29 May 2019
CSNOG 2

MANRS: Mutually Agreed Norms for Routing Security

Routing is at Risk

Let’s secure it together!

Kevin Meynell
Manager, Technical & Operational Engagement
meynell@isoc.org

Internet Society © 1992–2019

Background

There are 64,420 networks (Autonomous Systems) connected to Internet, each using a unique Autonomous System Number (ASN) to identify itself

~10,000 multi-homed ASes – networks connected to >=2 other networks

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path

The Routing Problem

Border Gateway Protocol (BGP) is based entirely on *trust* between networks

- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

The routing system is under attack!

MANRS

How big is the problem?

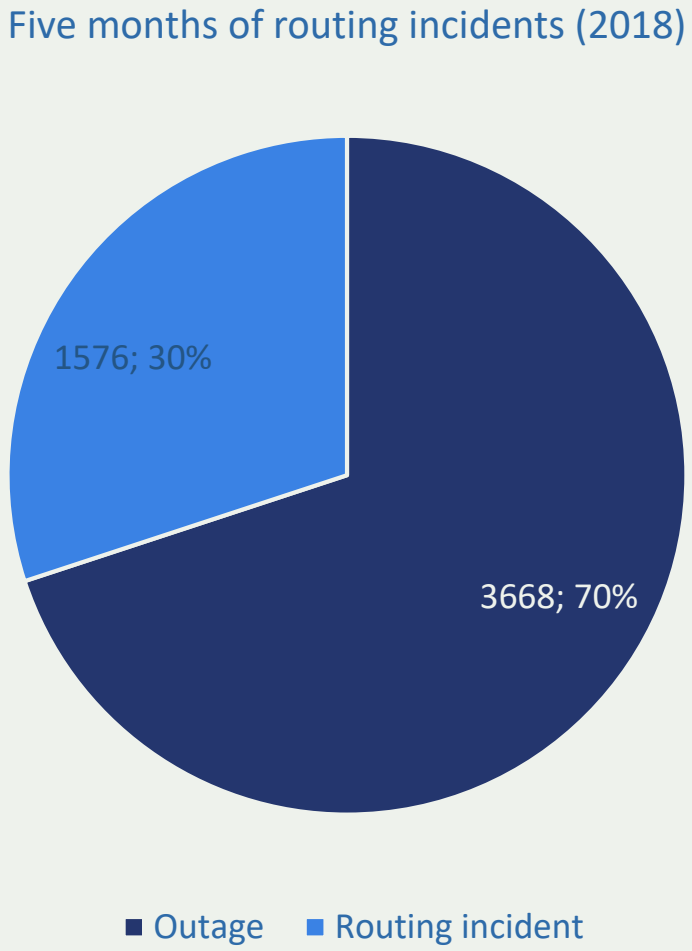
Some Facts & Figures

Routing Incidents Cause Real World Problems

Event	Explanation	Repercussions	Example
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	*The 2008 YouTube hijack* *April 2018 Amazon Route 53 hijack*
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for a MITM, including traffic inspection, modification and reconnaissance.	*September 2014. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria.*
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	*March 1, 2018. Memcached 1.3Tb/s reflection-amplificationattack reported by Akamai*

The routing system is constantly under attack

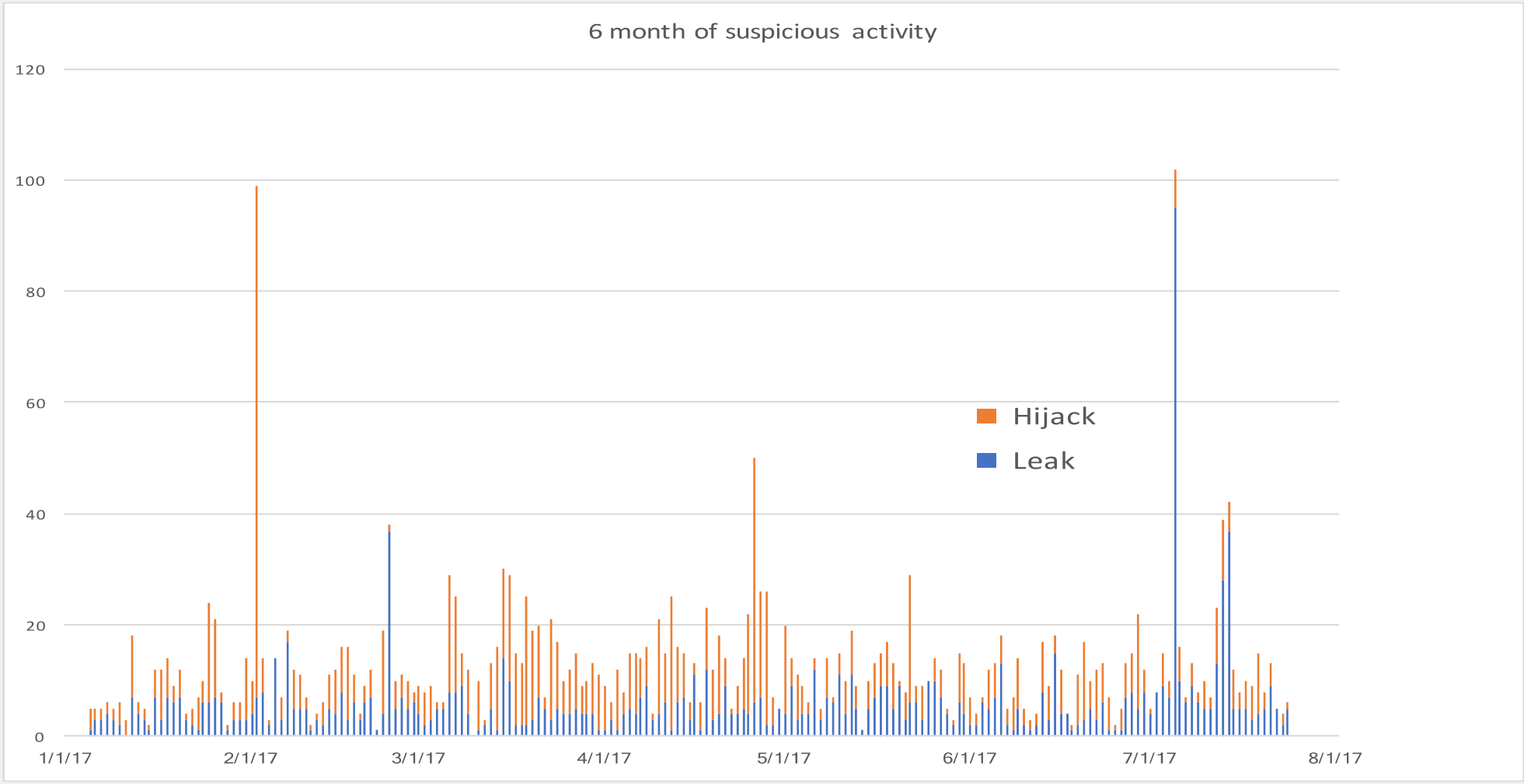
- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- **1,546 networks were responsible for 5304 routing incidents**
- **547 networks were responsible for 1576 routing incidents**



MANRS

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

No Day Without an Incident



http://bgpstream.com/

MANRS

Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to eliminate the most common threats in the global routing system

Brings together established industry best practices

Based on collaboration among participants and shared responsibility for the Internet infrastructure

MANRS Actions

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

Everyone benefits from improved Routing Security

Joining MANRS means joining a community of security-minded network operators committed to making the global routing infrastructure more robust and secure.

Heads off routing incidents, helping networks readily identify and address problems with customers or peers.

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

MANRS Participants – as of May 2019

155 Network Operators

279 Autonomous Systems (ASes)

32 Internet Exchange Points

10 partners (promotion, capacity building etc..)

MANRS Participants in Czechia

714 ASNs assigned to Czechia

1 ASN participating in MANRS (0.14%)

VSHosting s.r.o (AS43541) - 4 actions

Many Czech ASNs are already MANRS conformant though!

How to Implement MANRS

Documentation, Training & Tools

MANRS Implementation Guide

If you're not ready to join yet, implementation guidance is available to help you.

- Based on Best Current Operational Practices deployed by network operators around the world
- Recognition from the RIPE community by being published as RIPE-706
- https://www.manrs.org/bcop/

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

MANRS

Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS Observatory

Tool to impartially benchmark ASes to improve reputation and transparency

Provide factual state of security and resilience of Internet routing system over time

Allow MANRS participants to easily check for conformancy

Collates publicly available data sources

- BGPStream
- CIDR Report
- CAIDA Spoofer Database
- RIPE Database / Whois
- PeeringDB
- IRRs

MANRS Observatory

LOGOUT

OVERVIEW | HISTORY | DETAILS | COMPARISON | ABOUT

MONTH April 2019

Overview

State of Routing Security

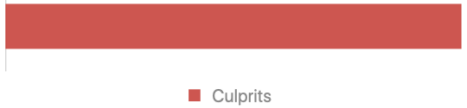
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
2'002	*Route misoriginations*	280
	Route leaks	305
	Bogon announcements	1'417

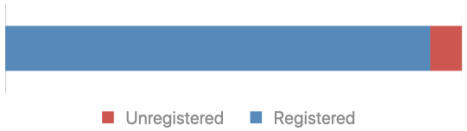
Culprits

Total		
941	*Culprits*	941



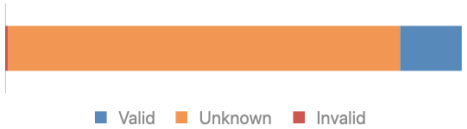
Routing completeness (IRR)

Total		
100%	*Unregistered*	7%
	Registered	93%



Routing completeness (RPKI)

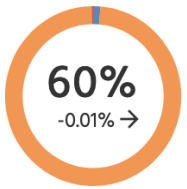
Total		
100%	*Valid*	14%
	Unknown	86%
	Invalid	1%



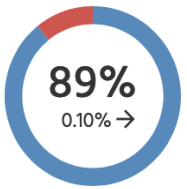
MANRS Readiness

Filtering

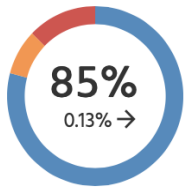
Anti-spoofing



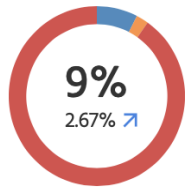
Coordination



Global Validation IRR



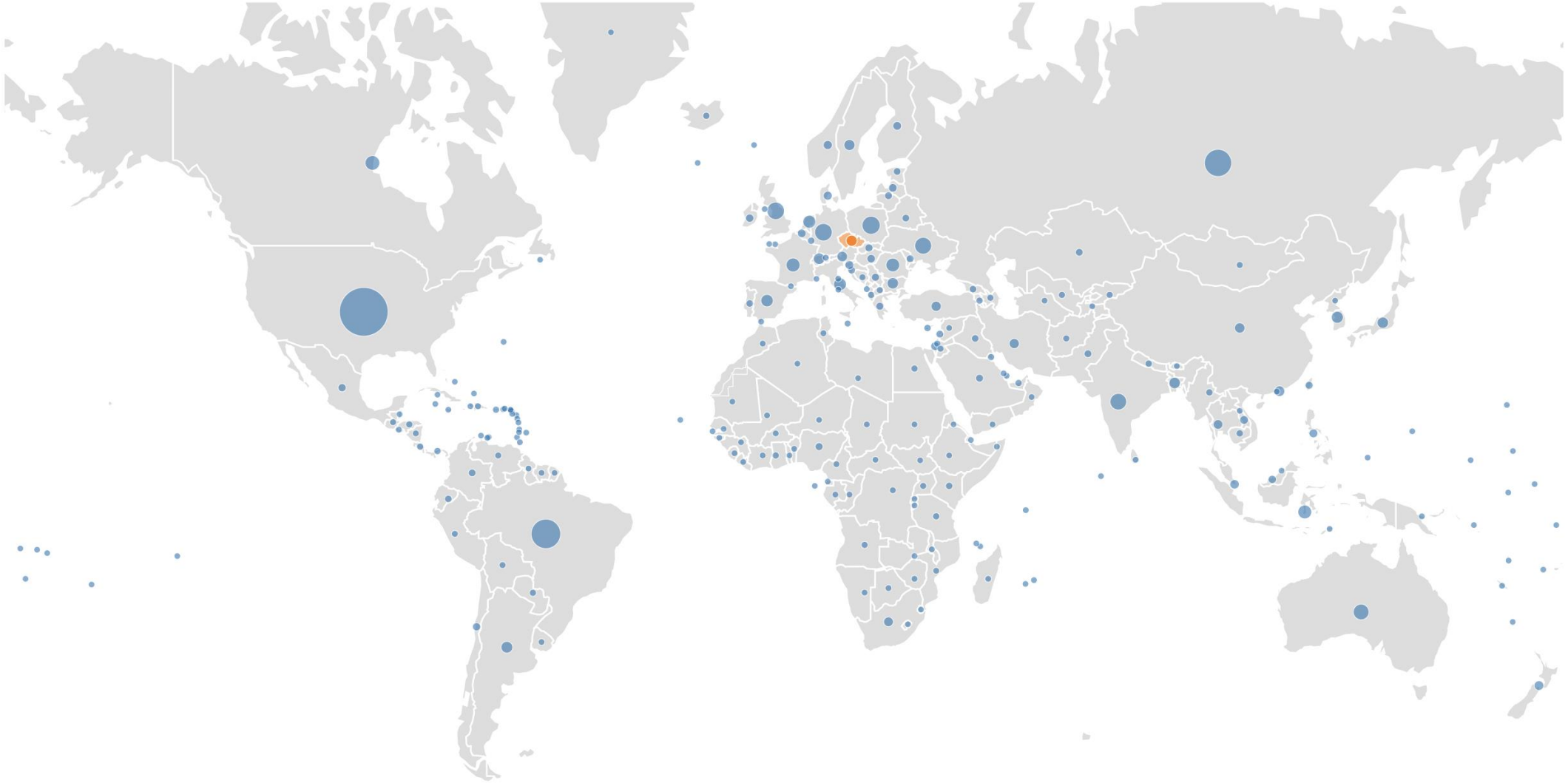
Global Validation RPKI



Ready Aspiring Lagging

Global view

Size: **Count** | Incidents | Culprits Region: **Country** | UN Regions | UN Sub-Regions | RIR Regions



MANRS Observatory

LOGOUT

OVERVIEW | HISTORY | DETAILS | COMPARISON | ABOUT

MONTH April 2019 COUNTRY Czechia

Overview

State of Routing Security

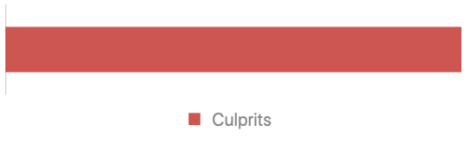
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
6	Route misoriginations	0
	Route leaks	1
	Bogon announcements	5

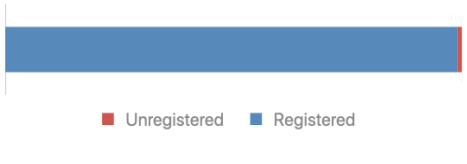
Culprits

Total		
2	Culprits	2



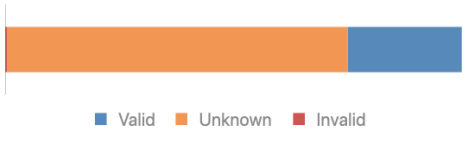
Routing completeness (IRR)

Total		
100%	Unregistered	1%
	Registered	99%



Routing completeness (RPKI)

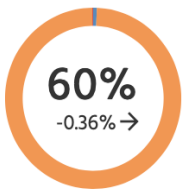
Total		
100%	Valid	25%
	Unknown	75%
	Invalid	0%



MANRS Readiness

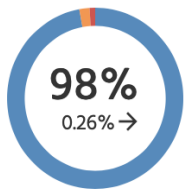
Filtering

Anti-spoofing

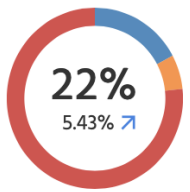


Coordination

Global Validation IRR



Global Validation RPKI

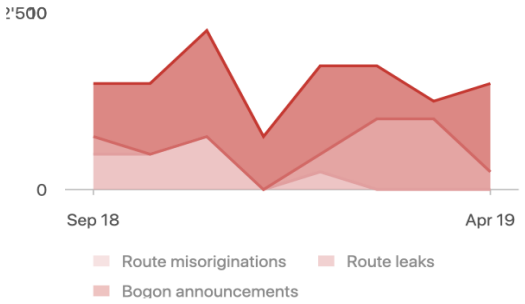


Ready Aspiring Lagging

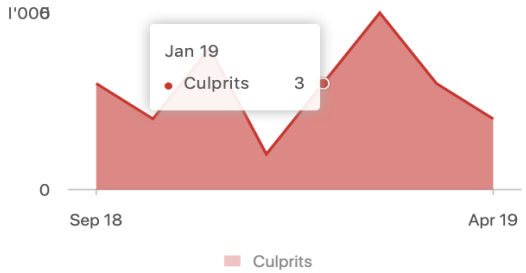
History

September 2018 - April 2019

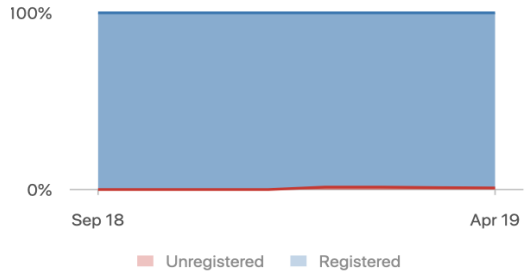
Incidents



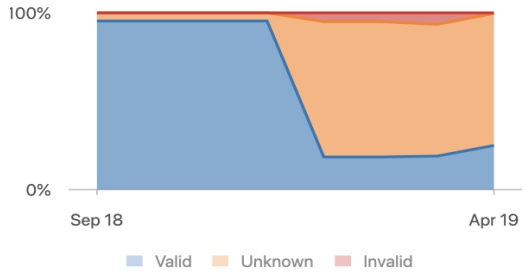
Culprits



Routing completeness (IRR)



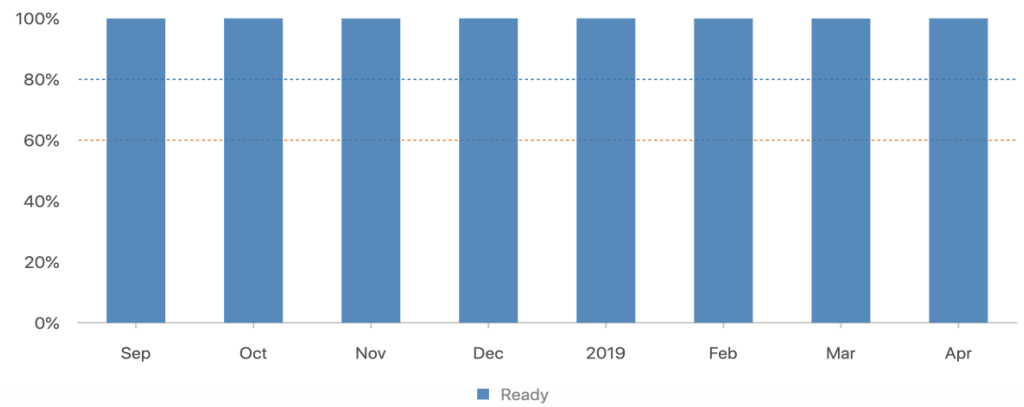
Routing completeness (RPKI)



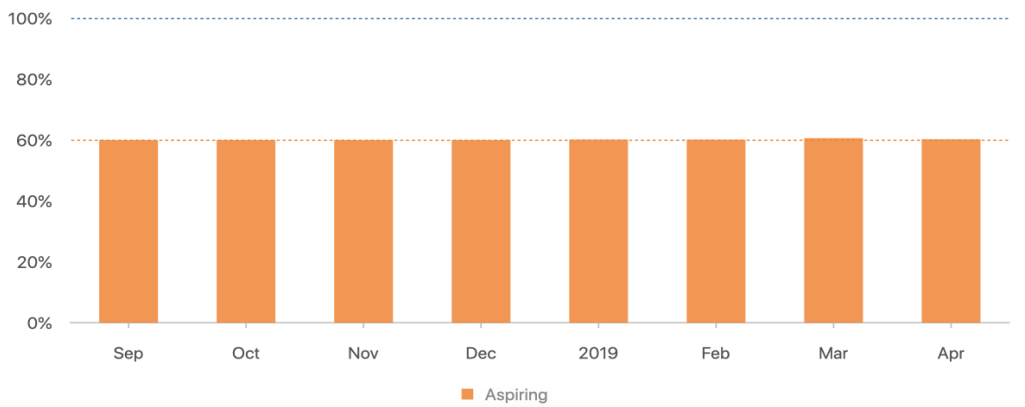
MANRS Readiness

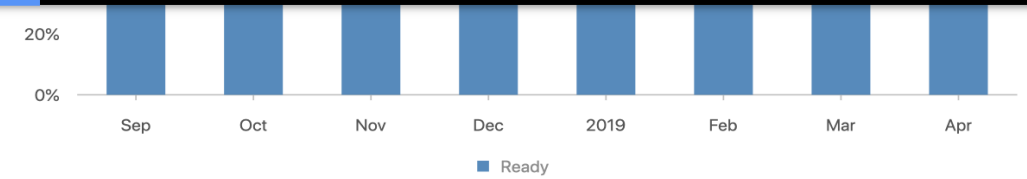
Overall | Metrics

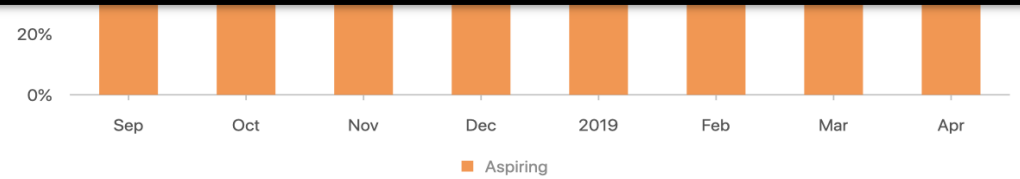
Filtering



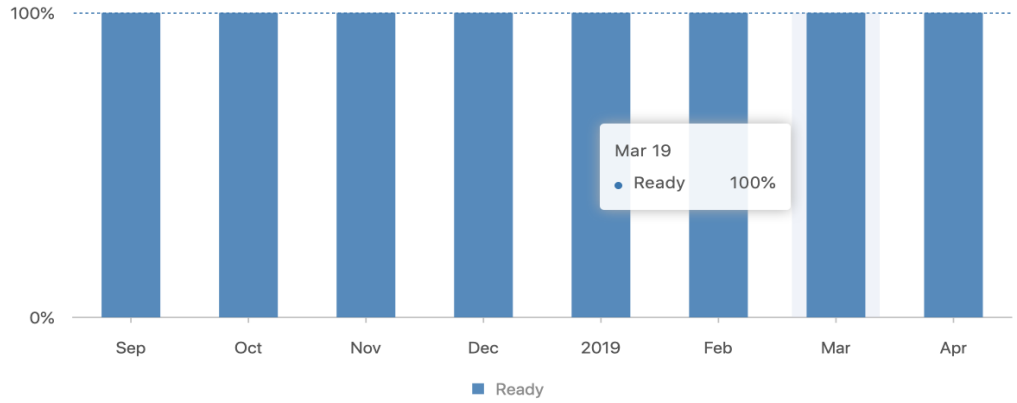
Anti-spoofing



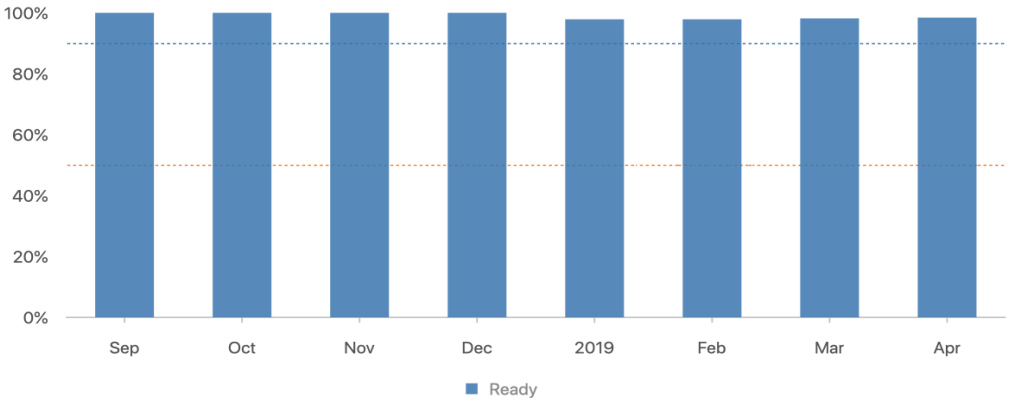




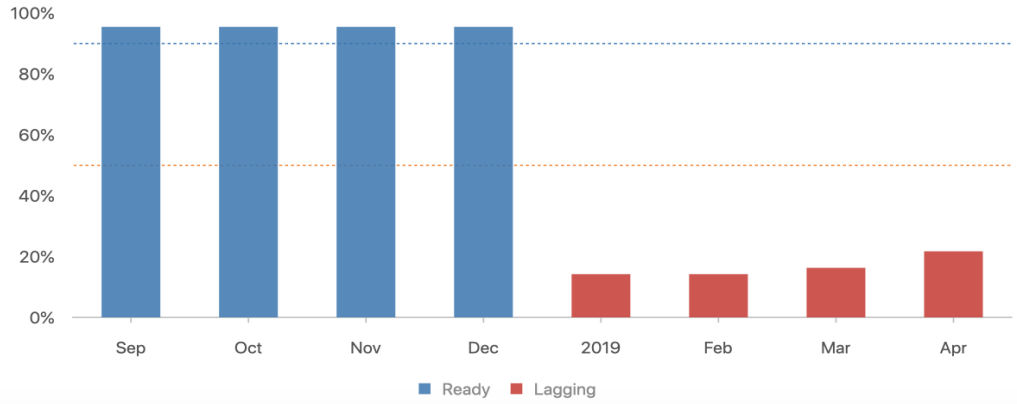
Coordination



Global Validation IRR



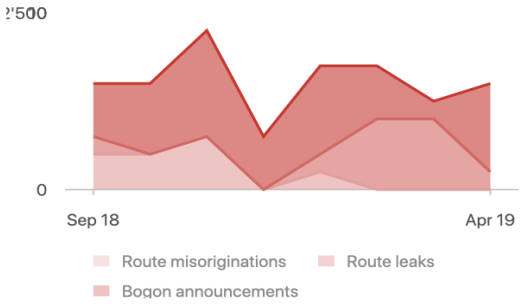
Global Validation RPKI



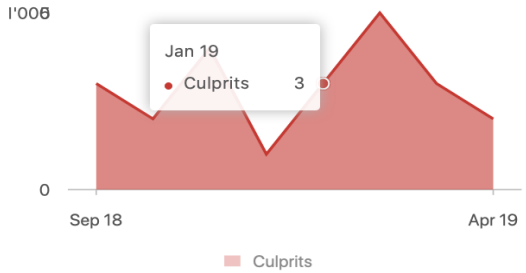
History

September 2018 - April 2019

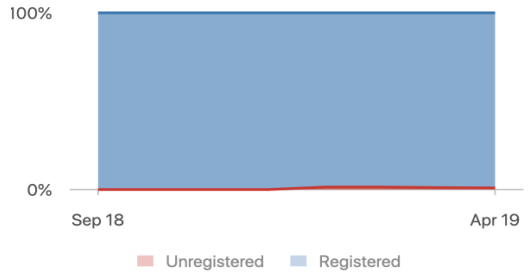
Incidents



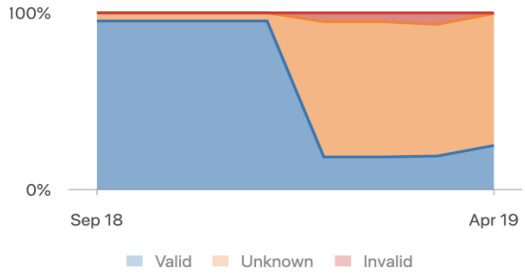
Culprits



Routing completeness (IRR)



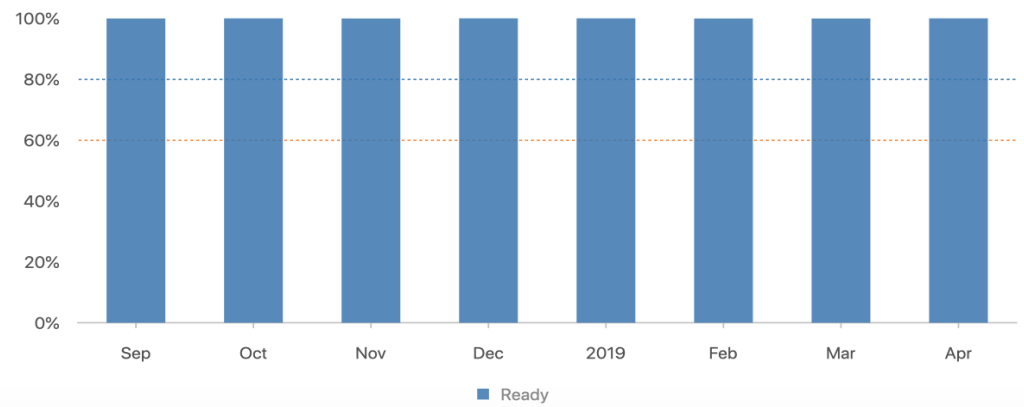
Routing completeness (RPKI)



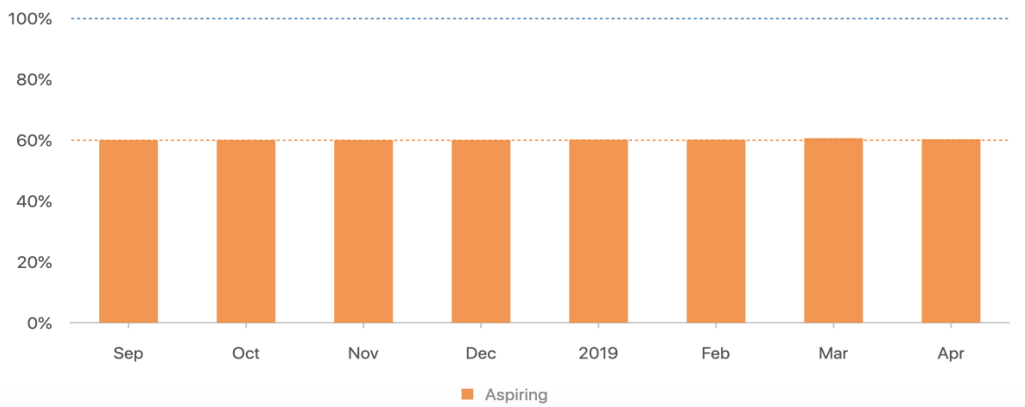
MANRS Readiness

Overall | Metrics

Filtering



Anti-spoofing



MONTH April 2019 COUNTRY Czechia

Details

Severity: All | Ready | Aspiring | Lagging

Scope: All | Filtering | Anti-spoofing | Coordination | Global Validation IRR | Global Validation RPKI

Result Limit: 100 | 200 | 500 | 1000

Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
2571	DHLNET - DHL Information Servic	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	92%	0%
2852	CESNET2 - CESNET z.s.p.o.	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	83%
3229	INTEK-AS - Intek Ltd.	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	0%
5588	GTSCE - T-Mobile Czech Republic	CZ	Europe	Eastern Europe	RIPE NCC	79%	60%	100%	100%	0%
5610	O2-CZECH-REPUBLIC - O2 Czech	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	65%
6679	SKADI-AS - Skadi Telecom JSC	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	67%	0%
6740	TISCALI - TS-Data s.r.o.	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	0%
6881	NIXCZ - NIX.CZ z.s.p.o.	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	100%
8251	NFX_ZSPO - FreeTel, s.r.o.	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	100%
8518	RFERL - RFE/RL, Inc., organizacni s	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	0%
8646	CLOUDINFRASTACK - cloudinfras	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	0%
8913	IPNET - Mopos Communications /	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	0%
9053	VSHOSTING-CDN - VSHosting s.r.	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	75%	67%
9080	GIN - Ipex Ltd.	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	0%
12344	CZECHITC - CZECH IT CLUSTER, d	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	100%
12570	ITSELF - itself s.r.o.	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	67%
12767	PRAGONET-AS - T-Mobile Czech I	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	0%
12984	PILSFREE - PilsFree, z. s.	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	0%
13036	TMOBILE-CZ - T-Mobile Czech Re	CZ	Europe	Eastern Europe	RIPE NCC	100%	60%	100%	100%	0%

MANRS Observatory

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

Details - ASN 2852

Download data

M1 - Route leak by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M2 - Route misorigin by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M1C - Route leak by a direct customer

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M2C - Route hijack by a direct customer

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M3 - Bogon prefixes announced by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M3C - Bogon prefixes propagated by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M4 - Bogon ASNs announced by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M4C - Bogon ASNs propagated by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

MANRS Observatory

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

M5 - Spoofing IP blocks

Absolute: **0.5** Normalized: **60%** Incident Count: **-**

Has records	Spoofed prefixes
False	-

M8 - Contact registration (RIR, IRR, PeeringDB)

Absolute: **0** Normalized: **100%** Incident Count: **-**

Checked on	Has contact info
2019-04-15	True

M7IRR - Registered routes (% of routes registered)

Absolute: **0%** Normalized: **100%** Incident Count: **-**

Number of prefixes	Number of unregistered prefixes	Unregistered prefixes	Checked on
23	0	-	2019-04-15

M7RPKI - Valid ROAs for routes (% of routes registered)

Absolute: **17%** Normalized: **83%** Incident Count: **-**

Number of prefixes	Number of unknown prefixes	Checked on
23	4	2019-04-15

M7RPKIN - Invalid routes

Absolute: **0%** Normalized: **100%** Incident Count: **-**

Number of prefixes	Number of invalid prefixes	Invalid prefixes
23	0	-

MANRS Observatory Access

Just launched beta test with MANRS Participants only

Aim to launch publicly later in the year

Discussing what levels of access should be available to participants and public

Still some false positives

There are sometimes good reasons for non-100% conformancy

BUT, this is all inherently public data anyway!

MANRS IXP Programme

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.

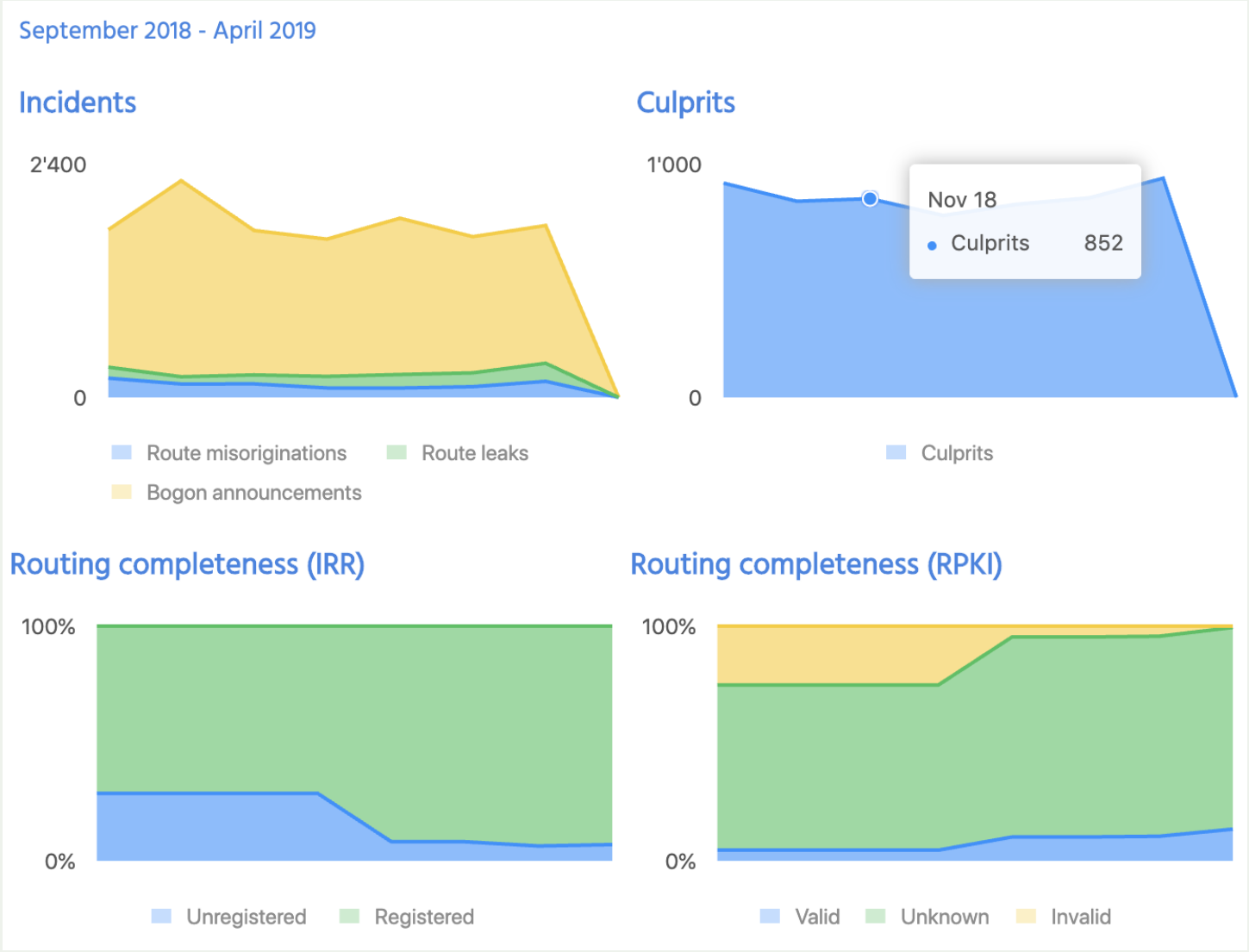
Action 4
Facilitate global operational communication and coordination

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.

Is the problem getting better or worse?



MANRS Community

MANRS needs to be community driven

MANRS should be (and is) a collaborative initiative of Internet operators

- Internet operators undertaking MANRS principles need to encourage use of best practices
- MANRS needs to be driven by leaders within their communities who strongly believe that routing security is an essential component for the future well being of the Internet
- Need feedback and recommendations for improving MANRS principles and best practices, e.g. MANRS Actions, MANRS Observatory, MANRS Implementation Guides, and training materials
- Internet Society can help with presentations, informational materials and merchandise (shirts and stickers)

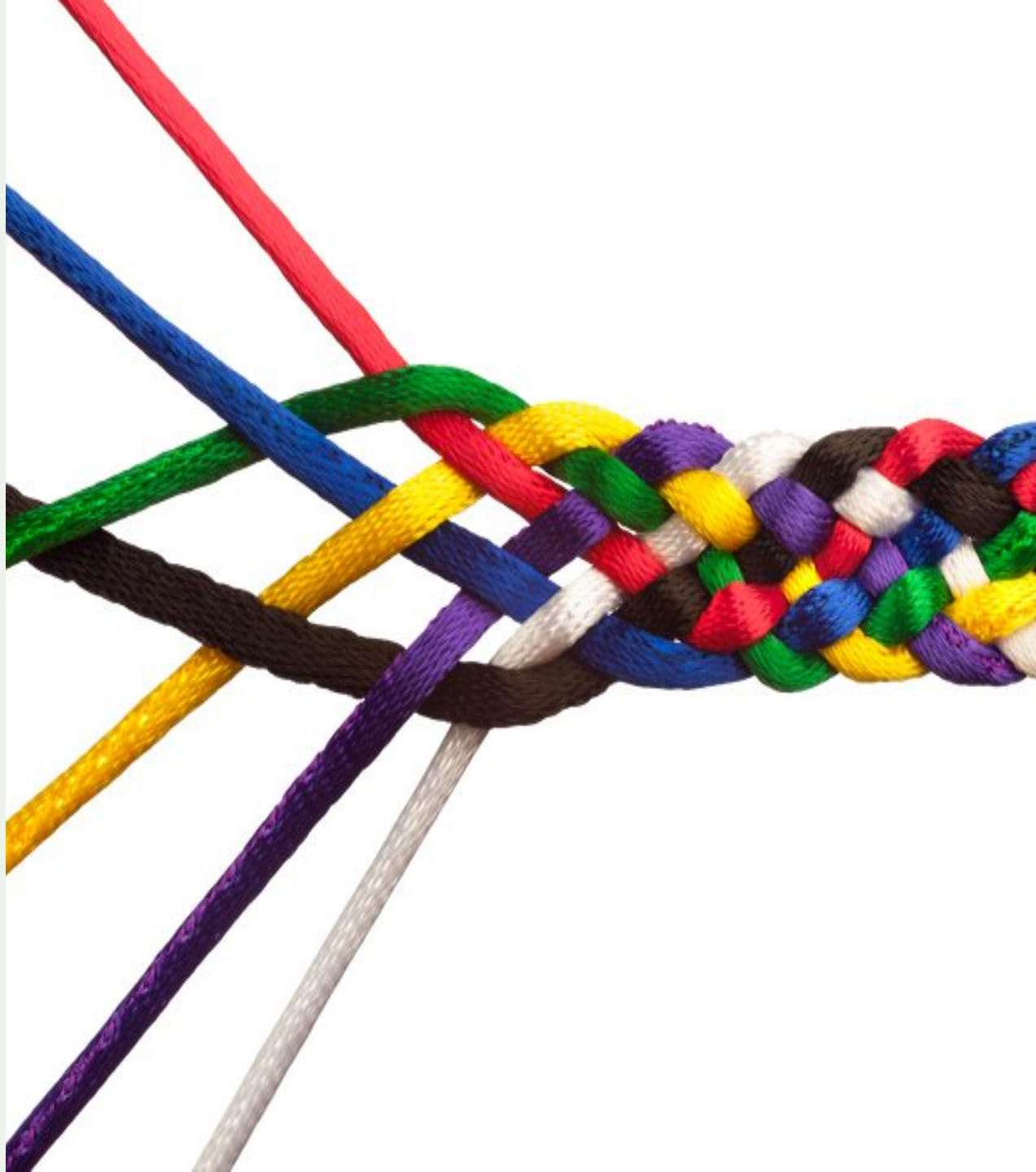
Join Us

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the manifesto and promote MANRS objectives



MANRS

Thank you.

Kevin Meynell
meynell@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120