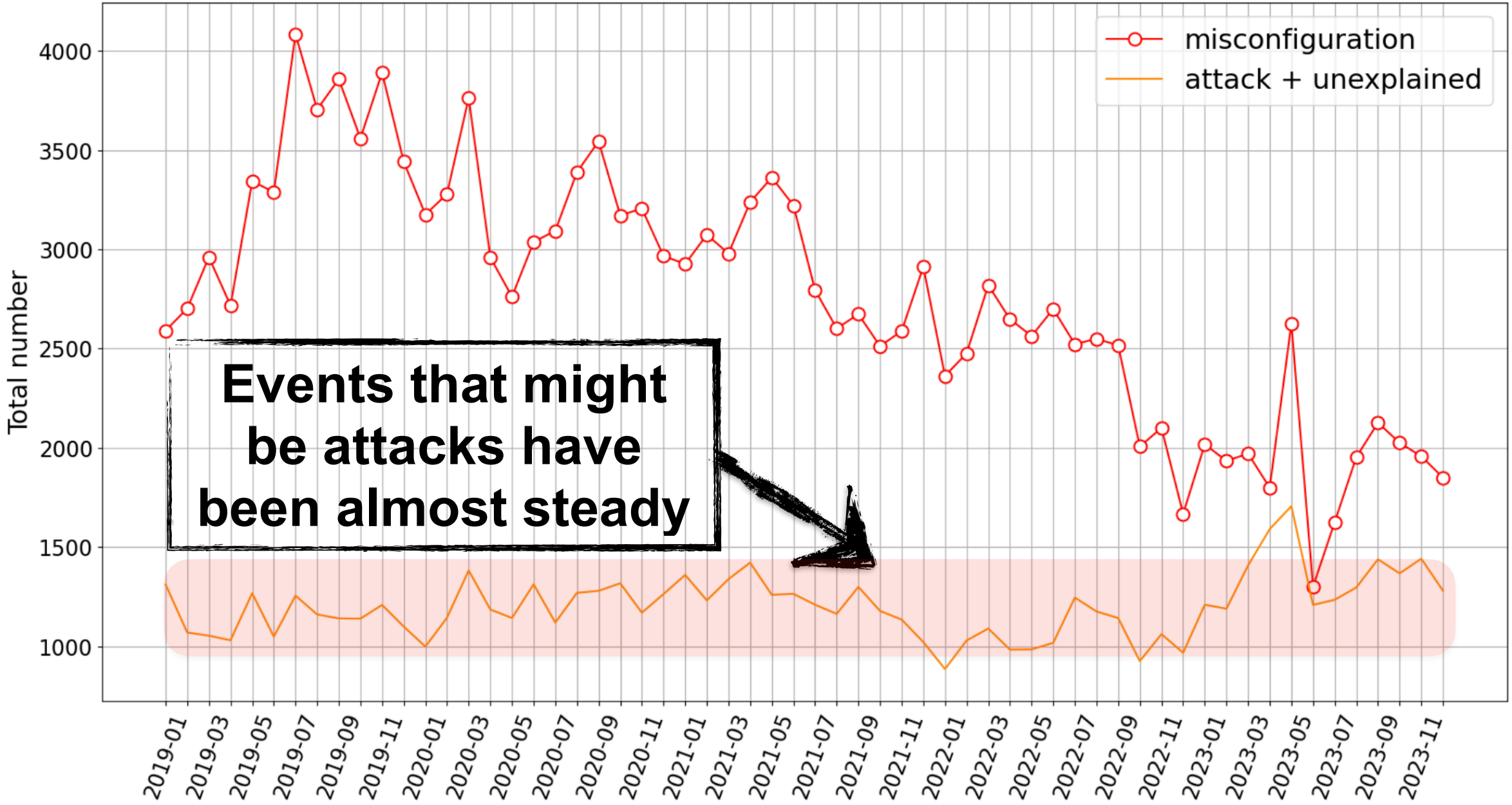
data from GRIP (https://bgp.live)

Incidents



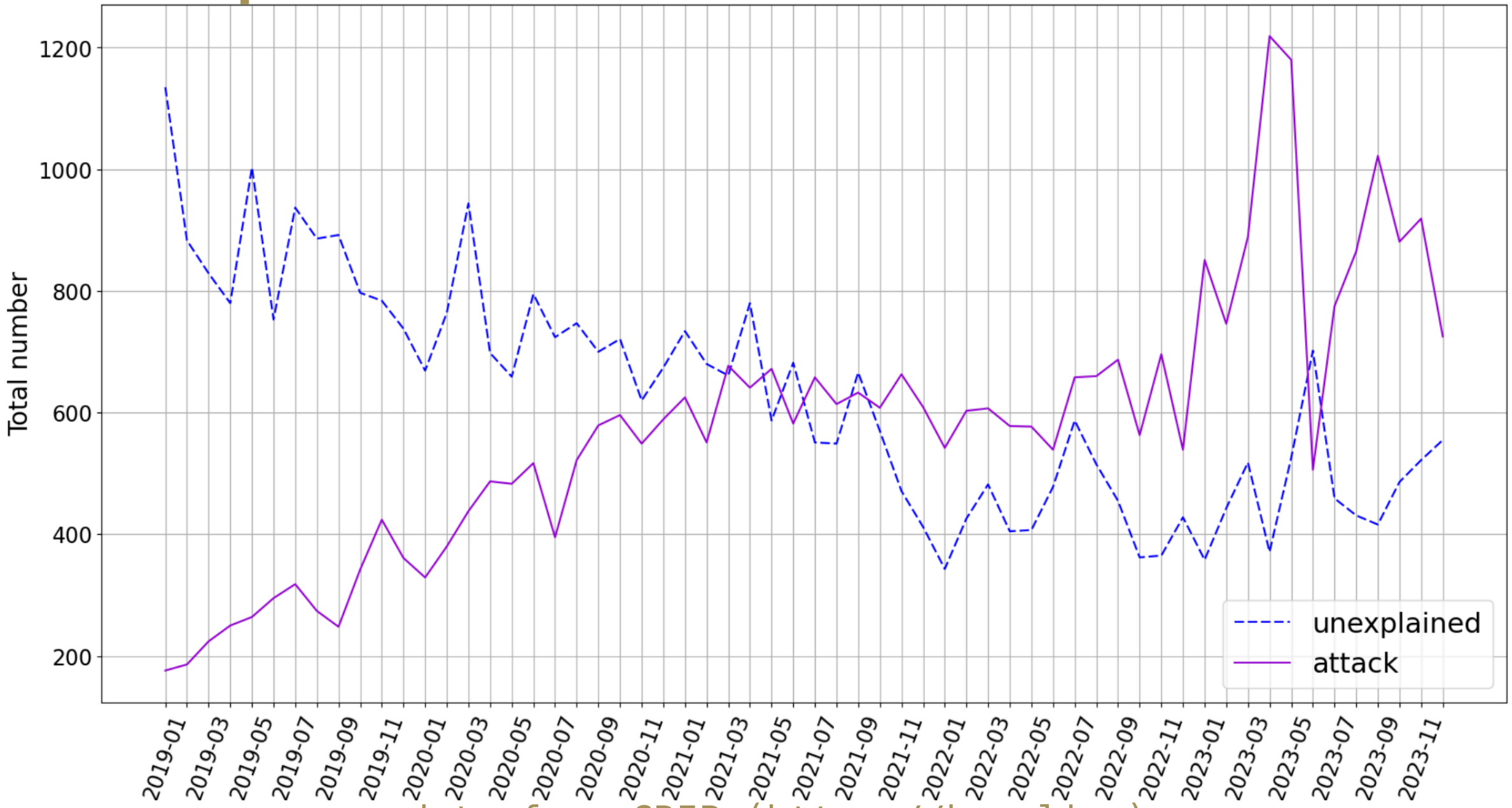
data from GRIP (https://bgp.live)

Incidents



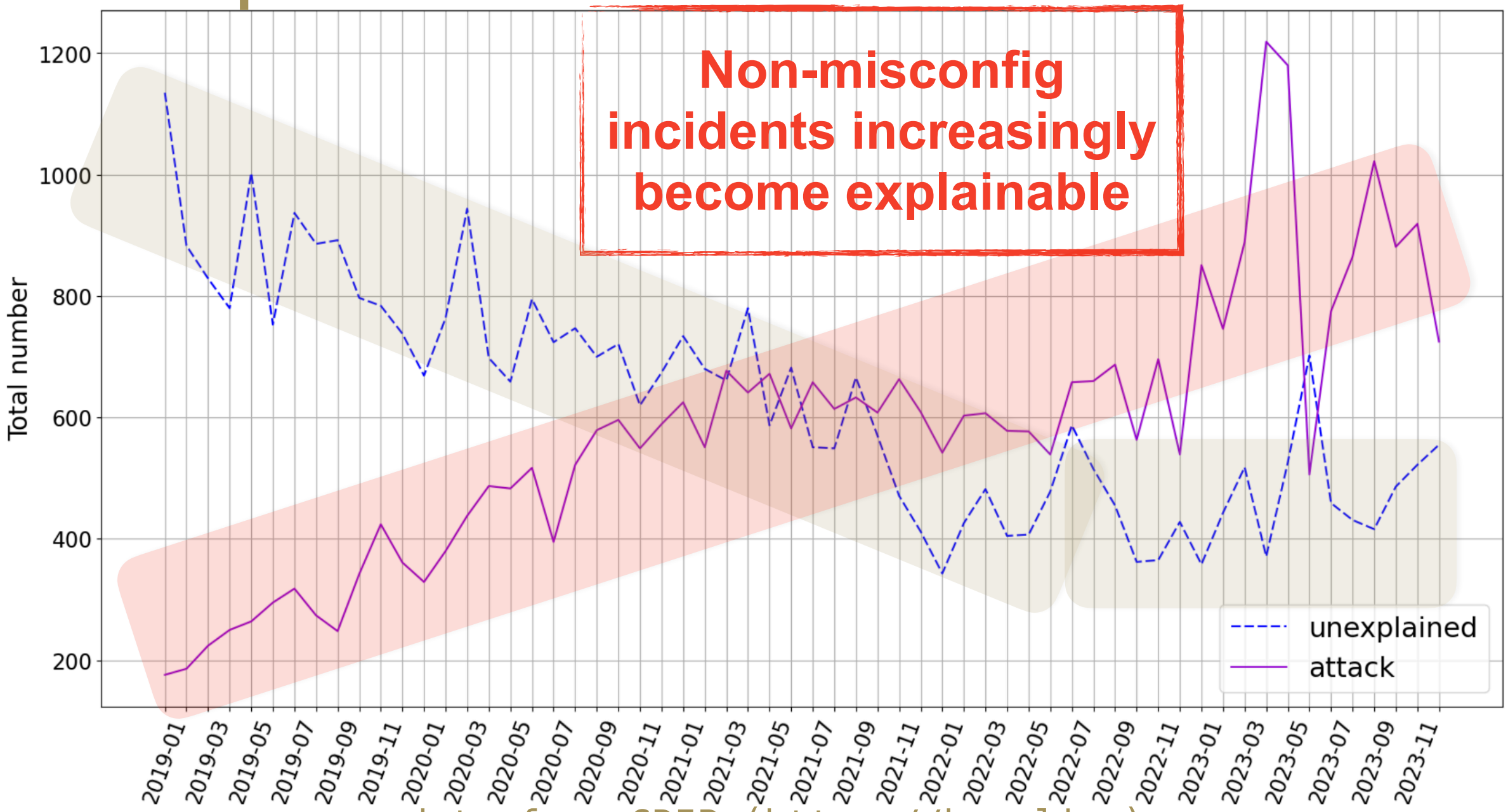
data from GRIP (https://bgp.live)

More “explainable” events



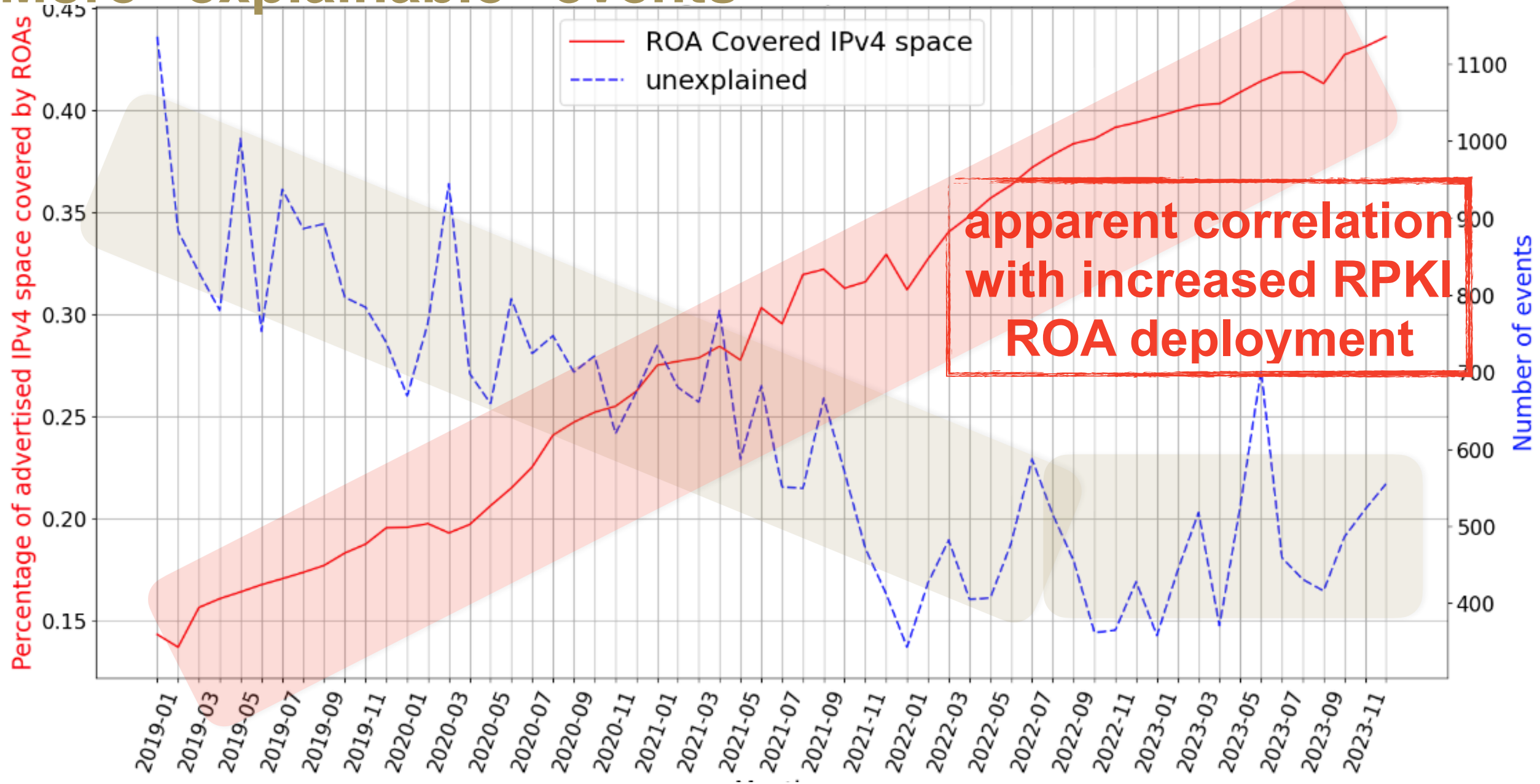
data from GRIP (https://bgp.live)

More “explainable” events



data from GRIP (https://bgp.live)

More “explainable” events



data from GRIP (https://bgp.live)

Incidents: more about misconfigurations…

https://grip.inetintel.cc.gatech.edu/events/moas/moas-1726358400-3_328494/102.69.223.0-24

Example of path prepending misconfig

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: Oct 16, 2024 10:35 PM): Oct 16, 2023 10:35 PM - Oct 16, 2024 10:35 PM

Search for events by prefix/ASN/tags: AS3 [Search]

Prefix Event Details

Potential Victim:	AS328494	**Start time:**	2024-09-15 00:00
Potential Attacker:	AS3	**End time:**	2024-09-15 00:05
Event type:	origin hijack (moas)	**Duration:**	5 min
Prefixes:	102.69.223.0/24		

Tags:

- Irr REACH All Oldcomer No Record
- Irr APNIC All Oldcomer No Record
- All Victims Stub Ases
- Irr OPENFACE All Oldcomer No Record
- Irr RIPE NONAUTH All Oldcomer No Record
- Irr REACH All Newcomer No Record
- Irr RADB All Oldcomer Exact Record
- Irr BELL All Oldcomer No Record
- Irr IDNIC All Newcomer No Record
- Irr LACNIC All Oldcomer No Record
- Irr CANARIE All Oldcomer No Record
- Irr ALTDB All Newcomer No Record
- Rpki All Oldcomer Unknown Roa
- Rpki All Newcomer Unknown Roa
- Irr RADB All Newcomer No Record
- Irr NTTCOM All Oldcomer No Record
- Irr RIPE NONAUTH All Newcomer No Record
- Rpki Some Newcomer Unknown Roa
- Rpki Some Oldcomer Unknown Roa
- Irr ARIN All Oldcomer No Record
- Irr NESTEGG All Oldcomer No Record
- Irr WCGDB All Oldcomer No Record
- Irr NTTCOM All Newcomer No Record
- Irr TC All Oldcomer No Record
- Irr JPIRR All Newcomer No Record
- Irr RIPE All Oldcomer No Record
- Not Previously Announced By Any Newcomer
- Irr BBOI All Newcomer No Record
- Irr WCGDB All Newcomer No Record
- Irr NESTEGG All Newcomer No Record
- Irr LEVEL3 All Oldcomer No Record
- Irr PANIX All Oldcomer No Record
- Irr PANIX All Newcomer No Record
- Irr TC All Newcomer No Record
- Irr IDNIC All Oldcomer No Record
- Irr AFRINIC All Oldcomer More Specific Record

https://grip.inetintel.cc.gatech.edu/events/moas/moas-1726358400-3_328494/102.69.223.0-24

Example of path prepending misconfig

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: Oct 16, 2024 10:35 PM): Oct 16, 2023 10:35 PM - Oct 16, 2024 10:35 PM

Search for events by prefix/ASN/tags: AS3 | Search

Event type:	origin hijack (moas)	**Duration:**	5 min
Prefixes:	102.69.223.0/24		

Tags:

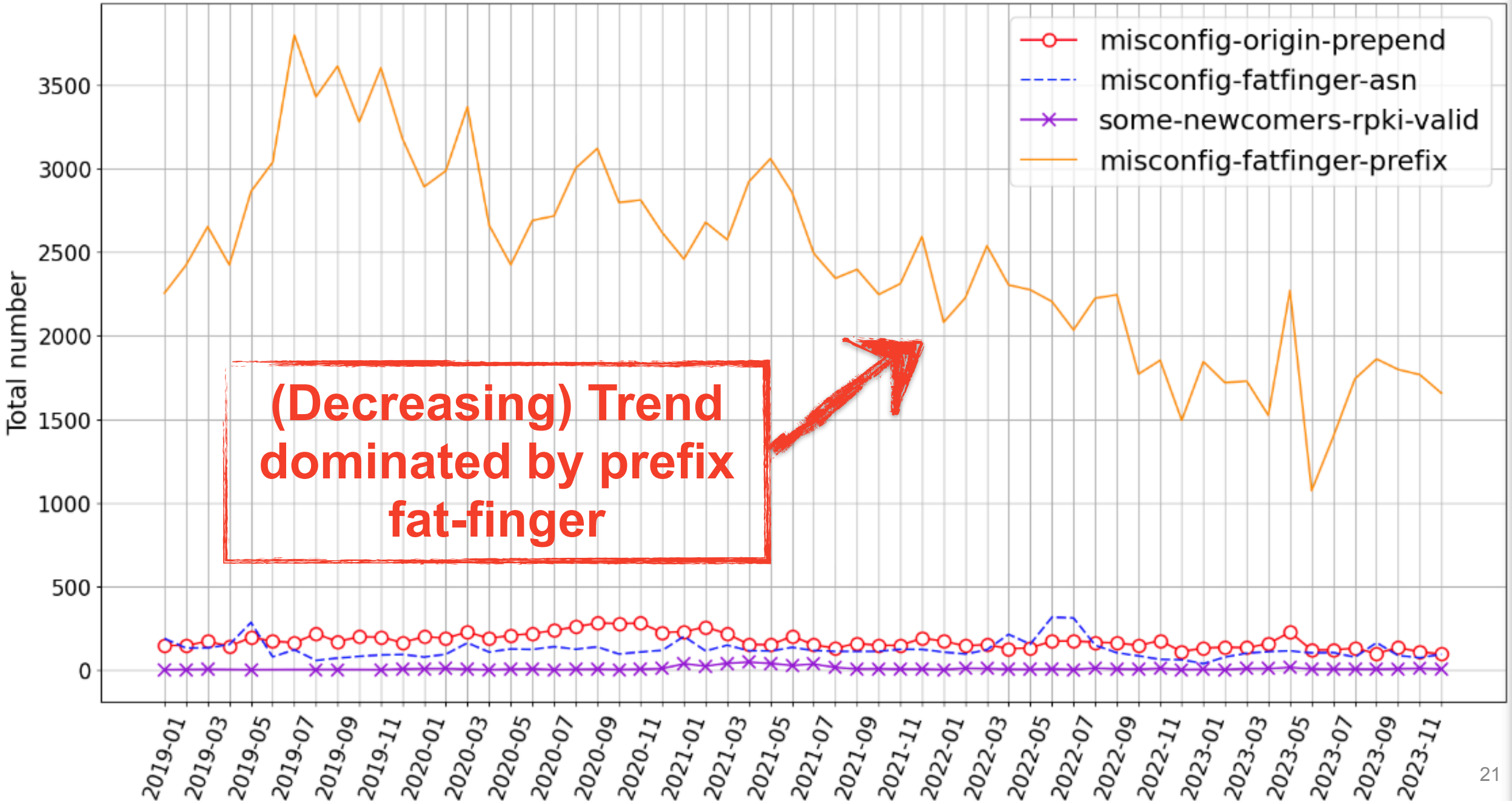
- Irr REACH All Oldcomer No Record
- Irr APNIC All Oldcomer No Record
- All Victims Stub Ases
- Irr OPENFACE All Oldcomer No Record
- Irr RIPE NONAUTH All Oldcomer No Record
- Irr REACH All Newcomer No Record
- Irr RADB All Oldcomer Exact Record
- Irr BELL All Oldcomer No Record
- Irr IDNIC All Newcomer No Record
- Irr LACNIC All Oldcomer No Record
- Irr CANARIE All Oldcomer No Record
- Irr ALTDB All Newcomer No Record
- Rpki All Oldcomer Unknown Roa
- Rpki All Newcomer Unknown Roa
- Irr RADB All Newcomer No Record
- Irr NTTCOM All Oldcomer No Record
- Irr RIPE NONAUTH All Newcomer No Record
- Rpki Some Newcomer Unknown Roa
- Rpki Some Oldcomer Unknown Roa
- Irr ARIN All Oldcomer No Record
- Irr NESTEGG All Oldcomer No Record
- Irr WCGDB All Oldcomer No Record
- Irr NTTCOM All Newcomer No Record
- Irr TC All Oldcomer No Record
- Irr JPIRR All Newcomer No Record
- Irr RIPE All Oldcomer No Record
- Not Previously Announced By Any Newcomer
- Irr BBOI All Newcomer No Record
- Irr WCGDB All Newcomer No Record
- Irr NESTEGG All Newcomer No Record
- Irr LEVEL3 All Oldcomer No Record
- Irr PANIX All Oldcomer No Record
- Irr PANIX All Newcomer No Record
- Irr TC All Newcomer No Record
- Irr IDNIC All Oldcomer No Record
- Irr AFRINIC All Oldcomer More Specific Record
- Irr AFRINIC All Newcomer No Record
- Irr JPIRR All Oldcomer No Record
- Irr ARIN All Newcomer No Record
- Some Victims Stub Ases
- Irr BBOI All Oldcomer No Record
- Irr APNIC All Newcomer No Record
- Irr LEVEL3 All Newcomer No Record
- Irr ALTDB All Oldcomer No Record
- All Newcomers Next To An Oldcomer
- Irr CANARIE All Newcomer No Record
- Irr LACNIC All Newcomer No Record
- Irr BELL All Newcomer No Record
- Newcomer Small Asn
- Oldcomers Always On Newcomer Originated Paths
- Irr OPENFACE All Newcomer No Record
- Irr RIPE All Newcomer No Record

Misconfigurations (2019-2023)

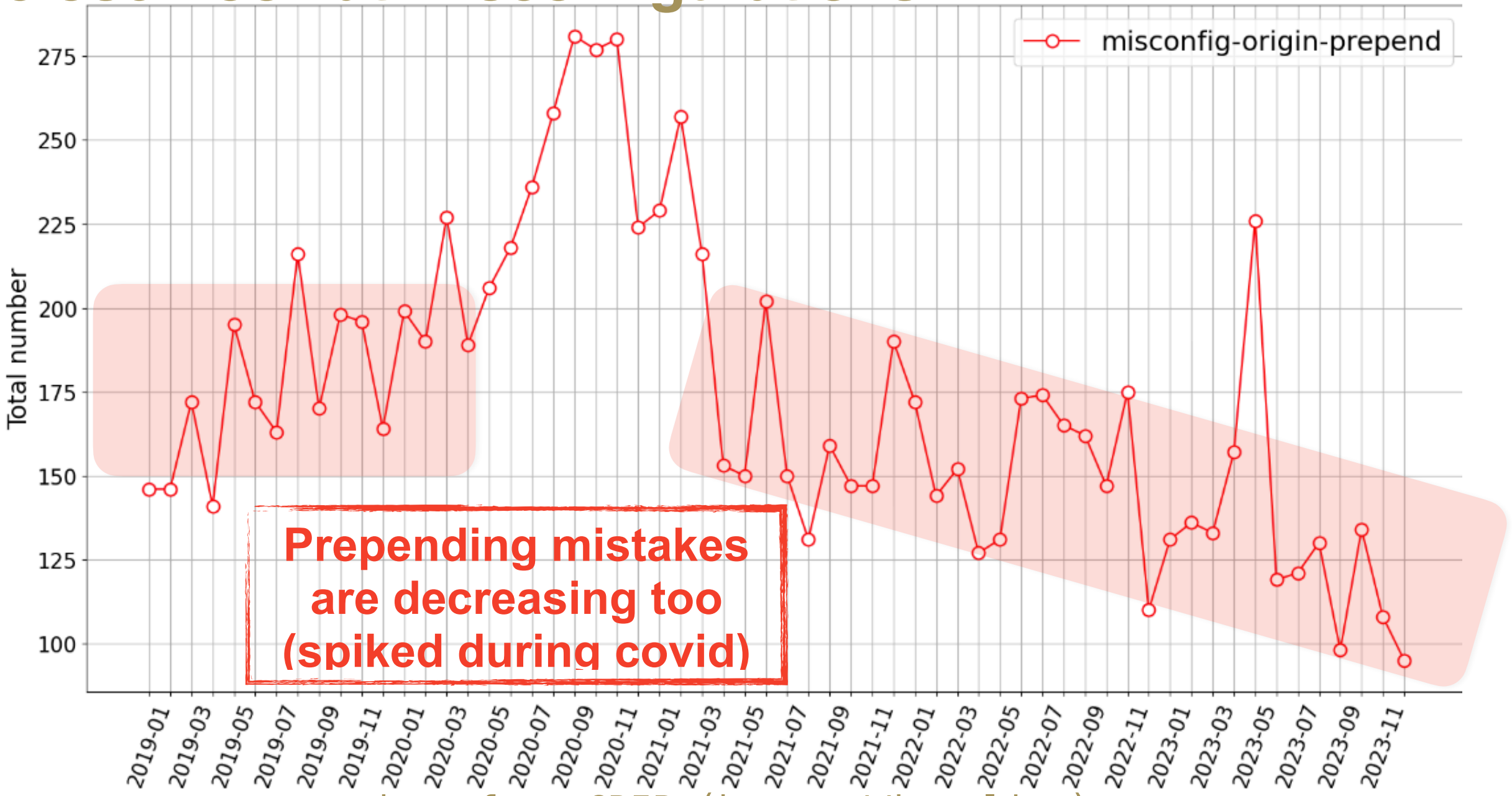
- Median duration
  - misconfig-origin-prepend: 15 min
  - misconfig-fatfinger-asn: 45 min
  - some-newcomers-rpki-valid: 60 min
  - misconfig-fatfinger-prefix: 500 min (> 8hrs)

data from GRIP (https://bgp.live)

A closer look at misconfigurations



A closer look at misconfigurations



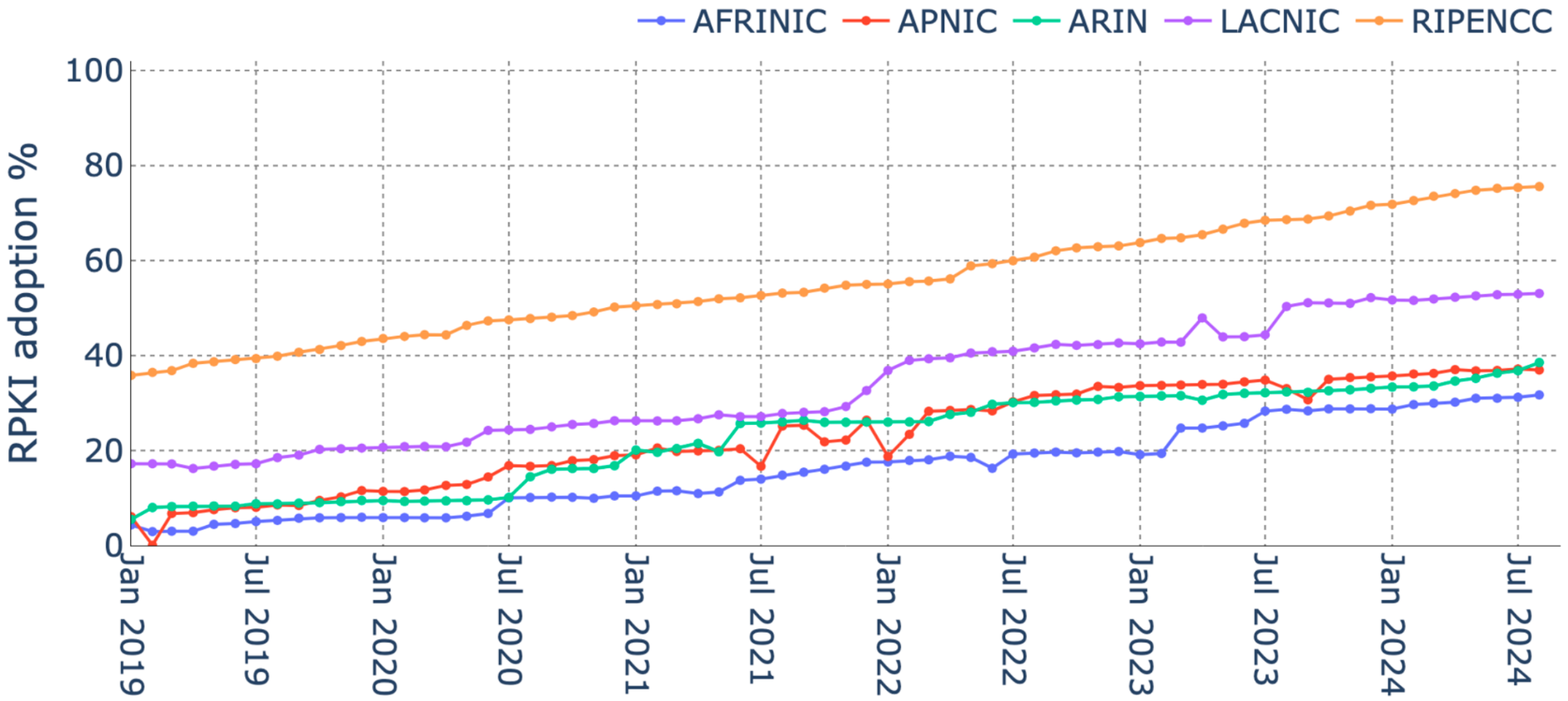
data from GRIP (https://bgp.live)

Barriers to RPKI deployment (led by Cecilia Testart)

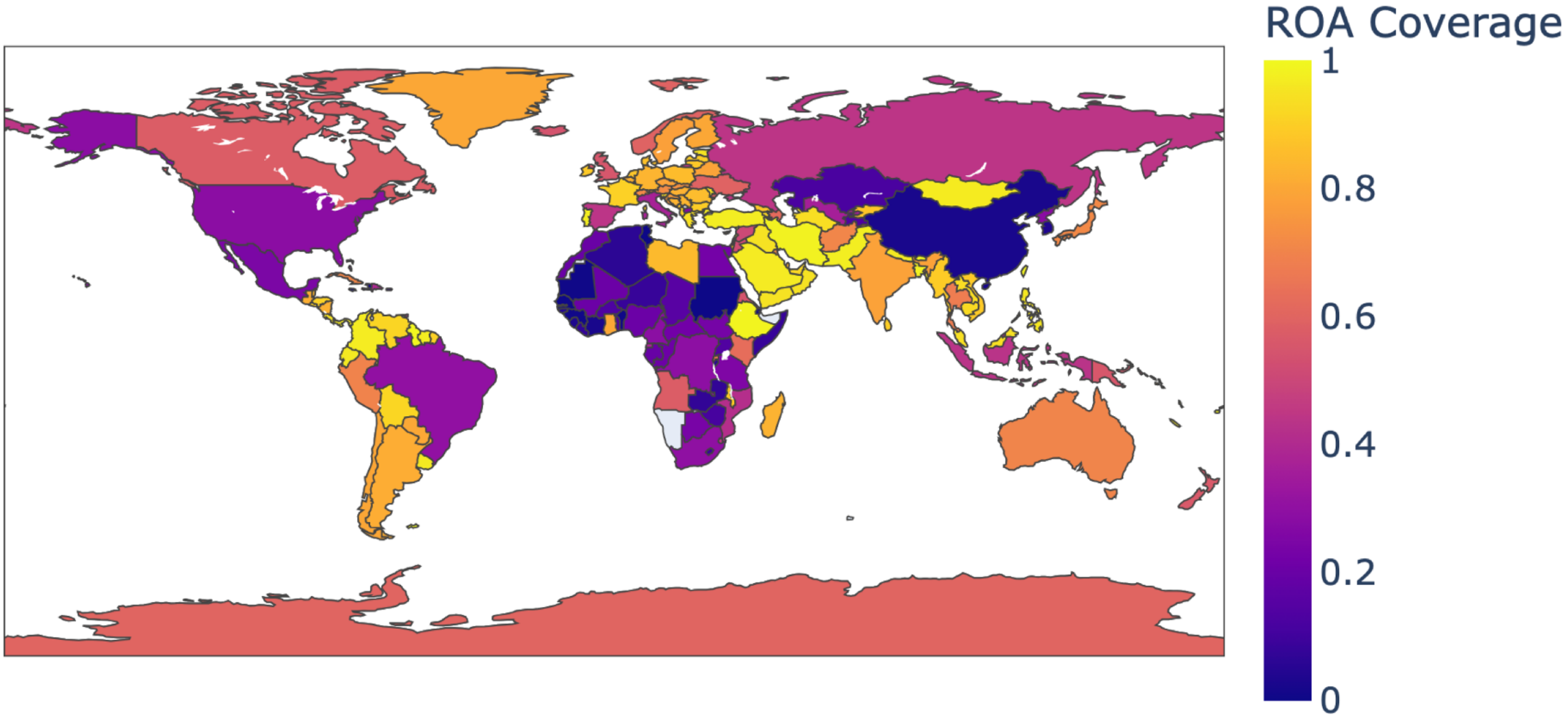
RPKI adoption status & challenges

- In 2024, ~50% IP address blocks in BGP are still not covered by RPKI
- Which types of networks are lagging in RPKI adoption and why?

- Four key characteristics impact organizations' RPKI adoption levels:
  - Geography
  - Network size
  - Business category
  - Complexity of the address space



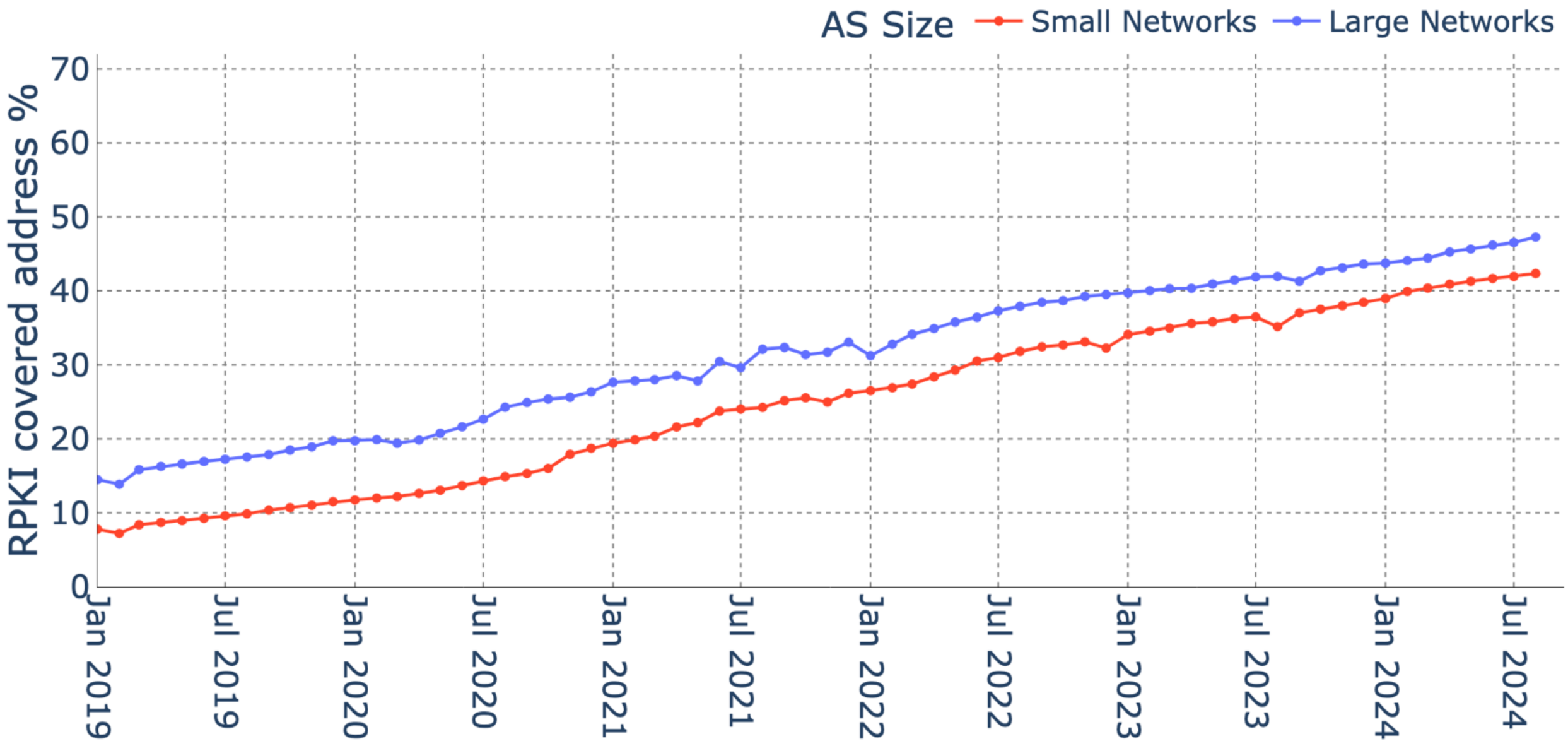
(Regional Internet Registries (RIRs) are the root of trust to verify the cryptographic validity of RPKI records. Each RIR has independently set up the process to issue and publish ROAs in their region)



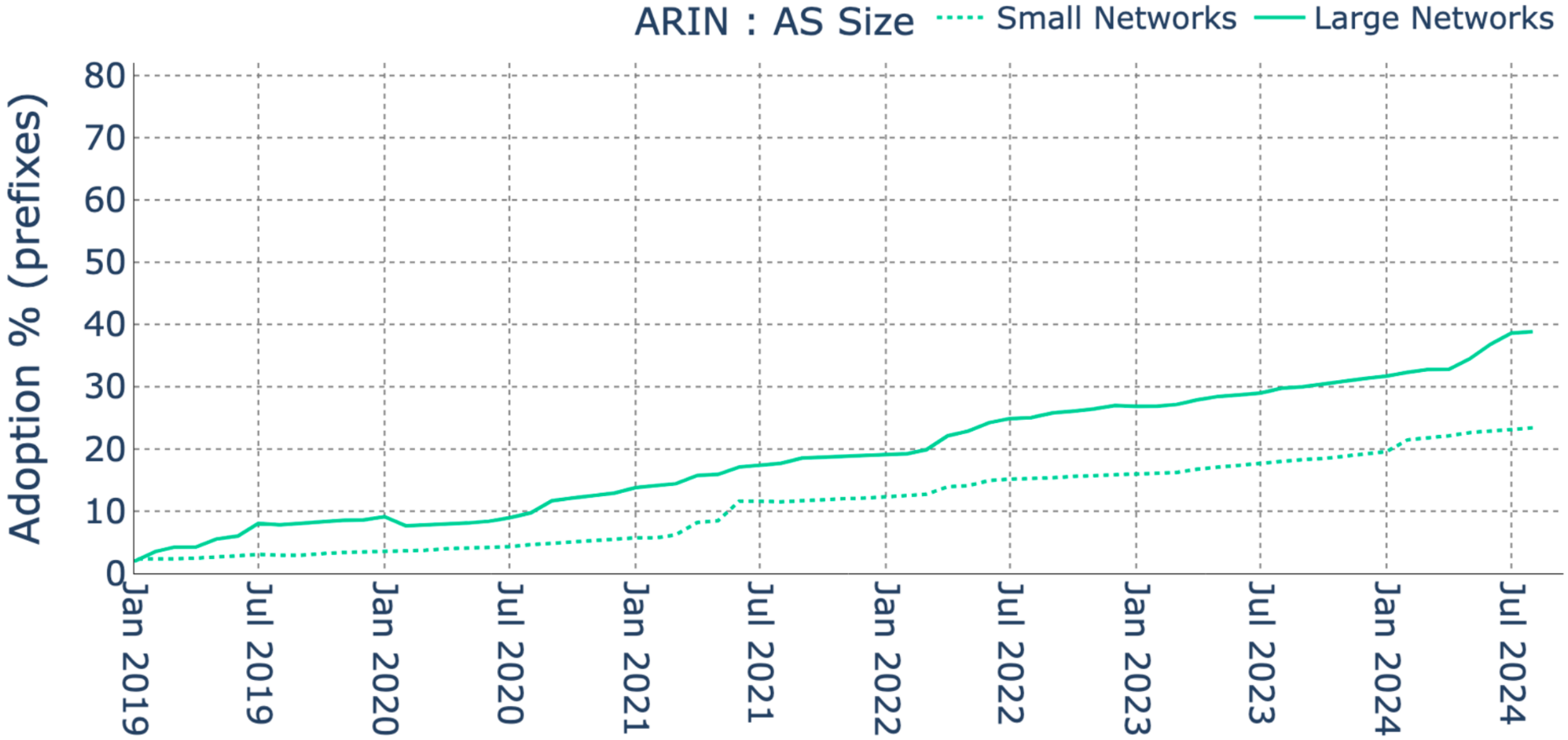
Coverage of countries in January 2024; Middle-east nations have the highest ROA coverage, while China has the lowest coverage among large nations

Possible explanations

- In the RIPE zone, most countries have over 50% RPKI adoption
  - Possibly due to RIPE's **community efforts** to train and promote RPKI adoption & development of tools for RPKI certificate issuance and management
- Middle Eastern countries including Israel, Turkey, Iraq, Iran, Lebanon, Oman, Saudi Arabia exhibit more than 90% RPKI adoption, possibly due to **market concentration** of network operators at a country level
- In the LACNIC zone, most countries have more than 80% RPKI adoption possibly due to proactive initiatives led by LACNIC, including **training and pushing RPKI registration**



Lack of incentives and awareness, as well as the complexity of operationalizing the issuance of RPKI ROAs may deter smaller networks from adoption



Lack of incentives and awareness, as well as the complexity of operationalizing the issuance of RPKI ROAs may deter smaller networks from adoption

RPKI coverage of address space originated by networks (ASNs) from select BGP.Tools and ASdb categories

BGP.Tools labels	RPKI cov.%	ASdb labels	RPKI cov.%
Government	20.3	Gov. and Reg. Agencies[4]	15.5
Academic	23.84	Colleges, Univ., and Prof. Schools	21.99
Mobile Data/Carrier	46.04	Phone Provider	33.34
Server Hosting	51.19	Hosting and Cloud Provider	57.41
Home ISP	45.06	Internet Service Provider (ISP)	44.78
Satellite Internet	85.84	Satellite Comm.	52.05

- Government and academic networks are mostly **small networks** and face the challenges small networks have for RPKI adoption (lack of awareness, training and management tools)
- Networks whose business does not involve Internet services also have **little financial incentive** to adopt RPKI since their users are unlikely to move to a competitor to improve their security stance

Internet Intelligence Lab

THANKS
Comments/Questions?

dainotti@gatech.edu

Cyber Security Framework (CSF) Profile for Internet Routing

Tony Tauber

October 2024

What is the CSF (Cyber Security Framework)?

Started by NIST	Manage and reduce cybersecurity risks	Taxonomy of high-level outcomes for an organization to:
• National Institute for Standards and Technology		• Understand • Assess • Prioritize • Communicate

What is the CSF not?

Not a checklist of things to do.

"The CSF provides a series of outcomes to prioritize and address cybersecurity risks but does not specify actions for meeting those outcomes."

What’s this CSF Profile thing?

Various Industries/Sectors have *taken* the Framework and *developed* a Profile to *apply* in their context.

What’s this CSF Profile for Internet Routing?

For the Internet Routing Operations community

Really? Who?

Some Cable ISPs started

First Public Draft – Jan 2024

Second Public Draft – Sep 2024

Now what?

Needs more and broader input and review!!

The Framework Core

A set of cybersecurity activities, desired outcomes, and applicable references.

It consists of six concurrent and continuous Functions:

- Govern
- Identity
- Protect
- Detect
- Respond
- Recover

Identify: Inventory Hardware

Subcategory	Applicability to Internet Routing
ID.AM-01: Inventories of hardware managed by the organization are maintained	Routing hardware should be inventoried, including BGP routers and computing devices used for RPKI and management functions.

Identify: Inventory Software

Subcategory	Applicability to Internet Routing
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	Routing software elements should be inventoried, including BGP router software, operating systems used by all relevant computing devices, the RPKI validator, and cryptographic packages such as those used for RPKI certificate authority.

Identify: Inventory Suppliers

Subcategory	Applicability to Internet Routing
ID.AM-04: Inventories of services provided by suppliers are maintained	Routing software elements should be inventoried, including BGP router software, operating systems used by all relevant computing devices, the RPKI validator, and cryptographic packages such as those used for RPKI certificate authority.

Identify: Inventory Vendors

Subcategory	Applicability to Internet Routing
ID.AM-04: Inventories of services provided by suppliers are maintained	Examples include MSAs (Master Service Agreements) and/or other contracts with vendors and suppliers… [including] other infrastructure hardware and software, but also services such as registries, monitoring and analysis systems, etc.

Protect: Identity Management

Subcategory	Applicability to Internet Routing
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Identities and credentials for routing devices are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.

Protect: Authentication Mgmt.

Subcategory	Applicability to Internet Routing
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Identities and credentials for external accounts, e.g., RIR accounts, need to be managed with special care due to the potential impact to internet routing from such compromised accounts.

Protect: Access Management

Subcategory	Applicability to Internet Routing
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	Physical access should be managed, monitored and enforced for routing devices, systems which manage routers, credential stores with routing related credentials and any backups.

Respond: Incident Management

Subcategory	Applicability to Internet Routing
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	Incident response plan for routing is executed in coordination with routing stakeholders, e.g., upstream service providers, IP interconnection partners, and customers.

Strengthening a business case for routing security: MANRS+

Is your connectivity provider a threat vector or the first line of defense?

GLOBAL CYBER ALLIANCE™

Why is Routing Security Hard?

Every network has a responsibility to implement basic routing security practices to mitigate threats. Otherwise - they are part of the problem.

But implementing best practices does not bring many immediate benefits. It costs time and money, and you probably can't charge extra for it.

A secure routing system benefits all. But even if you do everything right, your security is still in the hands of other networks.

This is a collective action problem.

A collaborative approach:

Mutually Agreed Norms for Routing Security (MANRS)

An undisputed minimum security baseline – the norm.

- Defined through MANRS Actions

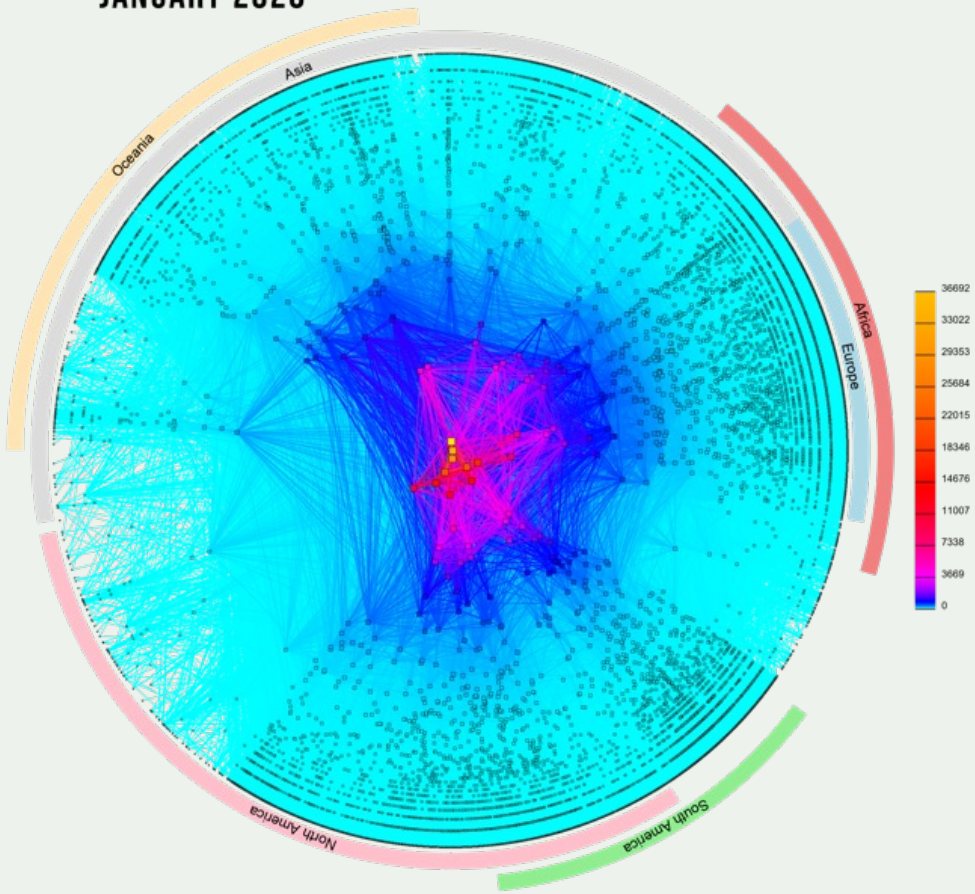
Demonstrated commitment by the participants

- Measured by the Observatory and published on https://www.manrs.org

The MANRS (and routing security) business case

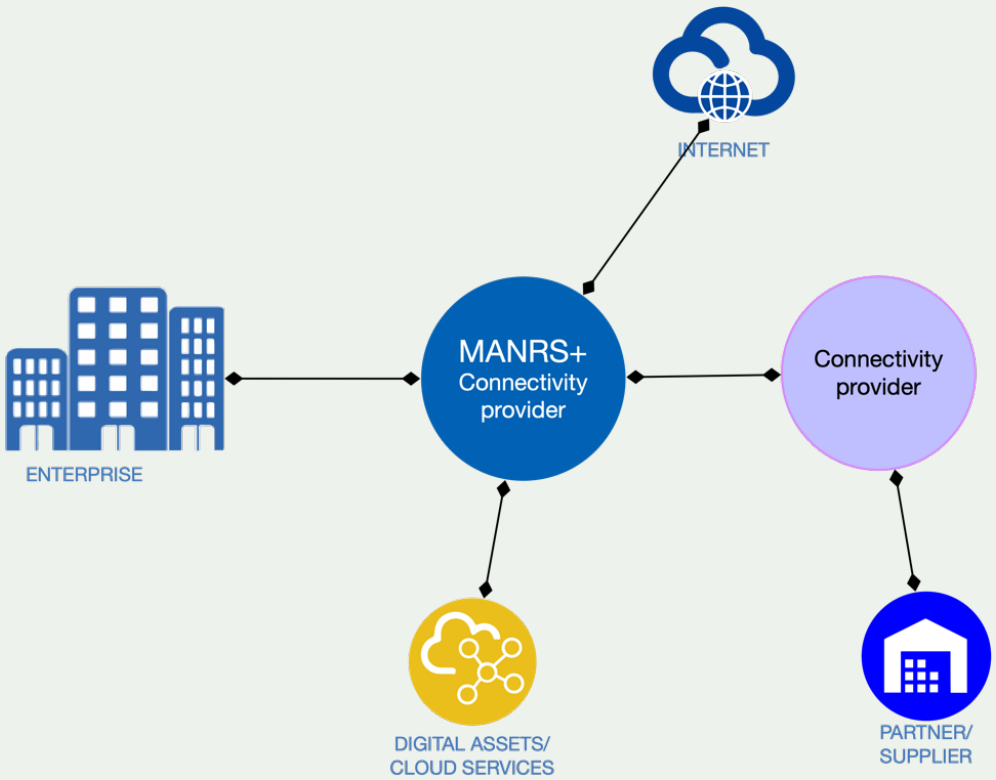
- **Protecting own network** by improving security processes and deploying essential controls
- **Improving security of the global routing system** (overcoming the collective action problem), because
  - routing security is a sum of all contributions
  - this is a way to promote a new baseline
  - a community has gravity to attract others
- **Gaining competitive advantage** by responding to **customer demands?**

CAIDA'S IPV4 AS CORE GRAPH
JANUARY 2020



https://www.caida.org/

Traffic security for enterprises – a smaller Internet

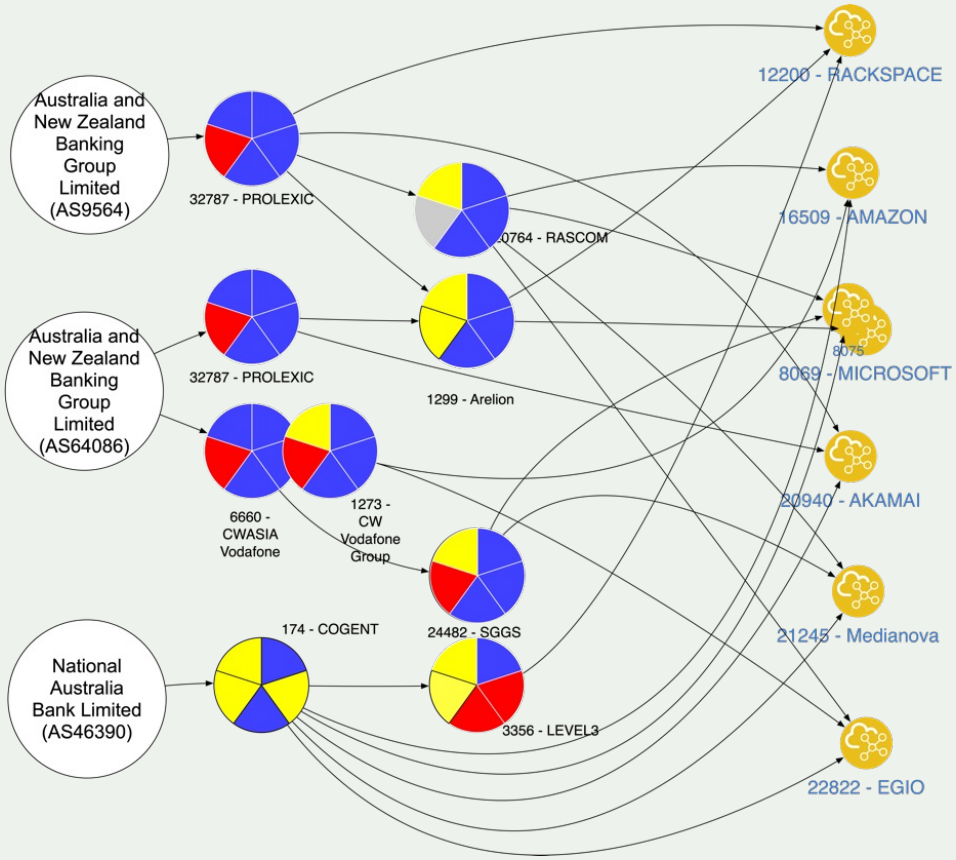


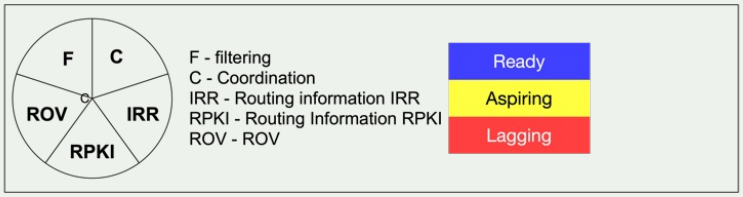
Enterprise's connectivity provider is the first line of defense against routing incidents.

Enterprise can reduce risk by implementing the MANRS actions.

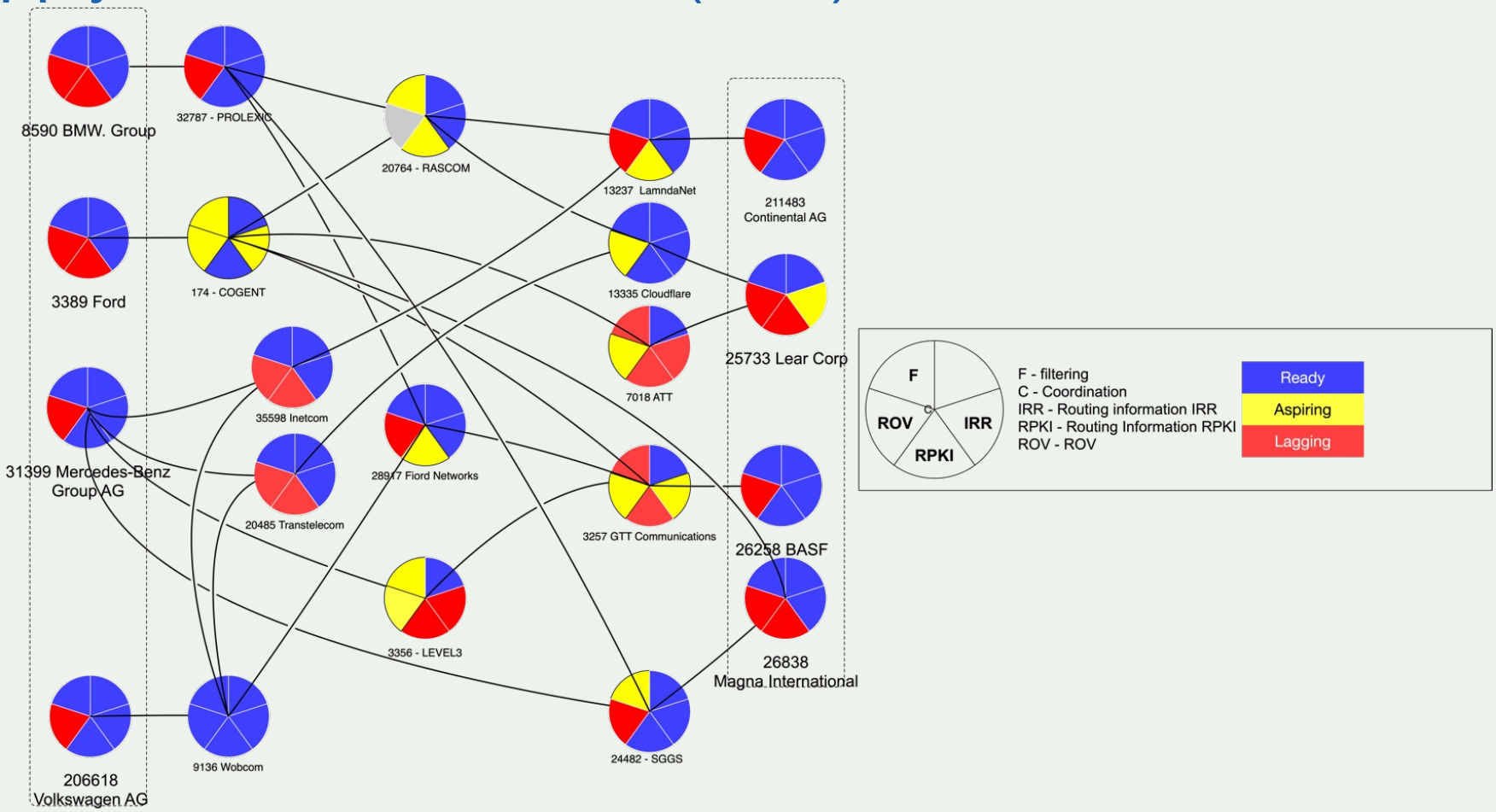
A strong and reliable tie with the connectivity provider(s) can achieve much more – secure the company supply chain.

Supply chain: AU banking





Supply chain: Automotive (B2B)



Routing security as part of supply chain security

85% of all ASes are origin-only networks. They fully depend on their connectivity provider for accessing their external digital assets and the Internet.

However, origin-only networks, mostly “enterprises” can contribute to a better routing security by:

1. Enterprises **implementing** routing security best practices in their network infrastructure.

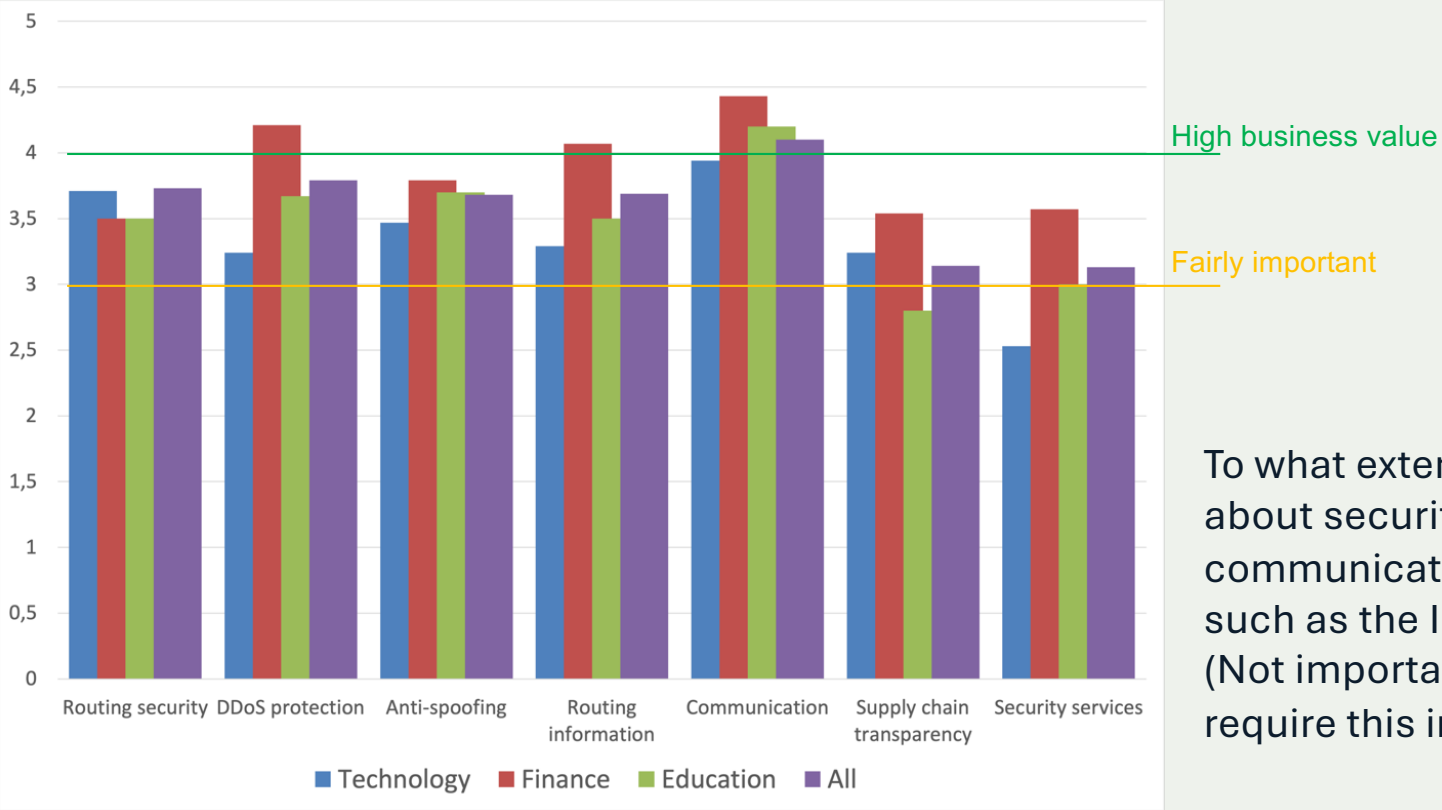
2. Enterprises **demanding** proper routing security controls from their connectivity and cloud providers.

Is your connectivity or cloud provider the first line of defense, or the weakest link?

MANRS+

- A framework for routing security, essential part of supply chain security
- Focus on the demands of enterprise customers in various industry sectors
  - *Extended set of requirements, covering a broader set of risks related to routing and traffic security*
- Conditioned to be included in/referenced from common infosec frameworks
  - *Stronger and more detailed requirements enforcing best practices in traffic security*
  - *High level of assurance of conformance. This includes more profound technical audit and process audit.*
  - *Developed in an transparent and inclusive manner – Standard Development Process*

Does traffic security matter to enterprises?



To what extent enterprise care about security of the global communication infrastructure, such as the Internet? Rating from 1 (Not important) to 5 (Essential, we require this in contracts).

Survey on Traffic security controls, https://www.manrs.org/2023/08/survey-shows-enterprises-value-routing-security-may-underestimate-their-ability-to-influence-vendors/

What should enterprises require from their connectivity provider? MANRS+ Requirements (Controls Matrix)

Routing Security
7 Controls

DDoS Attack Mitigation
4 Controls

Anti-spoofing Protection
2 Controls

Maintaining Routing Information
3 Controls

Global Communication
1 Control

Security Services
3 Controls

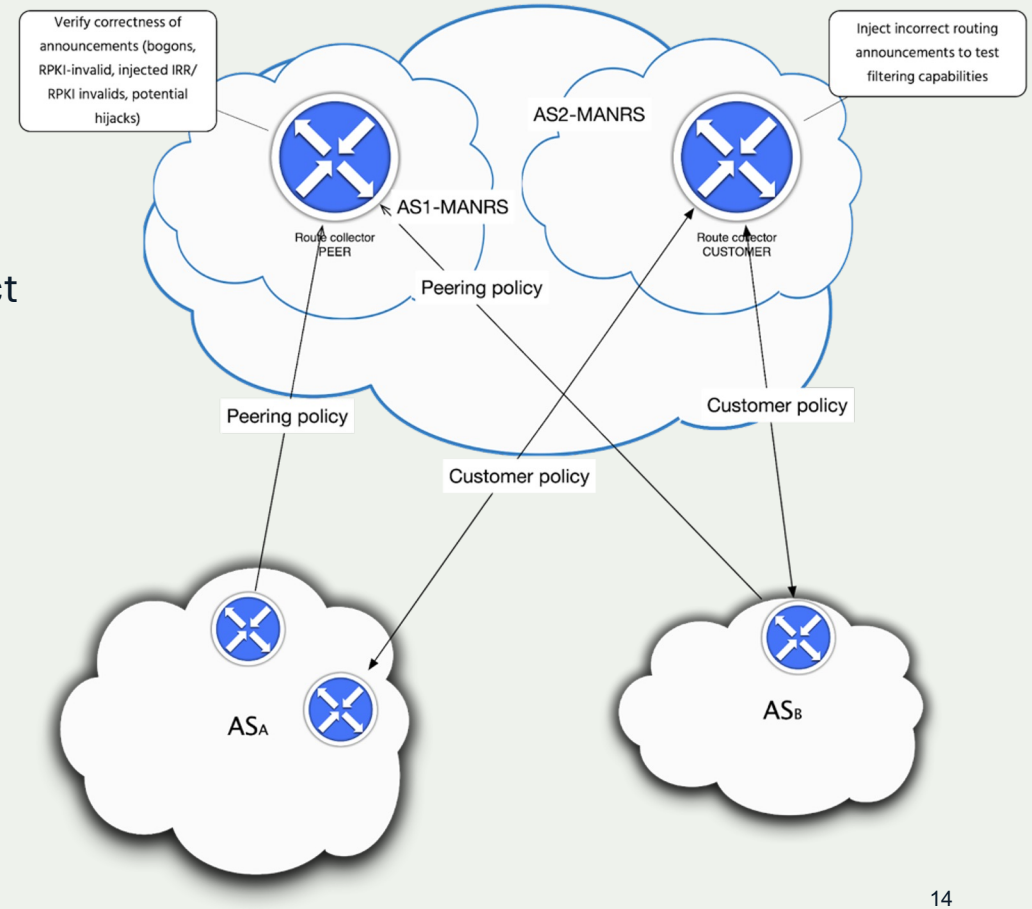
Current status

- Work is done by the MANRS+ WG:
  - https://manrs.org/about/manrs-working-group/
  - The WG meets monthly on Zoom, ongoing discussions are on the mailinglist
  - Anyone can join this effort → contact@manrs.org
  - The final draft of the Controls Matrix is ready

Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines (Auditing levels: Self declared, Measured, Audited)
Routing Security				
Routing Security	RPKI Route Origin Validation	RS-01	Any announcement received from a BGP neighbor or originated by the CP that is invalidated by an existing RPKI ROA is discarded and not announced to other BGP neigbours.	1. Check metrics from the measurement system indicating occurrence of incidents viola the control. Ensure that the metrics are within the defined range. [Measured] 2. Examine the validation workflow 3. Examine documentation which includes information about RPKI processes including RPKI Trust Anchors are used to import ROAs, how often updates to ROAs are imported how often these updates are published to their routers. Ensure that the documented procedures reflect best practices for ROV. [Self-declared][Audited]
Routing Security	IRR Filtering of Direct Customers	RS-02	In cases where RPKI Route Origin Validation cannot be effectively applied (e.g. no matching ROA is found), announcements received from a direct Enterprise customer and its customer cone (if exists) are filtered using a whitelist (allow-list) generated from the IRR or by other means. Exception is the cases where unless the number of aggregated prefixes from a customer exceeds 1000 (discuss).	1. Check metrics from the measurement system indicating occurrence of incidents viola the control. Ensure that the metrics are within the defined range. In case these cases ha on intrafaces that excluded from the requirement, verify that the number of aggregate prefixes exceeds 1000 (discuss)[Measured][Audited] 2. Examine the validation workflow that includes a fallback to prefix-list filtering in case cannot be performed (ROA not found). 3. Examine documentation of the process for configuring new customer connections, w includes description of how the direct customer cone prefix-lists are generated and app how they are validated, and how often these prefix-lists are published to their routers. must include templates or description of the automation process used to generate and the prefix-lists.[Self-declared][Audited]
Routing Security	Control a set of customer ASes (that can originate announcements)	RS-XX	The CP implements filtering permitting only ASNs for a direct customer and its downstream customers (if exists) to originate announcements. The set of permitted ASNs is obtained from an AS-SET in an IRR or by other means.	1. Check metrics from the measurement system indicating occurrence of incidents viola the control. Ensure that the metrics are within the defined range. [Measured][Audited] 2. Examine the validation workflow that includes filtering on origin ASN. 3. Examine documentation of the process for configuring new customer connections, w includes description of how the list of ASNs of the customer and its downstream custo (if exist), how it is validated, and how often this filter is published to their routers. This include templates or description of the automation process used to generate and apply filter.[Self-declared][Audited]

What still needs to be done

- Pilot the extended measurement infrastructure
- Test-run the audit procedures with a select group of operators → contact@manrs.org



Thank you.

contact@manrs.org