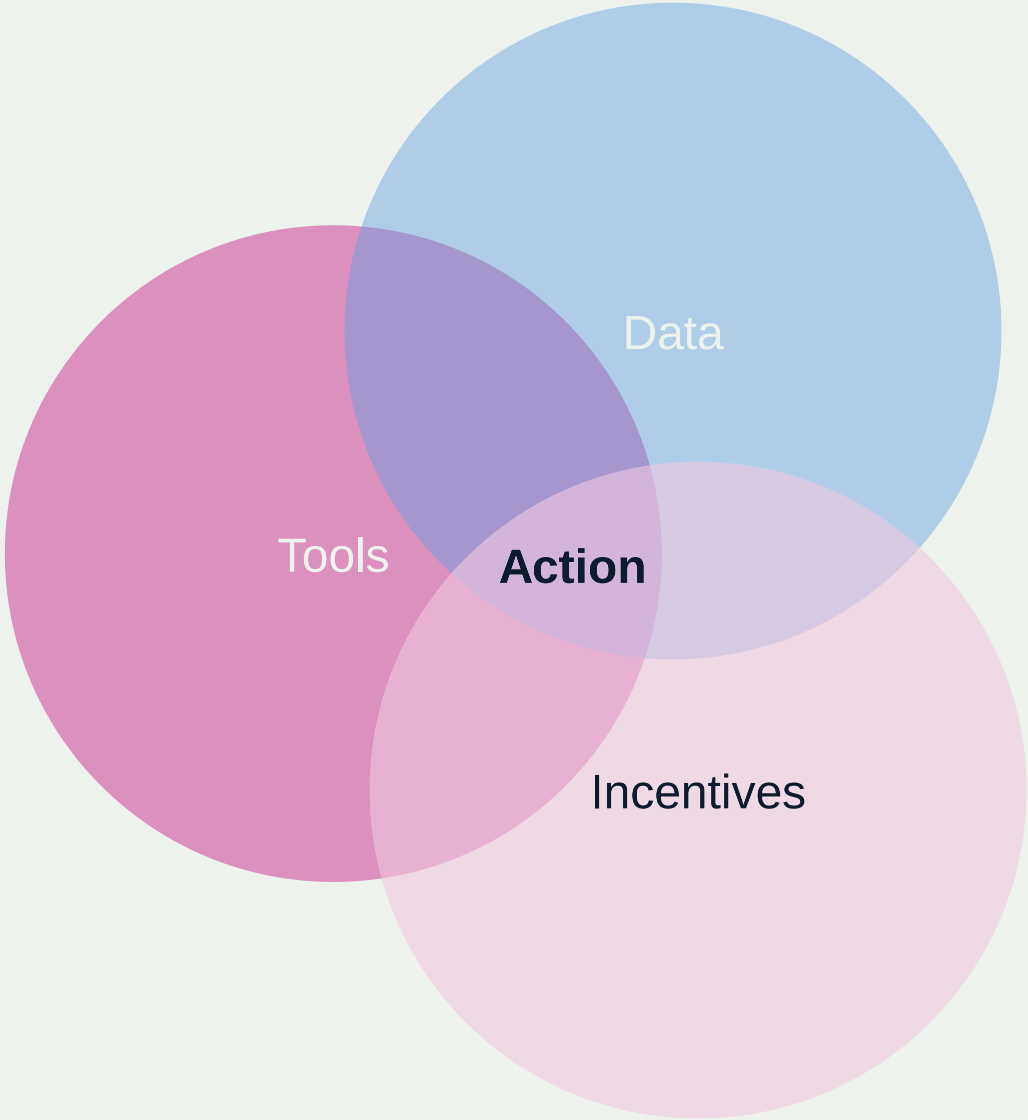
Better routing security through concerted action

2019

manrs@isoc.org

BGP is unsecure – what’s missing?



Mutually Agreed Norms for Routing Security

MANRS provides baseline recommendations in the form of Actions

- Distilled from common behaviors – BCPs, optimized for low cost and low risk of deployment
- With high potential of becoming norms

MANRS builds a visible community of security minded operators

- Social acceptance and peer pressure

MANRS

Network operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

IXPs

Action 1

Prevent propagation of incorrect routing information

This mandatory action requires IXPs to implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).

Action 2

Promote MANRS to the IXP membership

IXPs joining MANRS are expected to provide encouragement or assistance for their members to implement MANRS actions.

Action 3

Protect the peering platform

This action requires that the IXP has a published policy of traffic not allowed on the peering fabric and performs filtering of such traffic.

Action 4

Facilitate global operational communication and coordination

The IXP facilitates communication among members by providing necessary mailing lists and member directories.

Action 5

Provide monitoring and debugging tools to the members.

The IXP provides a looking glass for its members.

Content (work in progress)

Action 1

Prevent propagation of incorrect routing information

Action 2

Prevent traffic with spoofed source IP addresses

Action 3

Facilitate global operational communication and coordination

Action 4

Facilitate validation of routing information on a global scale

Action 5

Promote MANRS

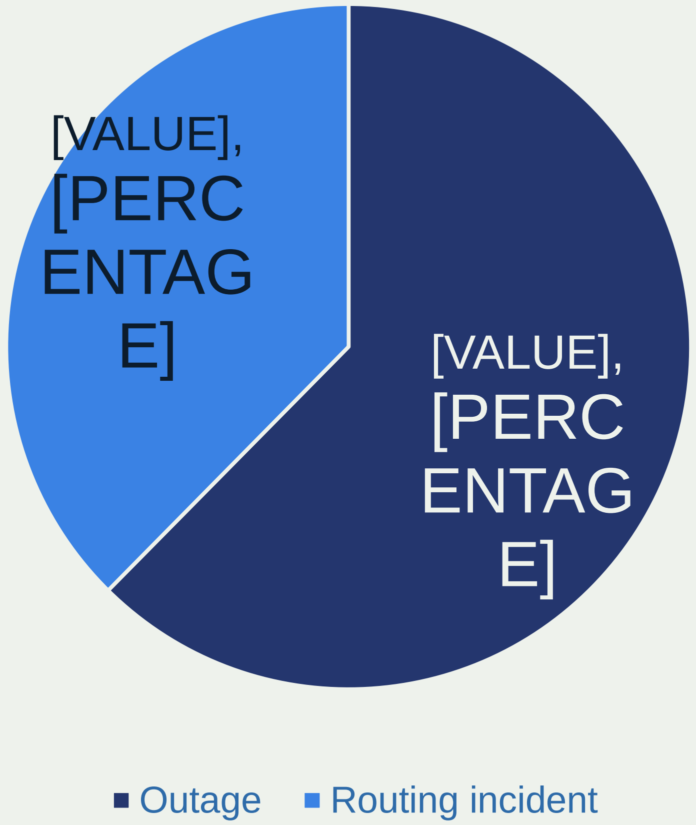
Action 6

Provide monitoring and debugging tools to peering partners

There is a problem

- 12,600 total incidents (either outages or attacks, like route leaks and hijacks)
- About 4.4% of all Autonomous Systems on the Internet were affected
- 2,737 Autonomous Systems were a victim of at least one routing incident
- 1,294 networks were responsible for 4739 routing incidents

Twelve months of routing incidents (2018)



Source: https://www.bgpstream.com/

There is a problem (comp. 2017)

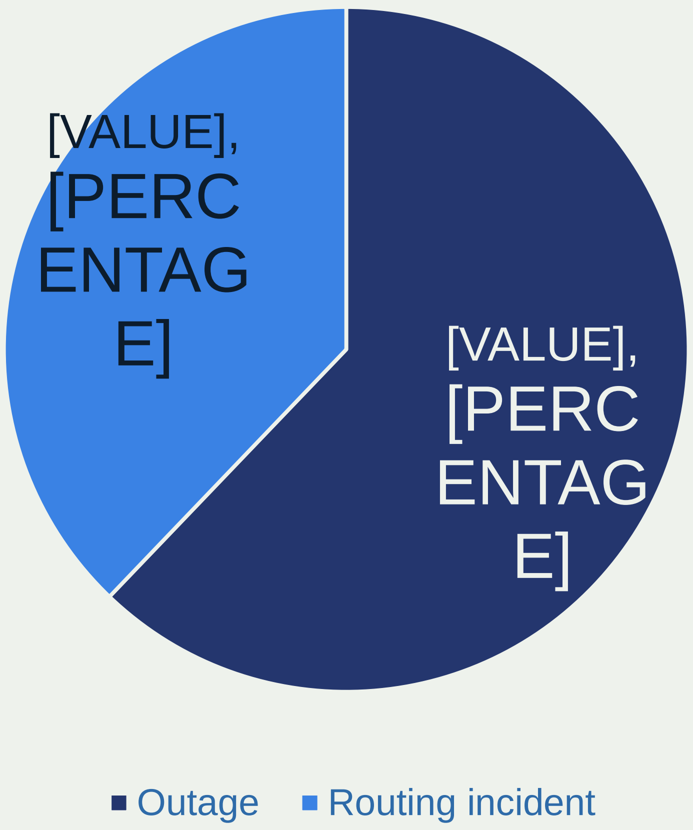
- 12,600 (↓9.6%) total incidents (either outages or attacks, like route leaks and hijacks)

- About 4.4% (↓1%) of all Autonomous Systems on the Internet were affected

- 2,737 (↓12%) Autonomous Systems were a victim of at least one routing incident

- 1,294 (↓17%) networks were responsible for 4739 routing incidents

Routing incidents (2017-2018)



Source: https://www.bgpstream.com/

2 years in review (2017, 2018)

Statistics of routing incidents generated from BGPStream data

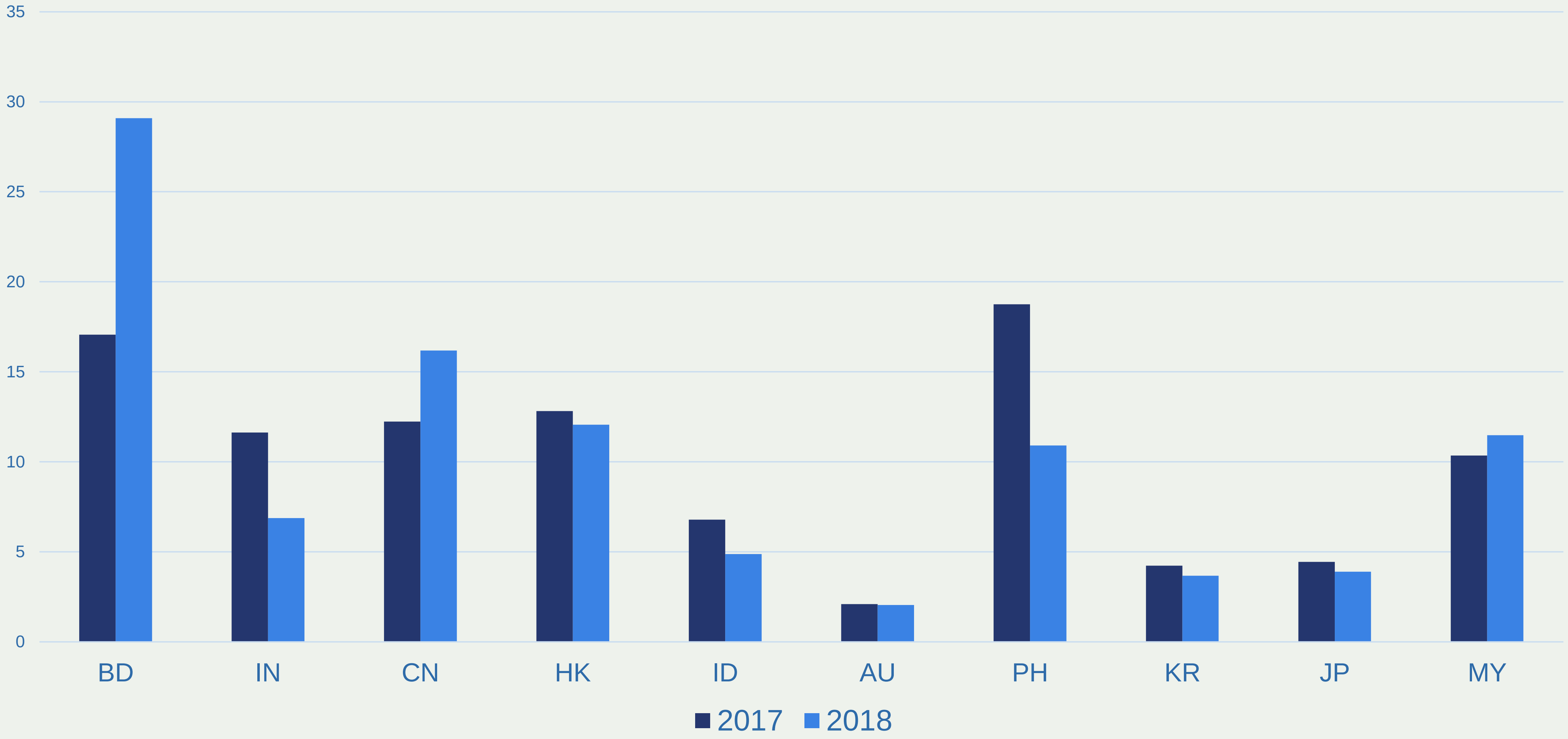
Caveats:

- Sometimes it is impossible to distinguish an attack from a legitimate (or consented) routing change
- CC attribution is based on geolocation MaxMind's GeoLite City data set

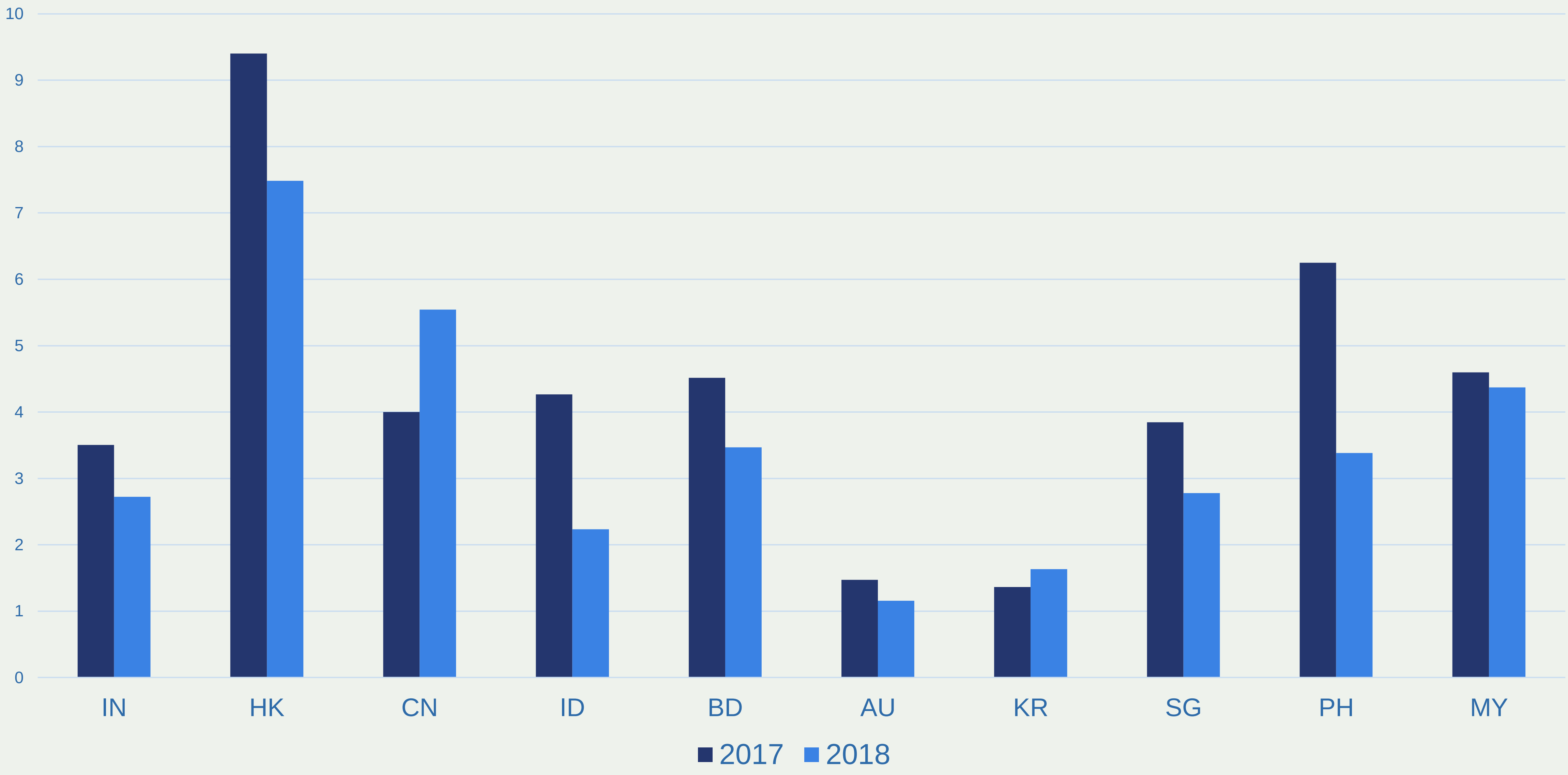
But:

- Using the same methodology we should get a pretty accurate picture of the dynamics

Potential victims: 2017 → 2018



Culprits: Positive dynamics

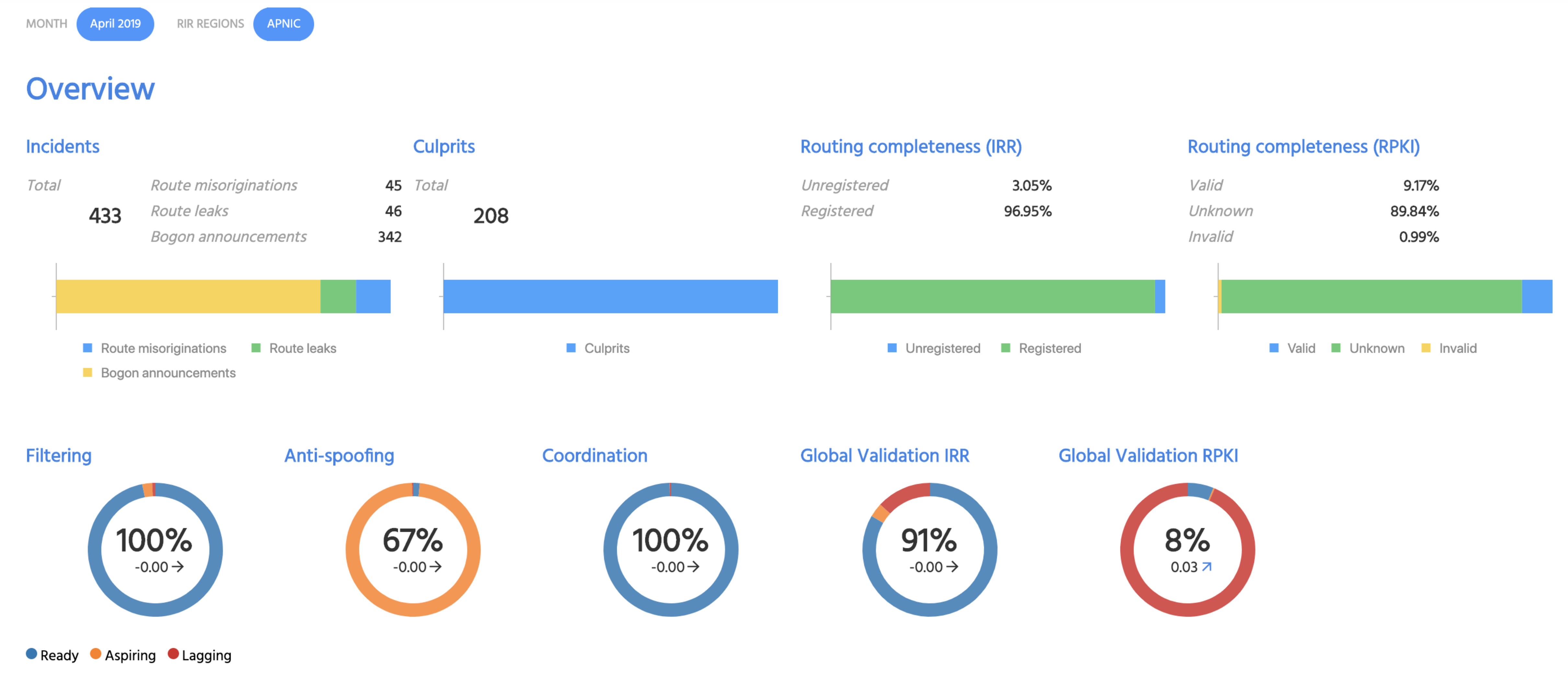


Can we track these data long term?

MANRS Observatory & Member Reports

- Longitudinal measurements of how routing security evolves
- MANRS as a reference point - ”MANRS Readiness”
- Inform the members of their readiness
- Improve transparency and credibility of the effort

State of routing security: APNIC region, April 2019



MONTH: April 2019 RIR REGIONS: APNIC

Overview

Incidents

Total		
433	*Route misoriginations*	45
	Route leaks	46
	Bogon announcements	342

Culprits

Total

208

Routing completeness (IRR)

Unregistered	3.05%
Registered	96.95%

Routing completeness (RPKI)

Valid	9.17%
Unknown	89.84%
Invalid	0.99%

Filtering

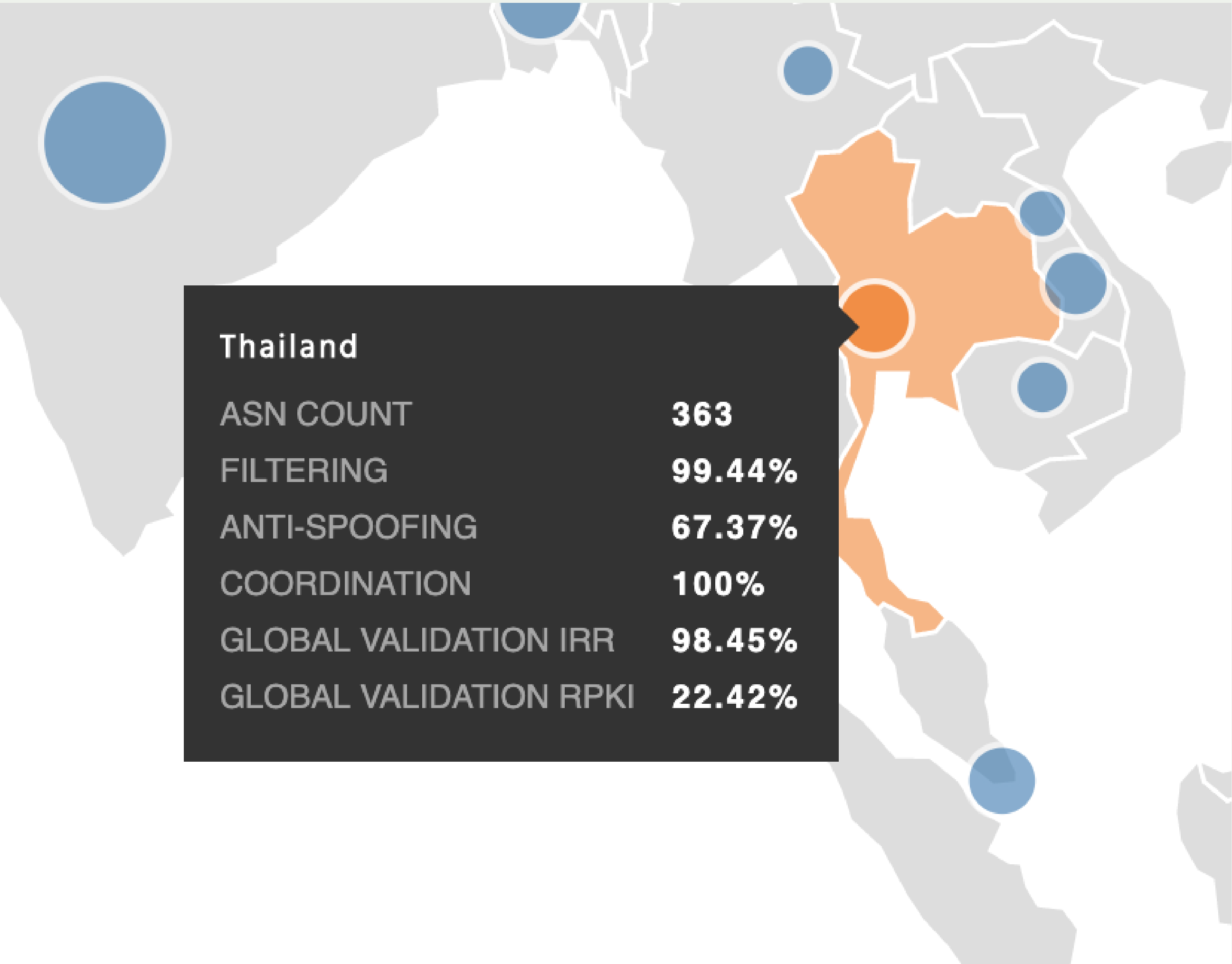
Anti-spoofing

Coordination

Global Validation IRR

Global Validation RPKI

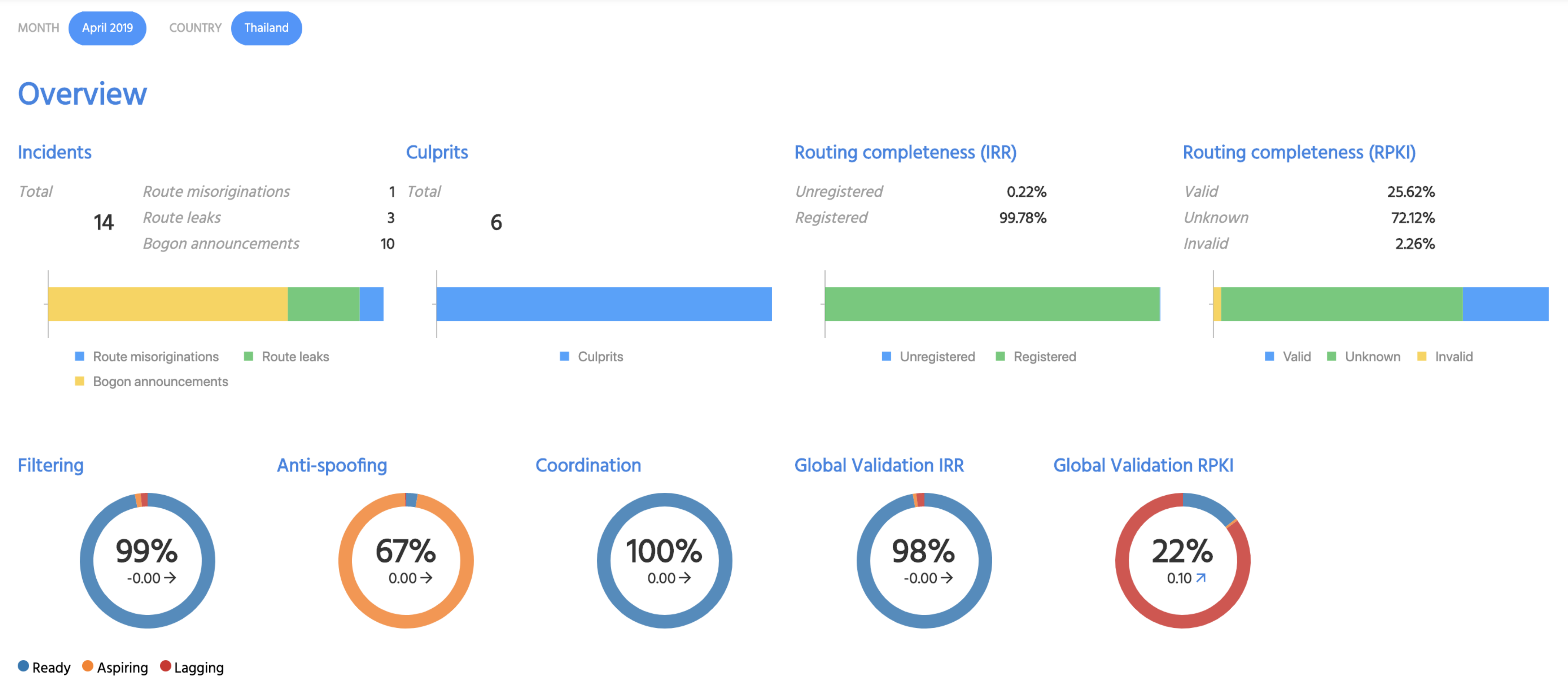
State of routing security: Thailand, April 2019



Thailand

ASN COUNT	363
FILTERING	99.44%
ANTI-SPOOFING	67.37%
COORDINATION	100%
GLOBAL VALIDATION IRR	98.45%
GLOBAL VALIDATION RPKI	22.42%

State of routing security: Thailand, April 2019



MONTH April 2019 COUNTRY Thailand

Overview

Incidents

Total		
14	*Route misoriginations*	1
	Route leaks	3
	Bogon announcements	10

Culprits

Total

6

Routing completeness (IRR)

Unregistered	0.22%
Registered	99.78%

Routing completeness (RPKI)

Valid	25.62%
Unknown	72.12%
Invalid	2.26%

Filtering

99%
-0.00 →

Anti-spoofing

67%
0.00 →

Coordination

100%
0.00 →

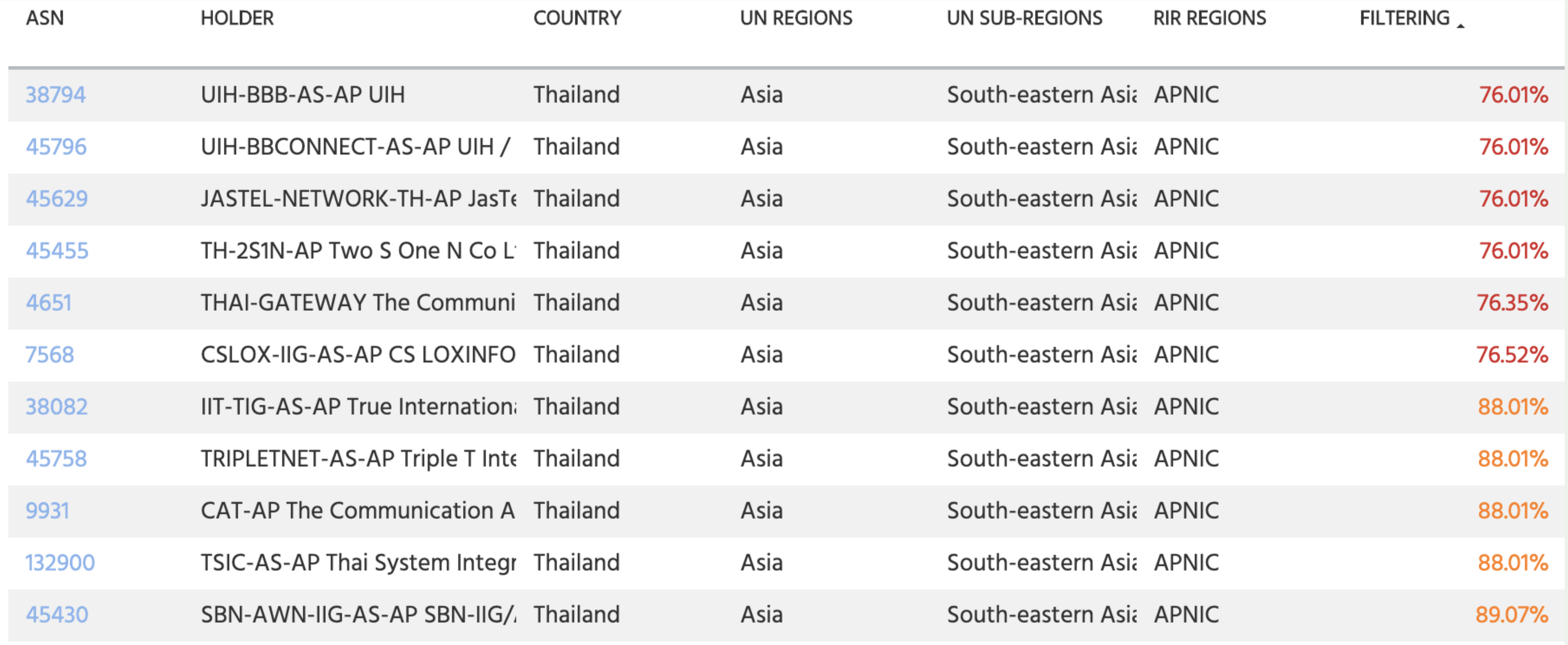
Global Validation IRR

98%
-0.00 →

Global Validation RPKI

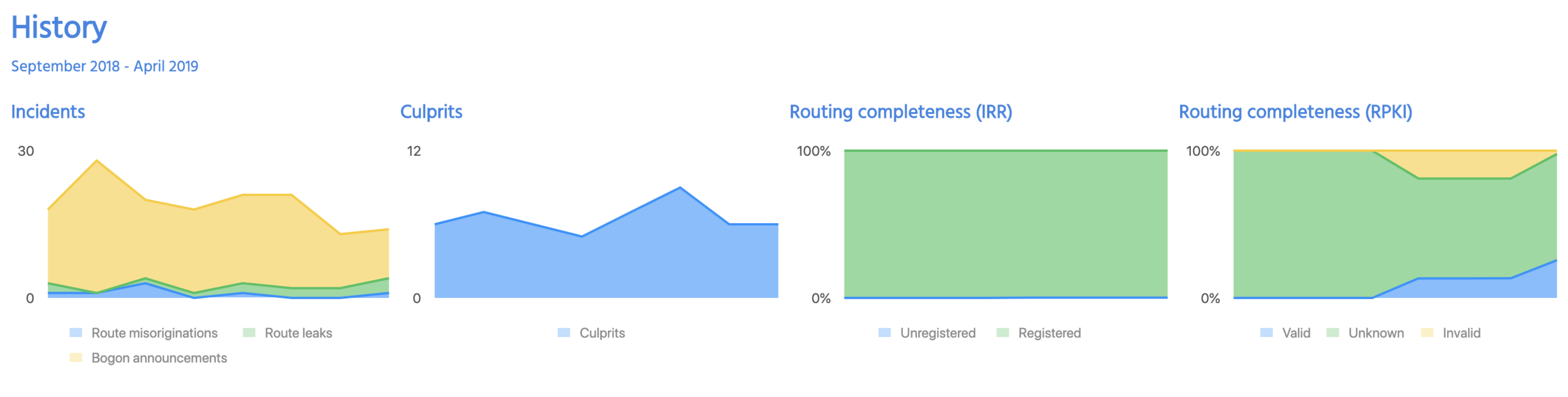
22%
0.10 ↗

State of routing security: Thailand, April 2019



ASN	HOLDER	COUNTRY	UN REGIONS	UN SUB-REGIONS	RIR REGIONS	FILTERING ▴
38794	UIH-BBB-AS-AP UIH	Thailand	Asia	South-eastern Asi	APNIC	76.01%
45796	UIH-BBCONNECT-AS-AP UIH /	Thailand	Asia	South-eastern Asi	APNIC	76.01%
45629	JASTEL-NETWORK-TH-AP JasTe	Thailand	Asia	South-eastern Asi	APNIC	76.01%
45455	TH-2S1N-AP Two S One N Co L	Thailand	Asia	South-eastern Asi	APNIC	76.01%
4651	THAI-GATEWAY The Communi	Thailand	Asia	South-eastern Asi	APNIC	76.35%
7568	CSLOX-IIG-AS-AP CS LOXINFO	Thailand	Asia	South-eastern Asi	APNIC	76.52%
38082	IIT-TIG-AS-AP True Internation	Thailand	Asia	South-eastern Asi	APNIC	88.01%
45758	TRIPLETNET-AS-AP Triple T Inte	Thailand	Asia	South-eastern Asi	APNIC	88.01%
9931	CAT-AP The Communication A	Thailand	Asia	South-eastern Asi	APNIC	88.01%
132900	TSIC-AS-AP Thai System Integr	Thailand	Asia	South-eastern Asi	APNIC	88.01%
45430	SBN-AWN-IIG-AS-AP SBN-IIG/	Thailand	Asia	South-eastern Asi	APNIC	89.07%

Evolution: September 2018 - April 2019



History

September 2018 - April 2019

Incidents

Culprits

Routing completeness (IRR)

Routing completeness (RPKI)

Network Operators from Thailand

Organization	Service Area	ASNs	Action 1: Filtering	Action 2: Anti Spoofing	Action 3: Coordinati on	Action 4: Global Validation
United Information Highway	TH	45796	✔□		✔□	✔□

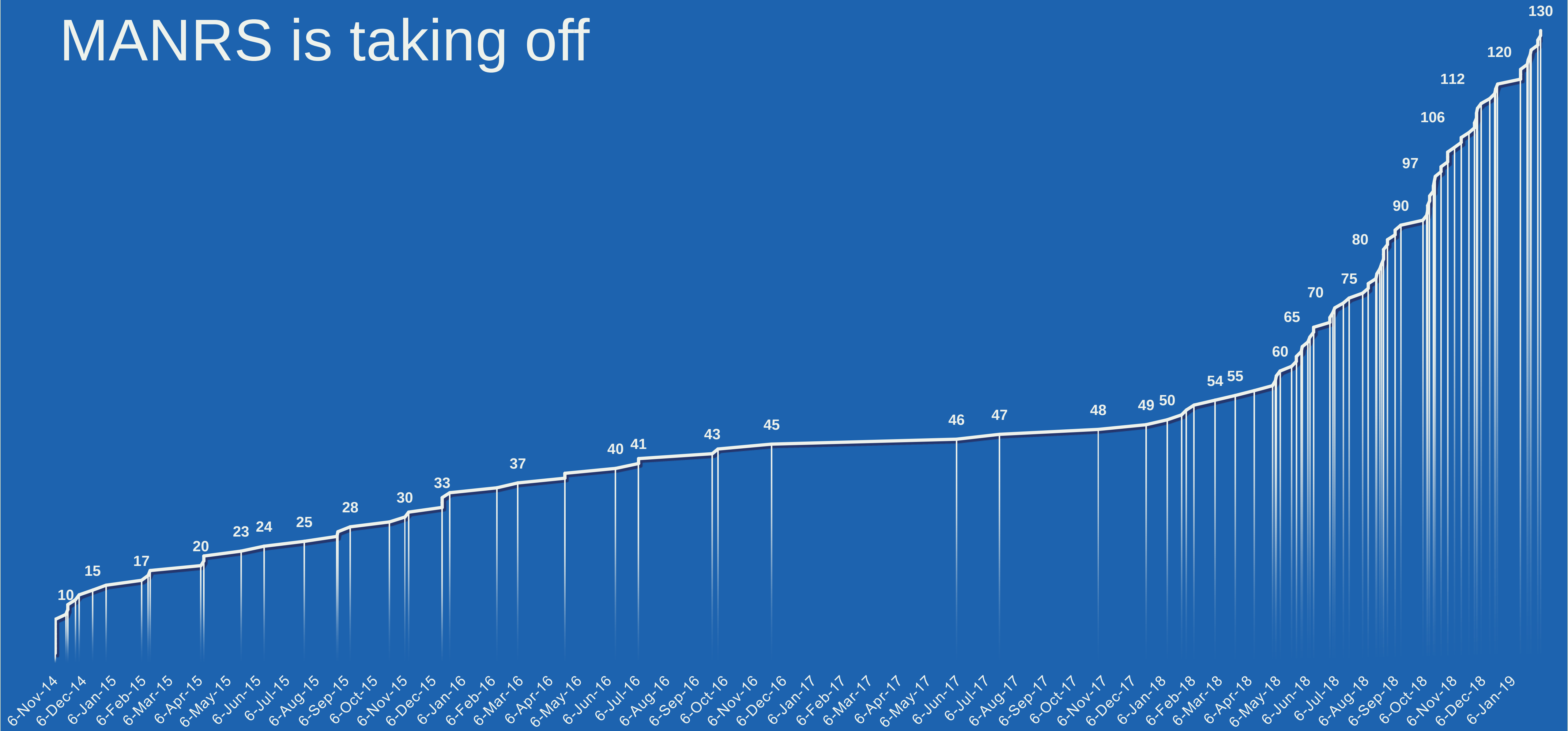
Internet Exchange Points from Thailand

Organization	Service Area	Action 1: Prevent	Action 2: Promote	Action 3: Protect	Action 4: Coordinate	Action5: Tools
BKNIX	TH	✔□	✔□	✔□	✔□	✔□

Why join MANRS?

- Improve your security posture and reduce the number and impact of routing incidents
- Demonstrate that these practices are reality
- Join a community of security-minded operators working together to make the Internet better
- Use MANRS as a competitive differentiator

MANRS is taking off



only together

manrs.org

#ProtectTheCore

MANRS Video:

https://www.youtube.com/embed/nJINk5p-HEE