12 November 2020
ENOG 17

Mutually Agreed Norms for Routing Security

Observing your MANRS

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

Background

There are ~70,000 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 *unverified trust* between networks

- No built-in validation that updates are legitimate
- Anyone can announce anything
- Lack of reliable resource data

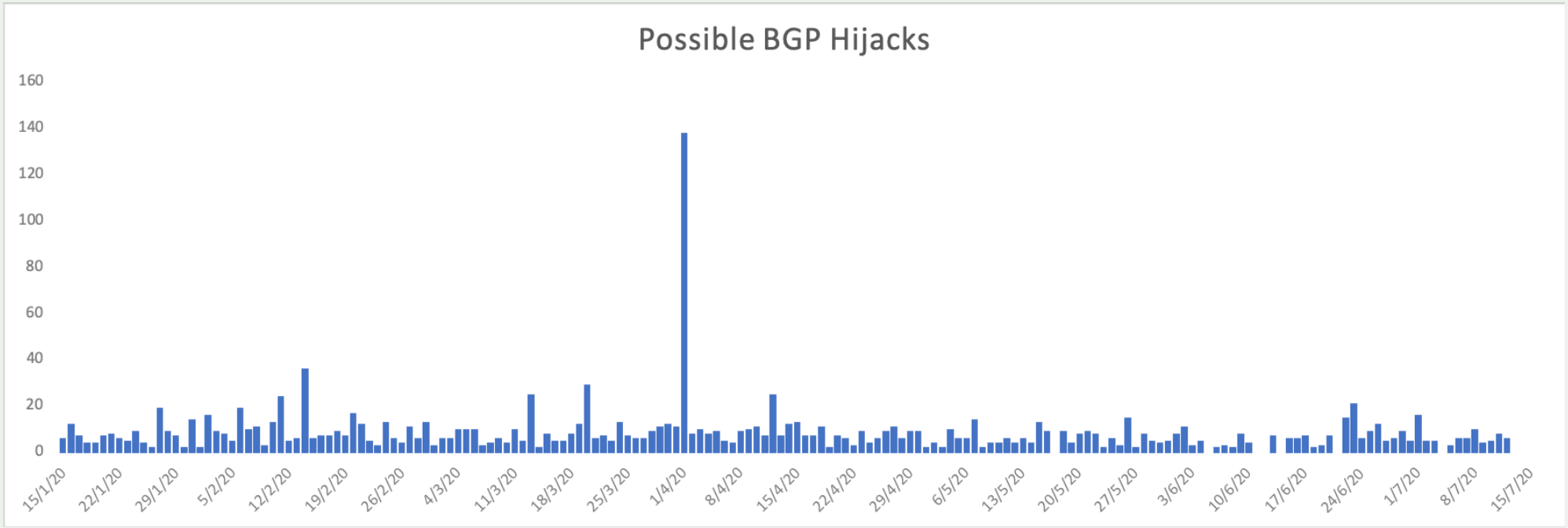
The routing system is under attack!

MANRS

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.	*June 2019. Verizon accepted incorrect routes from DQE Communications that diverted traffic destined for Cloudflare, Facebook & Amazon.*
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-amplification attack reported by Akamai*

The routing system is constantly under attack – incidents every day



http://bgpstream.com/

MANRS

Introduction to MANRS

Provides well-defined actions 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

3 programmes for Network Operators, IXPs & CDN/Cloud Providers (no fees)

MANRS Actions – Network Operators Programme

Launched November 2014. Actions 1, 3 and 4 are mandatory. Action 2 is optional.

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 relevant RIR database and/or PeeringDB

Global Validation

Facilitate validation of routing information on a global scale

Publish your routing data, so others can validate

Registering number resources in an IRR and/or creating ROAs for them

MANRS Actions – IXP Programme

Launched April 2018. Actions 1 and 2 are mandatory, plus at least one additional action is required.

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.

MANRS Actions - CDN & Cloud Programme

- Was launched on 31 March 2020 to complement existing Network Operators and IXP programme.
- Principles developed by large industry players including Akamai, Azion, Cloudflare, Comcast, Facebook, Google, Microsoft, Nexica Oracle, Redder, Telefonica, TORIX, Verisign.
- Conformance with Actions 1-5 is mandatory. Action 6 is optional.

Action 1

Prevent propagation of incorrect routing information

Egress filtering

Ingress filtering – non-transit peers, explicit whitelists

Action 2

Prevent traffic with illegitimate source IP addresses

Anti-spoofing controls to prevent packets with illegitimate source IP address

Action 3

Facilitate global operational communication and coordination

Contact information in relevant RIR database and/or PeeringDB

Action 4

Facilitate validation of routing information on a global scale

Publicly document ASNs and prefixes that are intended to be advertised to external parties

Action 5

Encourage MANRS adoption

Actively encourage MANRS adoption among the peers

Action 6

Provide monitoring and debugging tools to peering partners

Provide monitoring tools to indicate incorrect announcements from peers filtered by CDN & Cloud

The MANRS Observatory

Checking Conformance

MANRS Observatory - https://observatory.manrs.org/

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 / RIPE Stats
- PeeringDB
- IRRs
- RPKI Validator

MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH (PARTIAL) November 2020

Overview

State of Routing Security

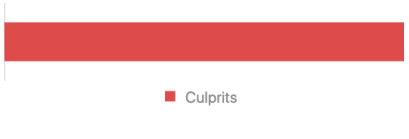
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
814	Route misoriginations	107
	Route leaks	65
	Bogon announcements	642

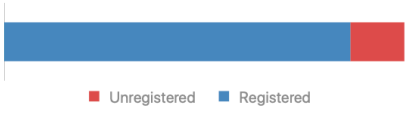
Culprits

Total		
678	Culprits	678



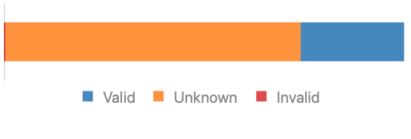
Routing completeness (IRR)

Total		
100%	Unregistered	13%
	Registered	87%



Routing completeness (RPKI)

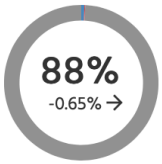
Total		
100%	Valid	26%
	Unknown	74%
	Invalid	1%



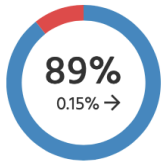
MANRS Readiness

Filtering

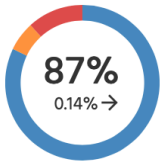
Anti-spoofing



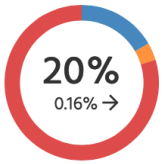
Coordination



Global Validation IRR



Global Validation RPKI

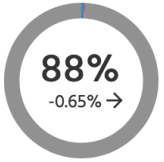


Ready Aspiring Lagging No Data Available

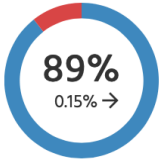
MANRS Readiness

Filtering

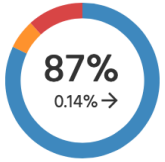
Anti-spoofing



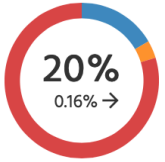
Coordination



Global Validation IRR



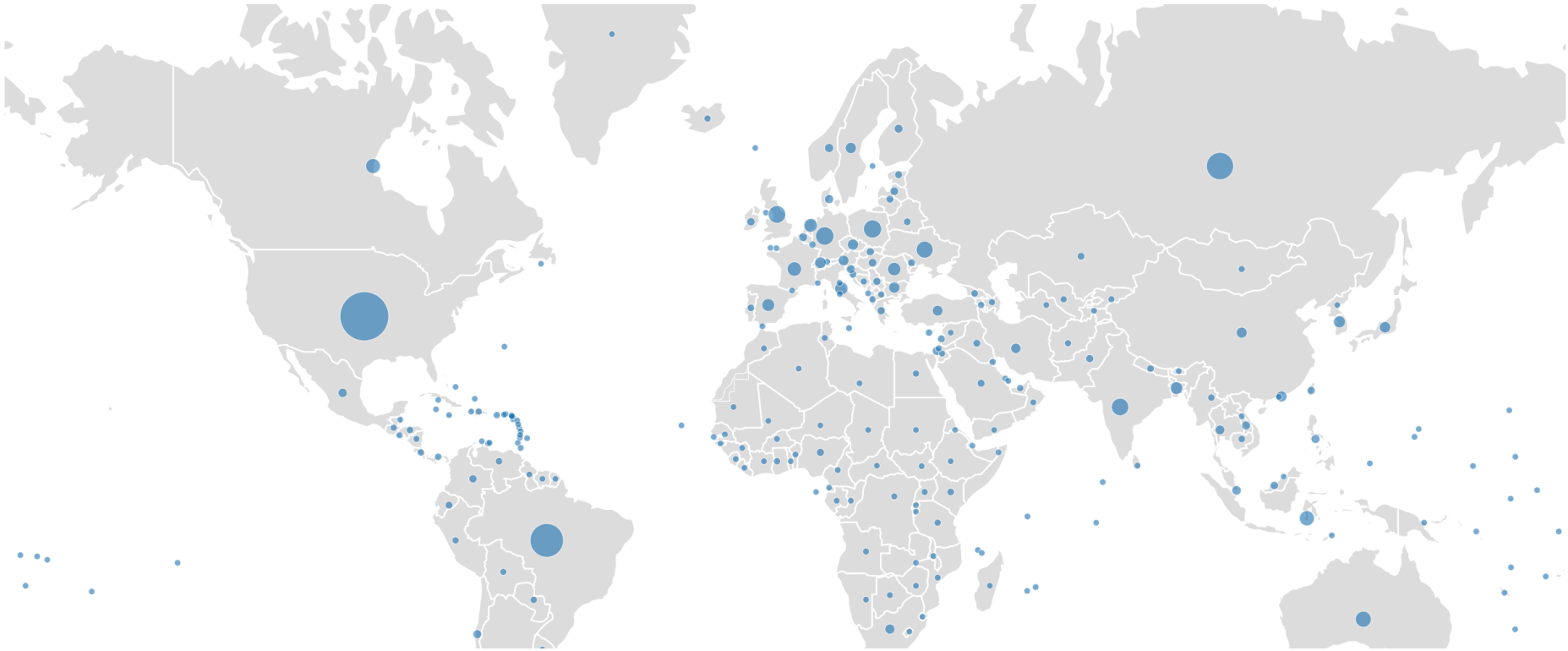
Global Validation RPKI



Ready Aspiring Lagging No Data Available

Global view

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



MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH (PARTIAL) November 2020 RIR REGIONS RIPE NCC

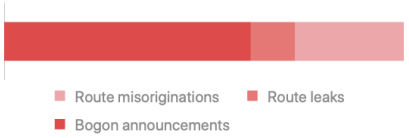
Overview

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

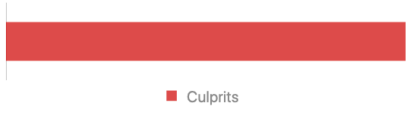
Incidents

Total		
172	Route misoriginations	47
	Route leaks	19
	Bogon announcements	106



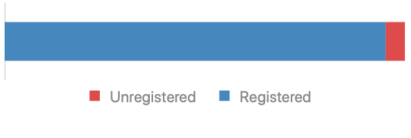
Culprits

Total		
162	Culprits	162



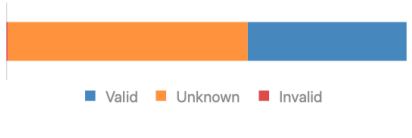
Routing completeness (IRR)

Total		
100%	Unregistered	5%
	Registered	95%



Routing completeness (RPKI)

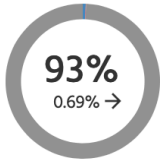
Total		
100%	Valid	40%
	Unknown	60%
	Invalid	1%



MANRS Readiness

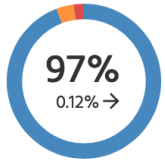
Filtering

Anti-spoofing

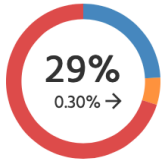


Coordination

Global Validation IRR



Global Validation RPKI



Ready Aspiring Lagging No Data Available

MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH (PARTIAL) November 2020 COUNTRY Russian Federation (the) Armenia Azerbaijan Belarus Georgia Kazakhstan Kyrgyzstan Moldova (the Republic of) Tajikistan Turkmenistan Ukraine Uzbekistan

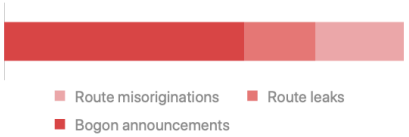
Overview

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

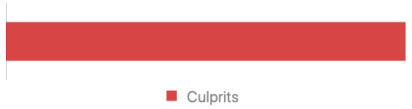
Incidents

Total		
45	Route misoriginations	10
	Route leaks	8
	Bogon announcements	27



Culprits

Total		
42	Culprits	42



Routing completeness (IRR)

Total		
100%	Unregistered	3%
	Registered	97%

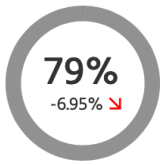
Routing completeness (RPKI)

Total		
100%	Valid	28%
	Unknown	72%
	Invalid	1%

MANRS Readiness

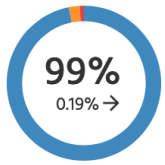
Filtering

Anti-spoofing

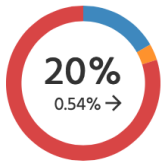


Coordination

Global Validation IRR



Global Validation RPKI



Ready Aspiring Lagging No Data Available

MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT ADMIN

MONTH (PARTIAL) November 2020 COUNTRY Russian Federation (the) Armenia Azerbaijan Belarus Georgia Kazakhstan Kyrgyzstan Moldova (the Republic of) Tajikistan Turkmenistan Ukraine Uzbekistan

Details

Severity: All | Ready | Aspiring | Lagging | No Data Available

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
1547	IDK-NETWORK - Societatea mixta	MD	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	0%
2118	RELCOM-AS - Limited Liability Co	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	98%	2%
2585	OPTICTELECOM-AS - Optic Telecc	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	0%
2587	FREE-NET-AS2587 - OOO FREEnet	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	0%
2601	RADIOLINK-AS - Radio-Link LLC	UA	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	0%
2848	MSU - Federal State Educational I	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	100%
2854	ROSPRINT-AS - LLC Orange Busin	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	3%
2864	ALJASKA-AS - PE Raniuk Mikola E	UA	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	100%
2875	JINR-AS - Joint Institute for Nucle	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	0%
3058	RAS-AS - Joint SuperComputer C	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	75%
3167	ASINFOPRO - Group of Company	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	0%
3168	ASINTELECOMTV - PE Dityatev Se	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	0%
3175	CITYTELECOM-MSK - Filanco LLC	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	2%
3179	AKVALIS-AS - Akvalis Ltd.	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	0%
3180	SMARTMS-AS - Smart Media Syst	RU	Europe	Eastern Europe	RIPE NCC	100%	-	100%	100%	100%

MANRS Dashboard

LOGOUT

OVERVIEW | HISTORY | DETAILS | COMPARISON | ABOUT | ADMIN

MONTH (PARTIAL) November 2020 ASN 3267 - RUNNET - The federal state a...

Overview

State of Routing Security

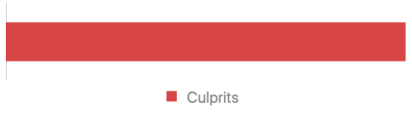
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
3	Route misoriginations	0
	Route leaks	1
	Bogon announcements	2

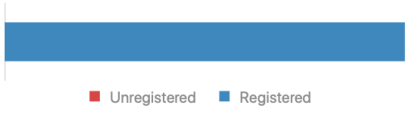
Culprits

Total		
1	Culprits	1



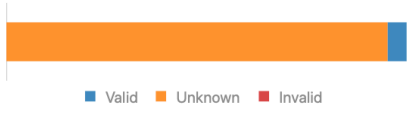
Routing completeness (IRR)

Total		
100%	Unregistered	0%
	Registered	100%



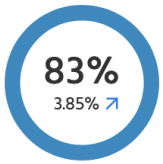
Routing completeness (RPKI)

Total		
100%	Valid	5%
	Unknown	95%
	Invalid	0%

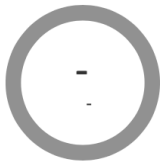


MANRS Readiness

Filtering



Anti-spoofing



Coordination

Global Validation IRR

Global Validation RPKI

Ready Aspiring Lagging No Data Available

MANRS **Dashboard** LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT ADMIN

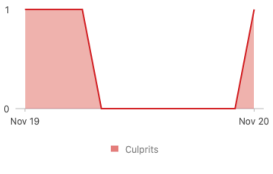
MONTH (PARTIAL) November 2020 ASN 3267 - RUNNET - The...

History

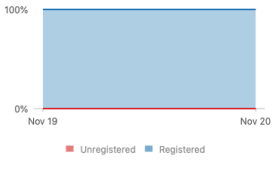
November 2019 - November 2020

Incidents

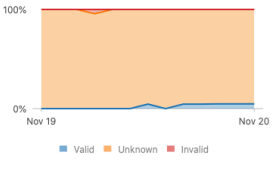
Culprits



Routing completeness (IRR)



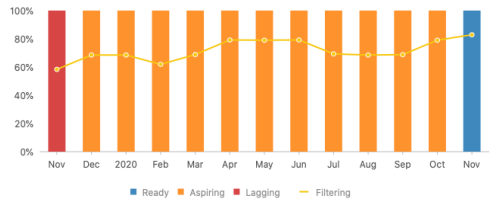
Routing completeness (RPKI)



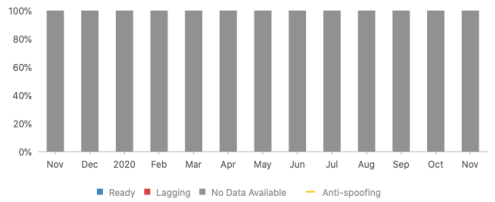
MANRS Readiness

Overall | Metrics

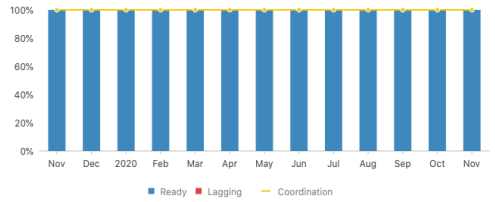
Filtering



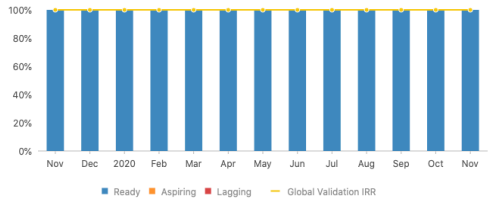
Anti-spoofing



Coordination



Global Validation IRR



MONTH (PARTIAL) November 2020 ASN 3267 - RUNNET - The...

Details - ASN 3267

Download data

M1 - Route leak by the AS

Absolute: **3.0** Normalized: **70%** Incident Count: **1**

Incident Id: 1 Absolute: 3.0 Start Date: 07-11-2020 12-59-39 End Date: 09-11-2020 01-00-00 Duration: 2d, 0m, 21s

Incident Id	Start Time	End Time	Duration	Prefix	Paths	Weight	Source	BGPstream EventId
1	2020-11-06 23:59:39	2020-11-09 00:00:00	2d, 0m, 21s	91.234.60.0/22	133812 137363 585...	1	bgpstream	259067

Download metrics data

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 Include possible related data

Download metrics data

M3 - Bogon prefixes announced by the AS

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

M3C - Bogon prefixes propagated by the AS

Absolute: **9.0** Normalized: **47%** Incident Count: **1**

Incident Id: 1 Absolute: 9.0 Start Date: 01-11-2020 01-00-00 End Date: 09-11-2020 01-00-00 Duration: 8d, 0m, 0s

Download metrics data

M4 - Bogon ASNs announced by the AS

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

Paths

133812 137363 58552 7473 6461 3267 198297 28917 1299 174 20764 198367

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

M4C - Bogon ASNs propagated by the AS

Absolute: **9.0** Normalized: **47%** Incident Count: **1**

Incident Id: 1 Absolute: 9.0 Start Date: 01-11-2020 01-00-00 End Date: 09-11-2020 01-00-00 Duration: 8d, 0m, 0s

Download metrics data

M5 - Spoofing IP blocks

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

Has records	Spoofed prefixes
False	-

Download metrics data

M8 - Contact registration (RIR, IRR, PeeringDB)

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

Checked on	Has contact info
2020-07-21	True

Download metrics data

M7IRR - Registered routes (% of routes registered)

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

Number of prefixes	unregistered prefixes	Unregistered prefixes	Checked on
21	0	-	2020-09-23

Download metrics data

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

Absolute: **95%** Normalized: **5%** Incident Count: **-**

Number of prefixes	Number of unknown prefixes	Routing consistency	Checked on
21	20	Routing consistency	2020-11-08

Download metrics data

M7RPKIN - Invalid routes

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

Number of prefixes	Number of invalid prefixes	Invalid prefixes
21	0	-

Download metrics data

AS Routing Consistency (as3267)

Reload this widget by entering a resource here

Prefixes | Imports | Exports

Show 10 entries Search:

prefix	In RIS	RIPE IRR	Other IRRs	RPKI
185.141.124.0/22	yes	yes	no	☺
193.232.68.0/23	yes	yes	no	
193.27.214.0/23	yes	yes	no	
194.190.224.0/19	yes	yes	no	
194.190.254.0/24	no	yes	no	
194.190.255.0/24	no	yes	no	
194.226.192.0/19	yes	yes	no	
194.85.160.0/20	yes	yes	no	
194.85.183.0/24	yes	yes	no	
194.85.32.0/20	yes	yes	no	

Showing 1 to 10 of 32 entries

MANRS Observatory Access

Current access policy:

- Public are able to view Overall, Regional and Economy aggregated data
- Only MANRS Participants have access to detailed data about their network
- Partner & Aspirant accounts can be made available to MANRS applicants

Caveats:

- Still some false positives
- There are sometimes good reasons for non-100% conformancy
- BUT, this is all inherently public data anyway!

MANRS Implementation Guide for Network Operators

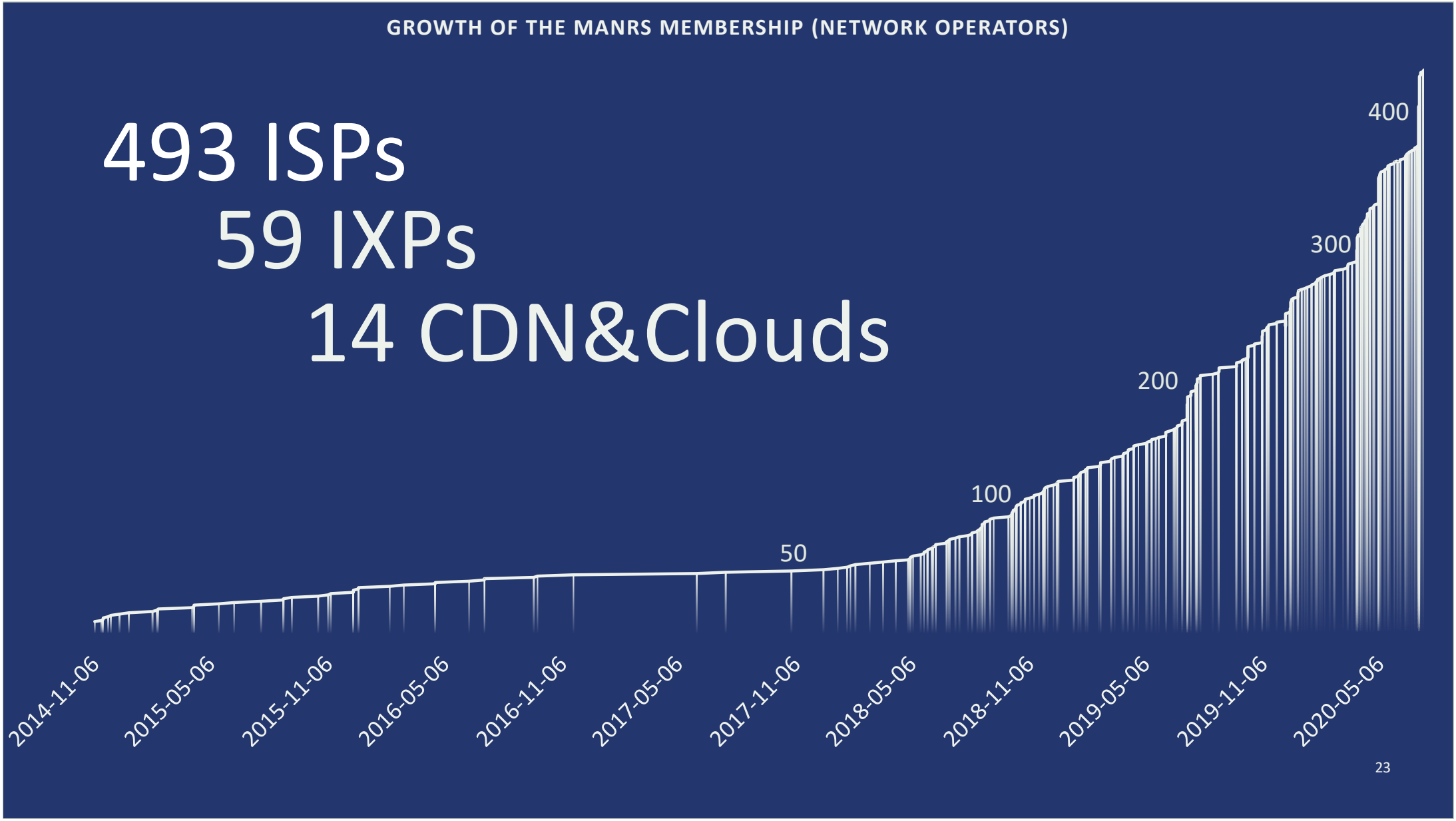
If you're not ready to join yet, implementation guidance is available to help you.

- 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

Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS Participation


GROWTH OF THE MANRS MEMBERSHIP (NETWORK OPERATORS)
493 ISPs
59 IXPs
14 CDN&Clouds
400
300
200
100
50
2014-11-06
2015-05-06
2015-11-06
2016-05-06
2016-11-06
2017-05-06
2017-11-06
2018-05-06
2018-11-06
2019-05-06
2019-11-06
2020-05-06
23

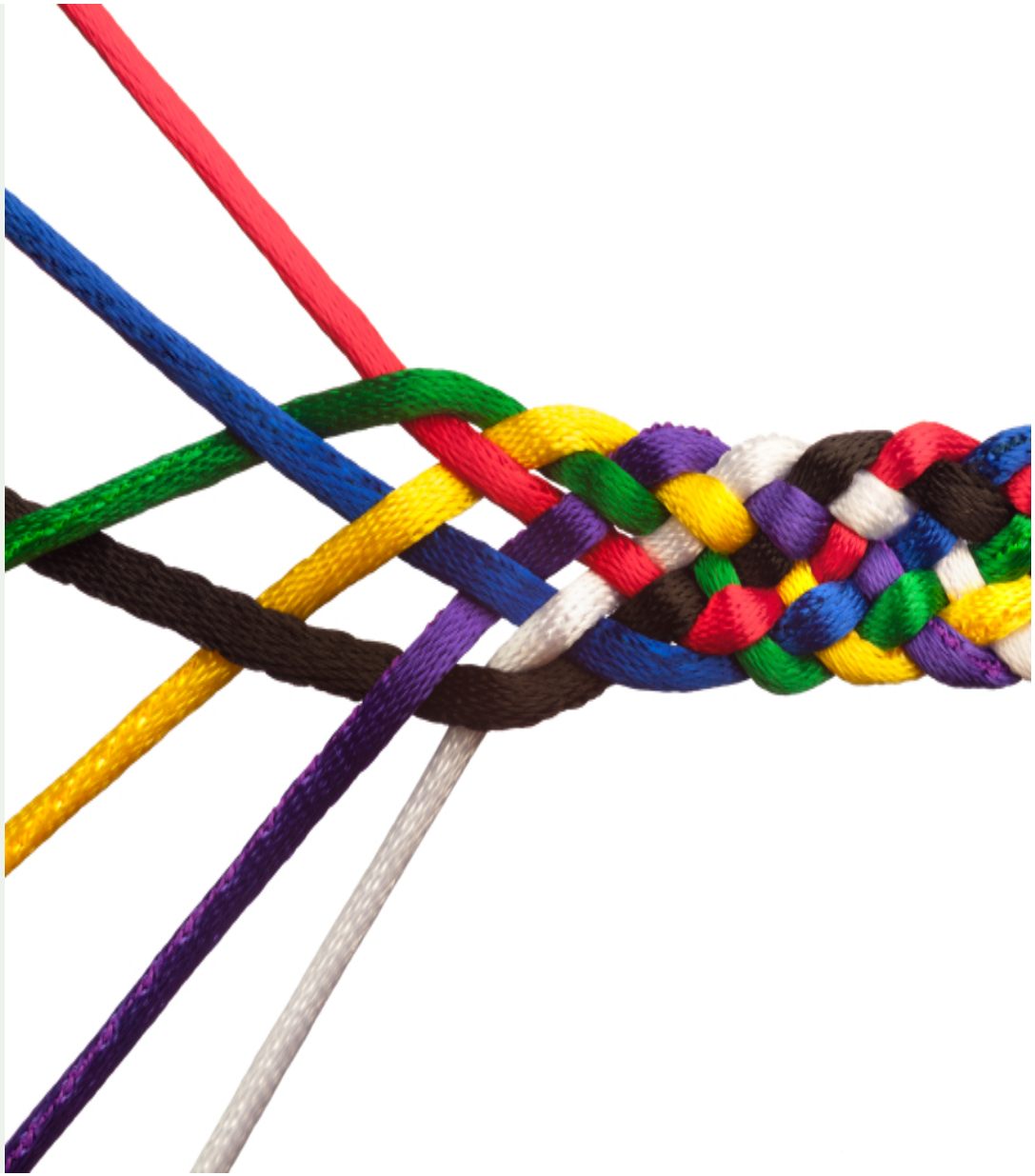
Join the MANRS Community

Visit https://www.manrs.org

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

Get Involved in the Community

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



MANRS