Introduction to the MANRS Observatory

Measuring readiness for the Mutually Agreed Norms for Routing Security (MANRS)

Dan York

york@isoc.org

Background

There are 66,000+ 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 *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!

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.	*November 2018. Google faced a major outage in many parts of the world thanks to a BGP leak. This incident that was caused by a Nigerian ISP MainOne.* *June 2019. Allegheny leaked routes from another provider to Verizon, causing significant outage.*
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	The root cause of reflection DDoS attacks	*March 1, 2018. Memcached 1.3Tb/s reflection-amplification attack reported by Akamai*

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 for 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

MANRS for Internet Exchange Points (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.

MANRS for CDN&Cloud - a draft action set

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 PeeringDB

and relevant RIR databases

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

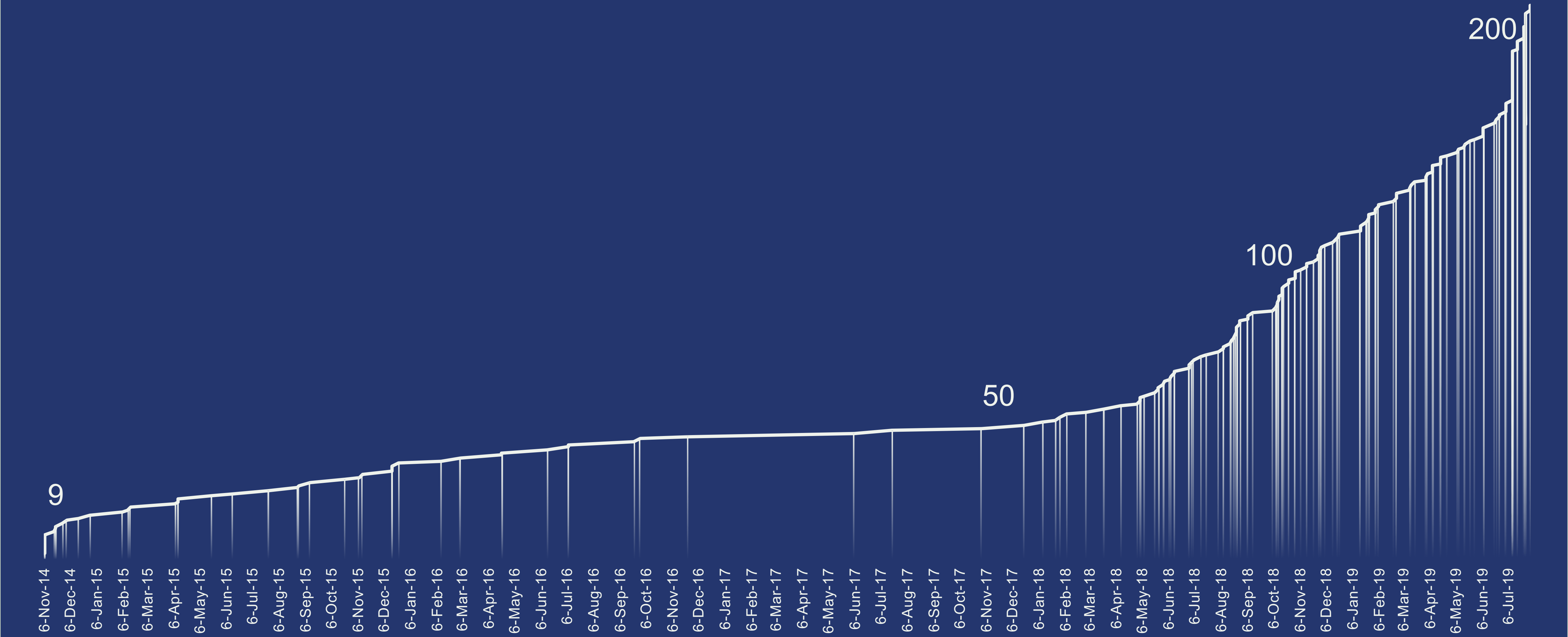
Provide monitoring tools to indicate incorrect announcements from peers that were filtered by the CDN&Cloud operator.

MANRS – increasing adoption

237 ISPs

42 IXPs

GROWTH OF THE MANRS MEMBERSHIP (NETWORK OPERATORS)



Measuring MANRS Readiness

Motivation

Inform MANRS members about their degree of commitment

- Improve reputation and transparency of the effort
- Facilitate continuous improvement and correction

Provide a factual state of routing security as it relates to MANRS

- Support the problem statement with data
- Demonstrate the impact and progress
- Network, country, region, over time

Improve robustness of the evaluation process

- Make it more comprehensive and consistent
- Reduce the load
- Allow preparation (self-assessment)

Measurement framework

- Passive
- Based on third party open data sources

Data sources and caveats

Action	Measurement	Data source	Caveats
Filtering *M1, M1C, M2, M2C*	Route hijacks and leaks	BGPStream.com	False positives, obscure algorithms, vantage points
Filtering *M3, M3C, M4, M4C*	“Bogon” announcements	CIDR report	Limited vantage points
Anti-spoofing *M5*	Negative tests	CAIDA Spoofer	Sparse, active
Coordination *M8*	Registered contacts	RIRs Whois DBs	Stale/non-responsive contacts not detected
Global validation *M7IRR, M7RPKI, M7RPKIN*	Coverage of routing announcements	IRRs, RPKI	

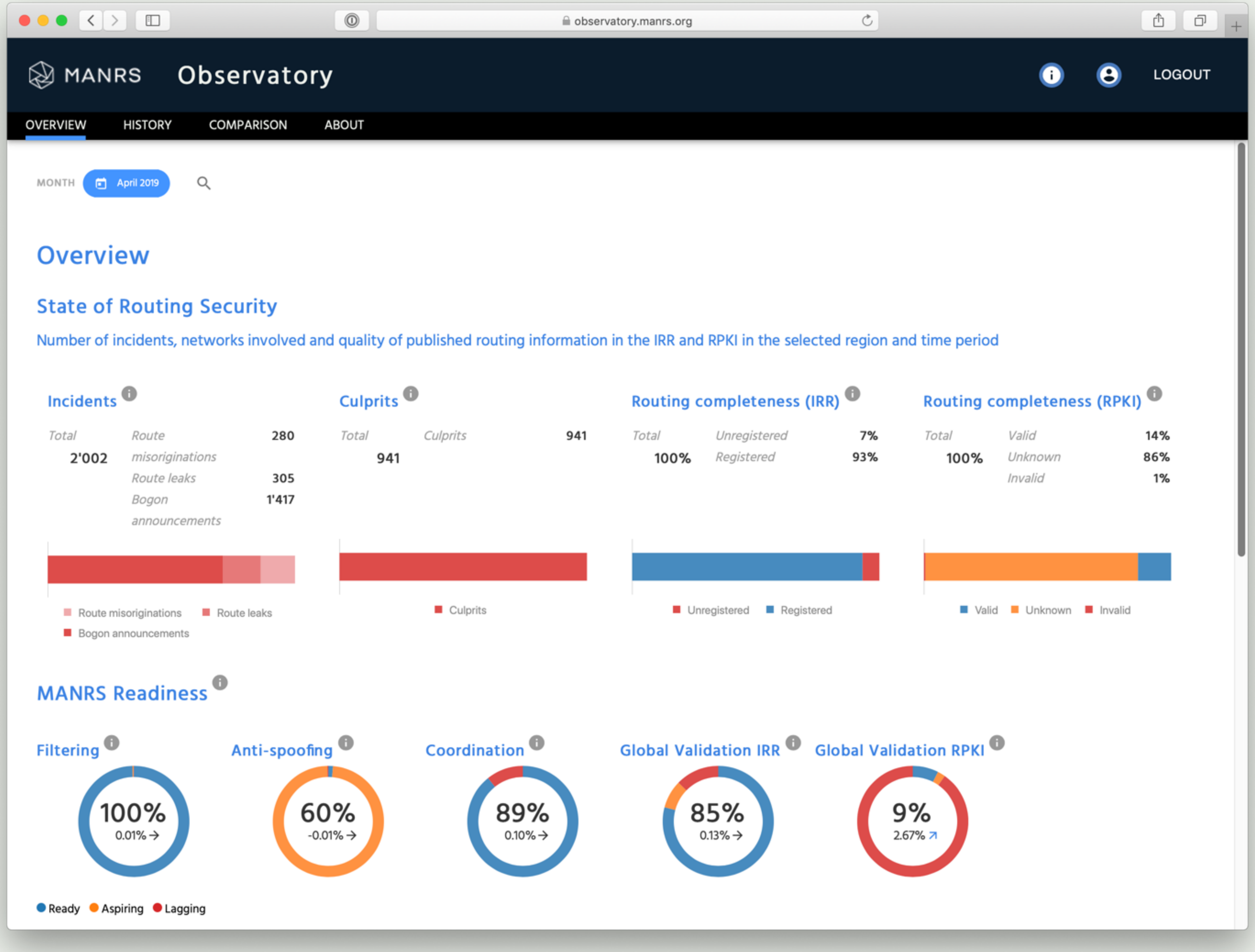
2 views of the Observatory

Public view – granularity: region, economy, pre-defined groups (e.g. MANRS)

Private view – granularity: region, economy, ASN

2 views of the Observatory

Public view



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)

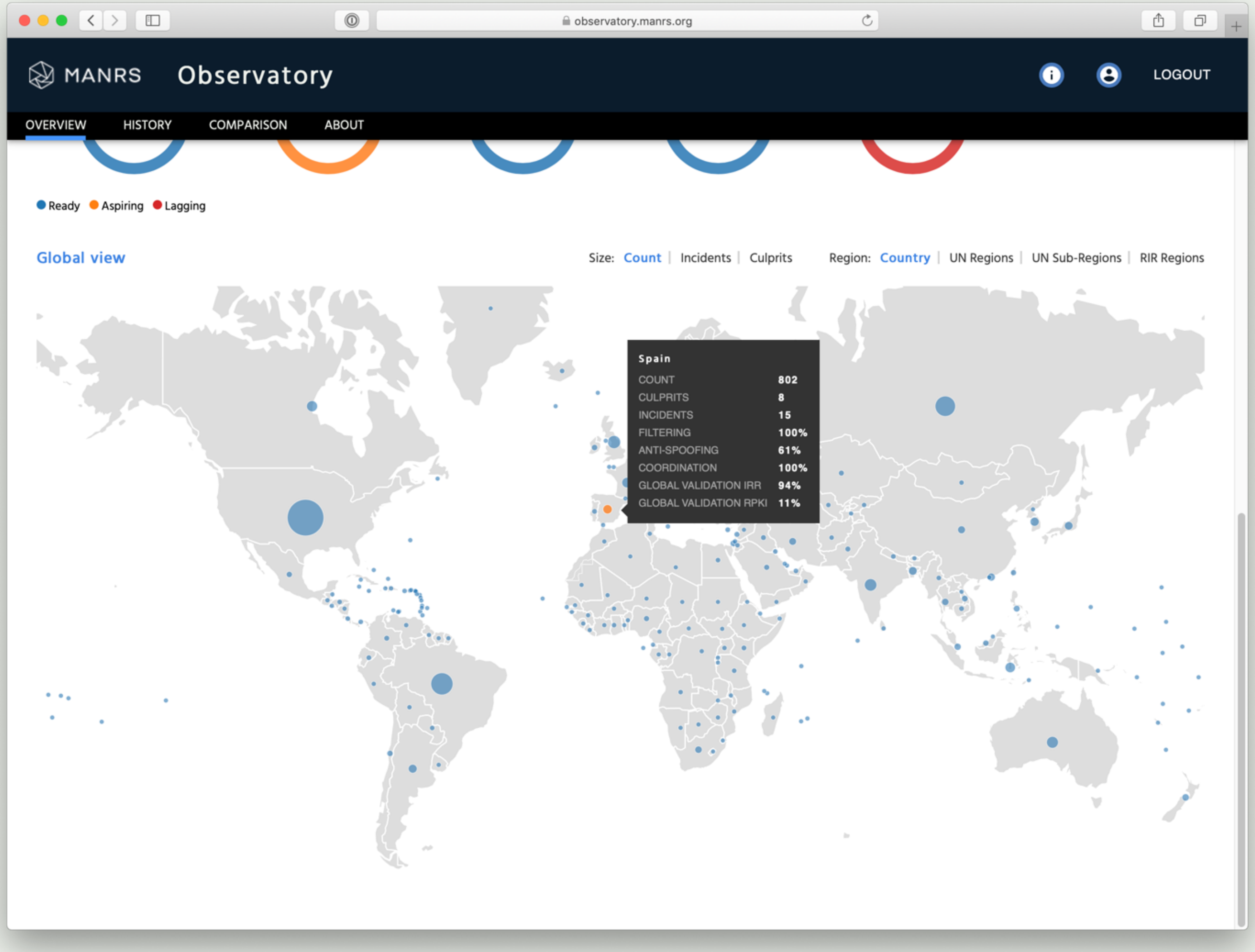
Total		
100%	*Unregistered*	7%
	Registered	93%

Routing completeness (RPKI)

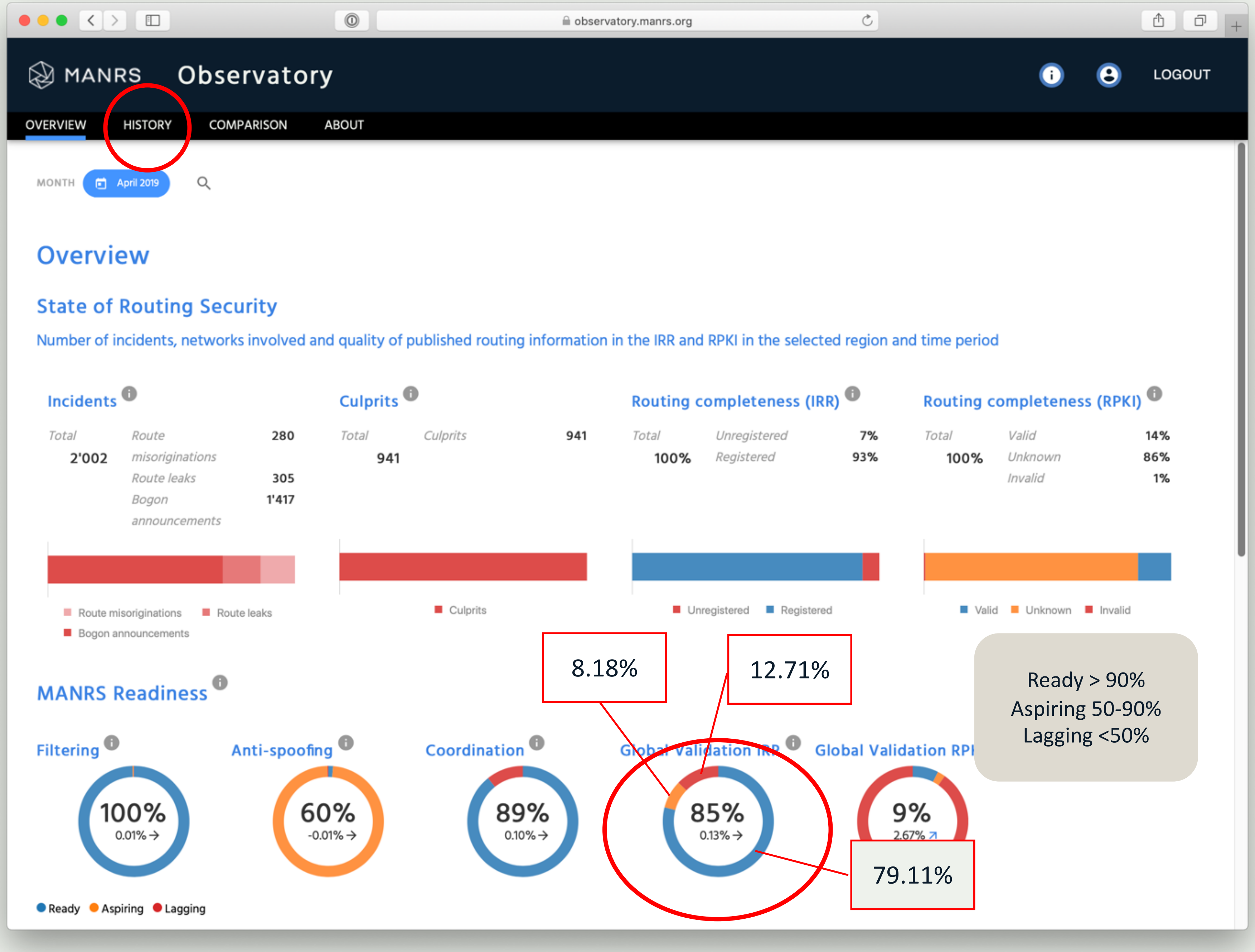
Total		
100%	*Valid*	14%
	Unknown	86%
	Invalid	1%

MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100% 0.01% →	60% -0.01% →	89% 0.10% →	85% 0.13% →	9% 2.67% ↗


observatory.manrs.org
MANRS
Observatory
LOGOUT
OVERVIEW
HISTORY
COMPARISON
ABOUT
● Ready ● Aspiring ● Lagging
Global view
Size: Count | Incidents | Culprits
Region: Country | UN Regions | UN Sub-Regions | RIR Regions

Spain	
COUNT	802
CULPRITS	8
INCIDENTS	15
FILTERING	100%
ANTI-SPOOFING	61%
COORDINATION	100%
GLOBAL VALIDATION IRR	94%
GLOBAL VALIDATION RPKI	11%



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

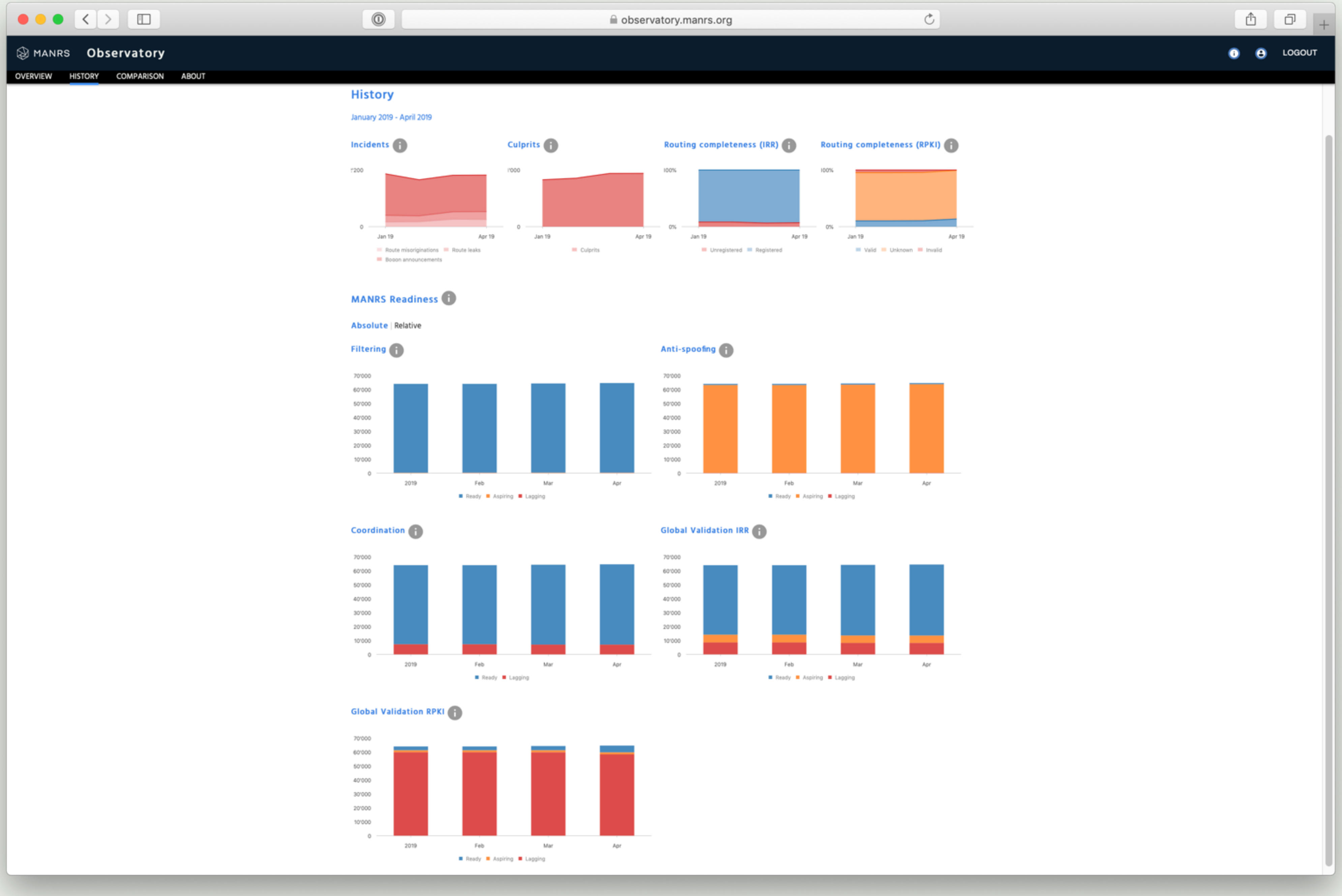
Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100% 0.01% →	60% -0.01% →	89% 0.10% →	85% 0.13% →	9% 2.67% ↗

8.18%

12.71%

79.11%

Ready > 90%
Aspiring 50-90%
Lagging <50%

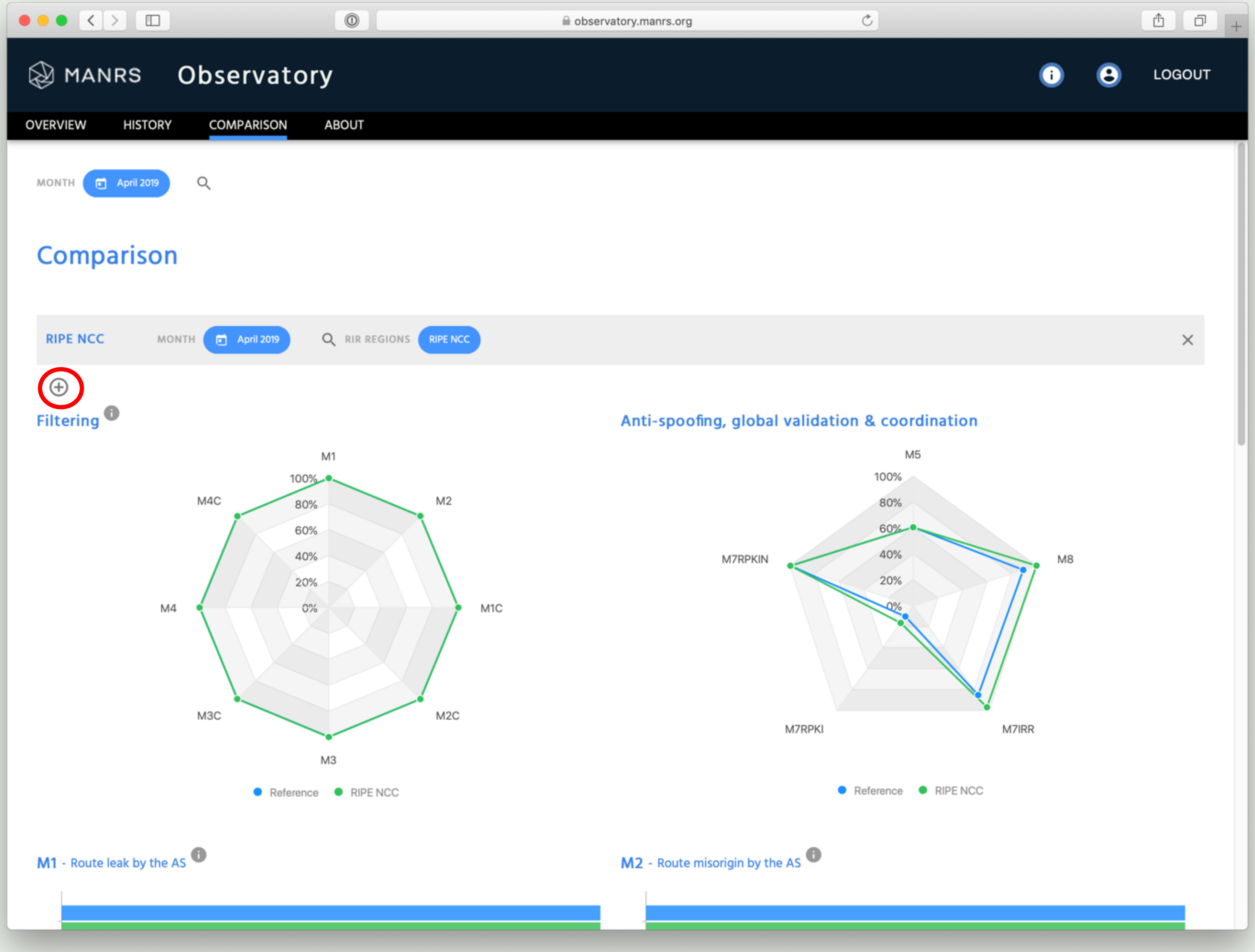


History

January 2019 - April 2019

MANRS Readiness

Absolute | Relative



MONTH April 2019

Comparison

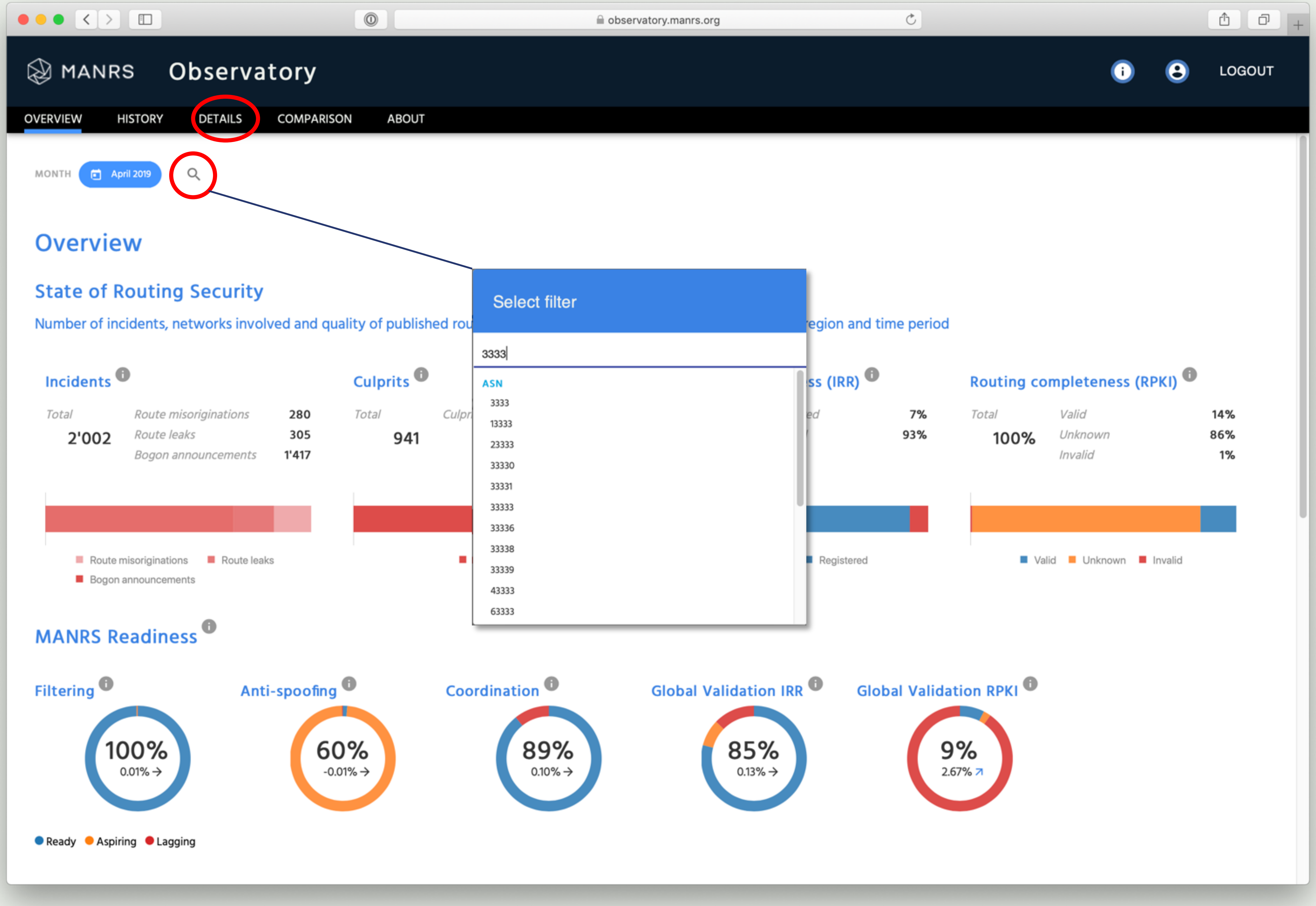
RIPE NCC MONTH April 2019 RIR REGIONS RIPE NCC

M1 - Route leak by the AS

M2 - Route misorigin by the AS

2 views of the Observatory

Private view



Overview

State of Routing Security

Number of incidents, networks involved and quality of published rou egion and time period

Select filter

3333

ASN

3333
13333
23333
33330
33331
33333
33336
33338
33339
43333
63333

Incidents

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

Culprits

Total *Culpr*

941

ss (IRR)

ed 7%

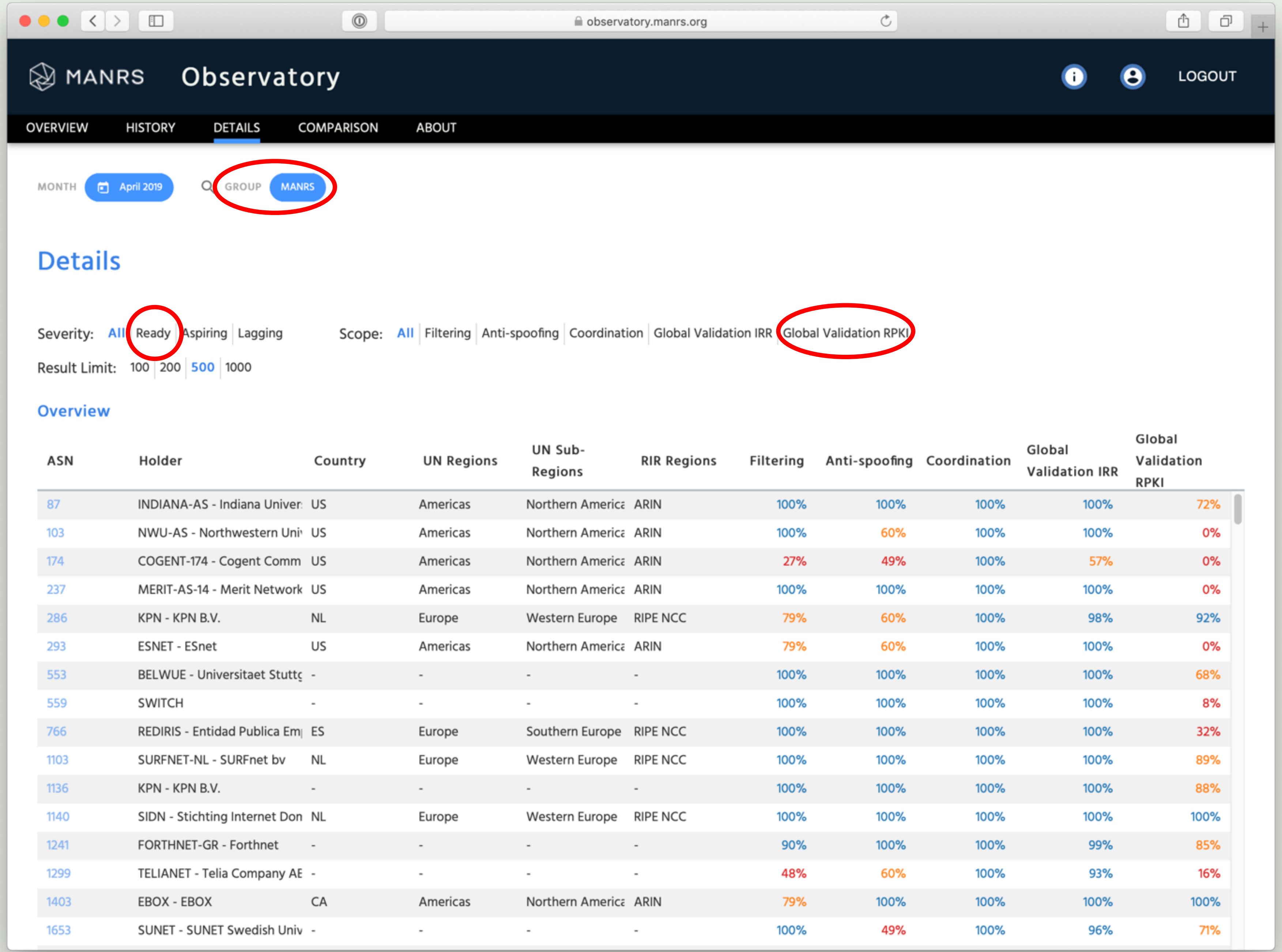
93%

Routing completeness (RPKI)

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

MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100% 0.01% →	60% -0.01% →	89% 0.10% →	85% 0.13% →	9% 2.67% ↗



MONTH April 2019 GROUP [✓ MANRS]

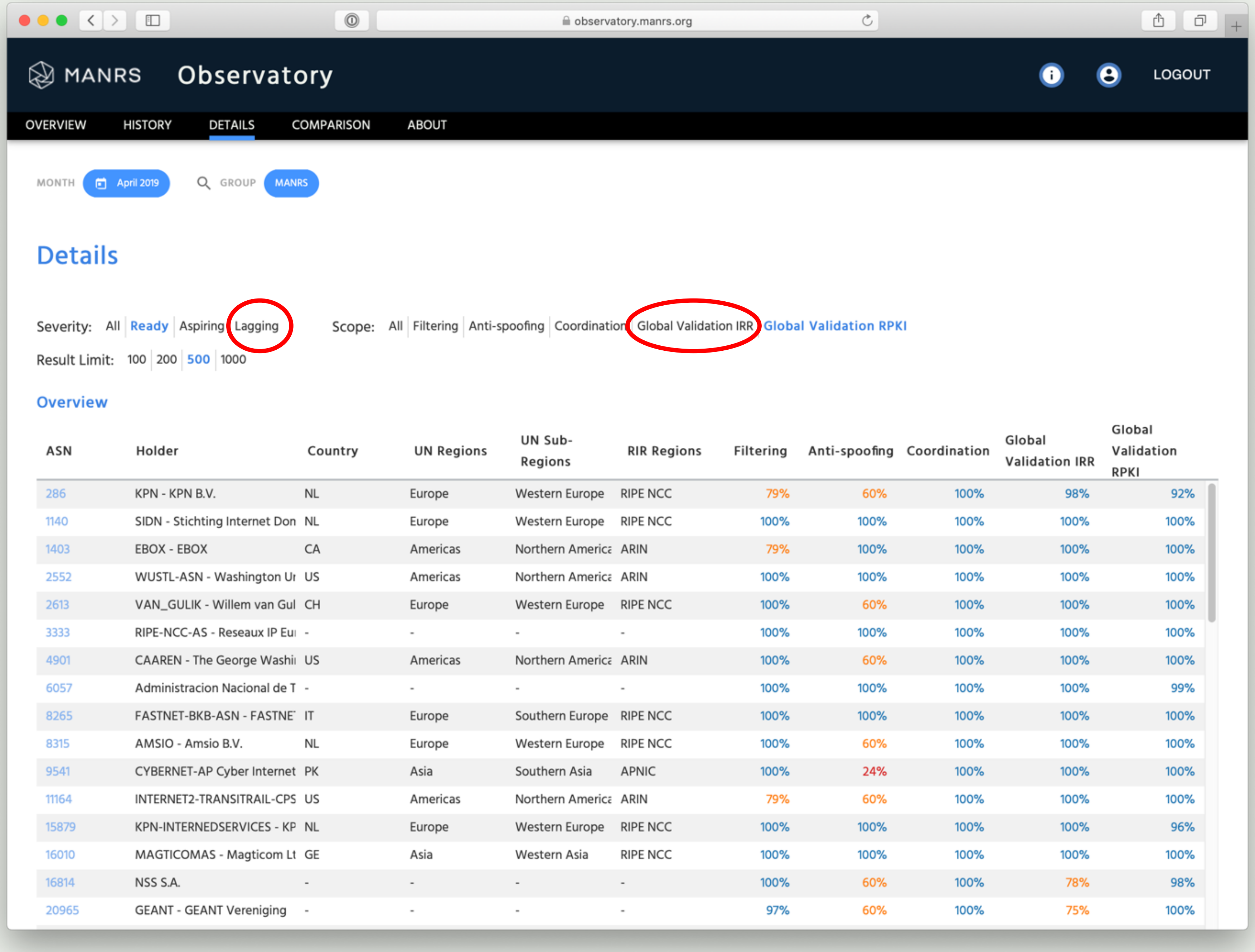
Details

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
87	INDIANA-AS - Indiana Univer:	US	Americas	Northern America	ARIN	100%	100%	100%	100%	72%
103	NWU-AS - Northwestern Uni	US	Americas	Northern America	ARIN	100%	60%	100%	100%	0%
174	COGENT-174 - Cogent Comm	US	Americas	Northern America	ARIN	27%	49%	100%	57%	0%
237	MERIT-AS-14 - Merit Network	US	Americas	Northern America	ARIN	100%	100%	100%	100%	0%
286	KPN - KPN B.V.	NL	Europe	Western Europe	RIPE NCC	79%	60%	100%	98%	92%
293	ESNET - ESnet	US	Americas	Northern America	ARIN	79%	60%	100%	100%	0%
553	BELWUE - Universitaet Stuttg	-	-	-	-	100%	100%	100%	100%	68%
559	SWITCH	-	-	-	-	100%	100%	100%	100%	8%
766	REDIRIS - Entidad Publica Em	ES	Europe	Southern Europe	RIPE NCC	100%	100%	100%	100%	32%
1103	SURFNET-NL - SURFnet bv	NL	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	89%
1136	KPN - KPN B.V.	-	-	-	-	100%	100%	100%	100%	88%
1140	SIDN - Stichting Internet Don	NL	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	100%
1241	FORTHNET-GR - Forthnet	-	-	-	-	90%	100%	100%	99%	85%
1299	TELIANET - Telia Company AE	-	-	-	-	48%	60%	100%	93%	16%
1403	EBOX - EBOX	CA	Americas	Northern America	ARIN	79%	100%	100%	100%	100%
1653	SUNET - SUNET Swedish Univ	-	-	-	-	100%	49%	100%	96%	71%



observatory.manrs.org

MANRS Observatory

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

MONTH April 2019 GROUP MANRS

Details

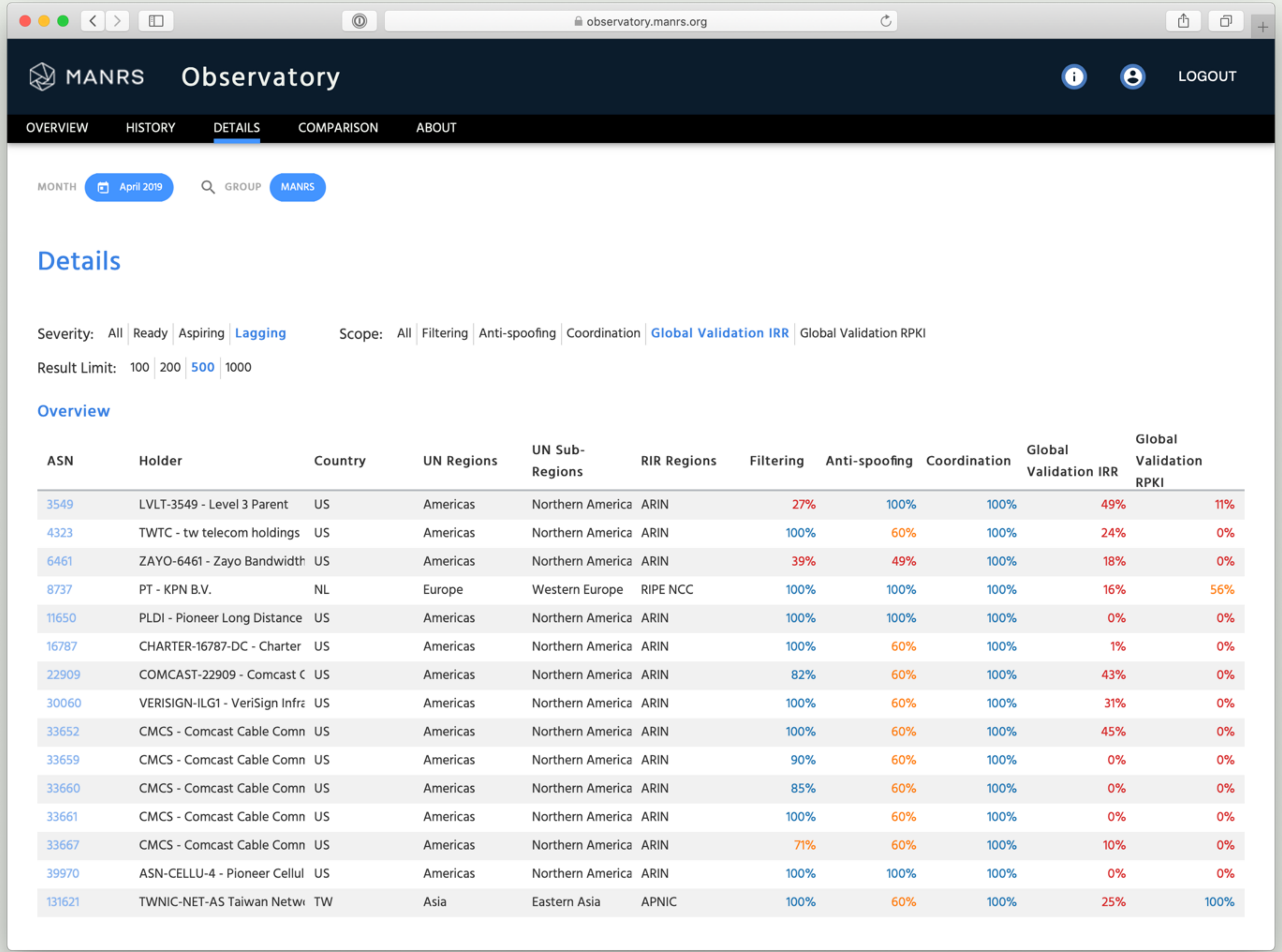
Severity: All | Ready | Aspiring | Lagging

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
286	KPN - KPN B.V.	NL	Europe	Western Europe	RIPE NCC	79%	60%	100%	98%	92%
1140	SIDN - Stichting Internet Don	NL	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	100%
1403	EBOX - EBOX	CA	Americas	Northern Americ	ARIN	79%	100%	100%	100%	100%
2552	WUSTL-ASN - Washington Ur	US	Americas	Northern Americ	ARIN	100%	100%	100%	100%	100%
2613	VAN_GULIK - Willem van Gul	CH	Europe	Western Europe	RIPE NCC	100%	60%	100%	100%	100%
3333	RIPE-NCC-AS - Reseaux IP Eu	-	-	-	-	100%	100%	100%	100%	100%
4901	CAAREN - The George Washi	US	Americas	Northern Americ	ARIN	100%	60%	100%	100%	100%
6057	Administracion Nacional de T	-	-	-	-	100%	100%	100%	100%	99%
8265	FASTNET-BKB-ASN - FASTNE	IT	Europe	Southern Europe	RIPE NCC	100%	100%	100%	100%	100%
8315	AMSIO - Amsio B.V.	NL	Europe	Western Europe	RIPE NCC	100%	60%	100%	100%	100%
9541	CYBERNET-AP Cyber Internet	PK	Asia	Southern Asia	APNIC	100%	24%	100%	100%	100%
11164	INTERNET2-TRANSITRAIL-CPS	US	Americas	Northern Americ	ARIN	79%	60%	100%	100%	100%
15879	KPN-INTERNEDSERVICES - KP	NL	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	96%
16010	MAGTICOMAS - Magticom Lt	GE	Asia	Western Asia	RIPE NCC	100%	100%	100%	100%	100%
16814	NSS S.A.	-	-	-	-	100%	60%	100%	78%	98%
20965	GEANT - GEANT Vereniging	-	-	-	-	97%	60%	100%	75%	100%



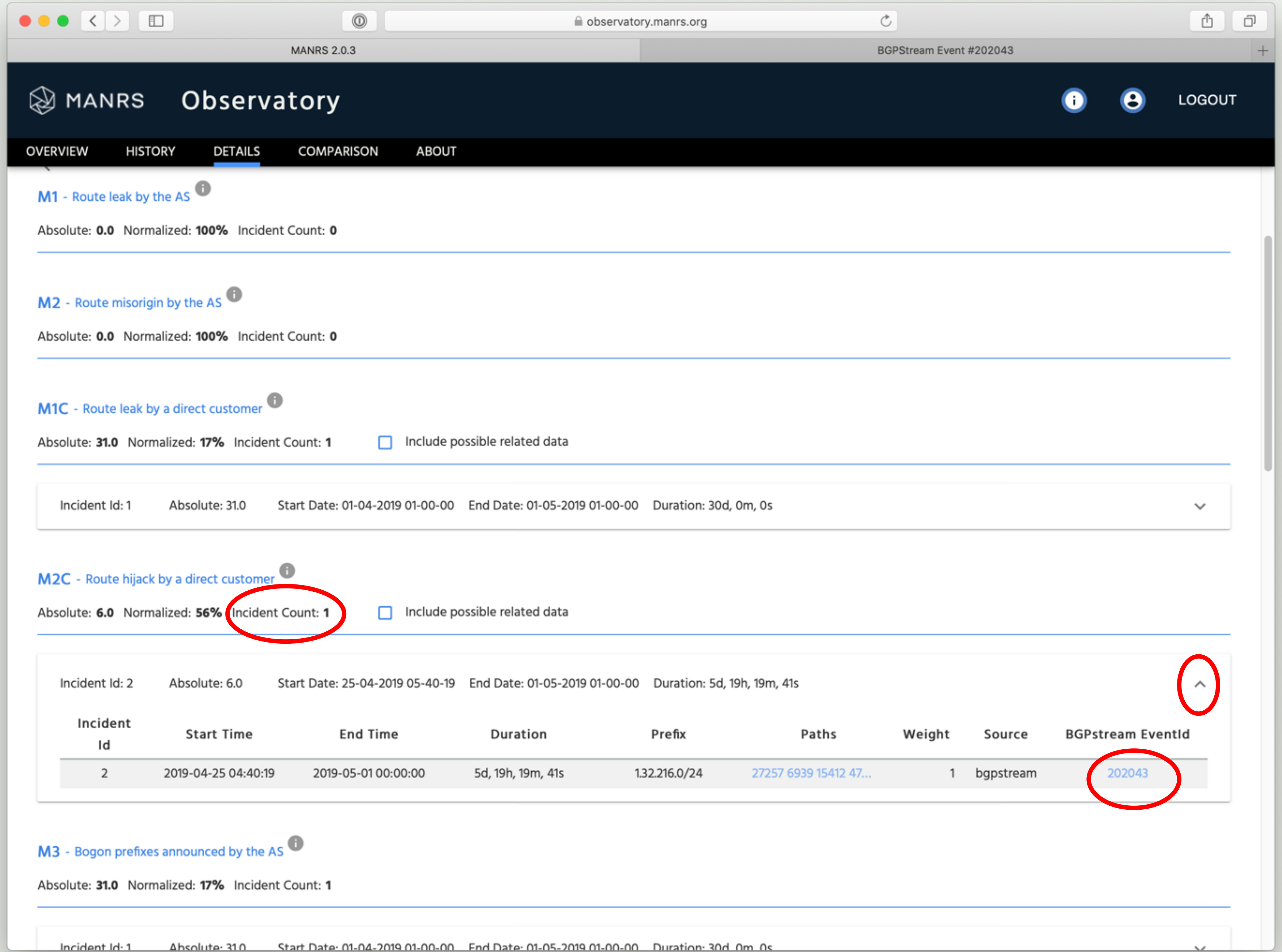
Details

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
3549	LVLT-3549 - Level 3 Parent	US	Americas	Northern America	ARIN	27%	100%	100%	49%	11%
4323	TWTC - tw telecom holdings	US	Americas	Northern America	ARIN	100%	60%	100%	24%	0%
6461	ZAYO-6461 - Zayo Bandwidth	US	Americas	Northern America	ARIN	39%	49%	100%	18%	0%
8737	PT - KPN B.V.	NL	Europe	Western Europe	RIPE NCC	100%	100%	100%	16%	56%
11650	PLDI - Pioneer Long Distance	US	Americas	Northern America	ARIN	100%	100%	100%	0%	0%
16787	CHARTER-16787-DC - Charter	US	Americas	Northern America	ARIN	100%	60%	100%	1%	0%
22909	COMCAST-22909 - Comcast C	US	Americas	Northern America	ARIN	82%	60%	100%	43%	0%
30060	VERISIGN-ILG1 - VeriSign Infra	US	Americas	Northern America	ARIN	100%	60%	100%	31%	0%
33652	CMCS - Comcast Cable Comn	US	Americas	Northern America	ARIN	100%	60%	100%	45%	0%
33659	CMCS - Comcast Cable Comn	US	Americas	Northern America	ARIN	90%	60%	100%	0%	0%
33660	CMCS - Comcast Cable Comn	US	Americas	Northern America	ARIN	85%	60%	100%	0%	0%
33661	CMCS - Comcast Cable Comn	US	Americas	Northern America	ARIN	100%	60%	100%	0%	0%
33667	CMCS - Comcast Cable Comn	US	Americas	Northern America	ARIN	71%	60%	100%	10%	0%
39970	ASN-CELLU-4 - Pioneer Cellul	US	Americas	Northern America	ARIN	100%	100%	100%	0%	0%
131621	TWNIC-NET-AS Taiwan Netw	TW	Asia	Eastern Asia	APNIC	100%	60%	100%	25%	100%



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: **31.0** Normalized: **17%** Incident Count: **1** □ Include possible related data

Incident Id: 1 Absolute: 31.0 Start Date: 01-04-2019 01-00-00 End Date: 01-05-2019 01-00-00 Duration: 30d, 0m, 0s

M2C - Route hijack by a direct customer

Absolute: **6.0** Normalized: **56%** Incident Count: **1** □ Include possible related data

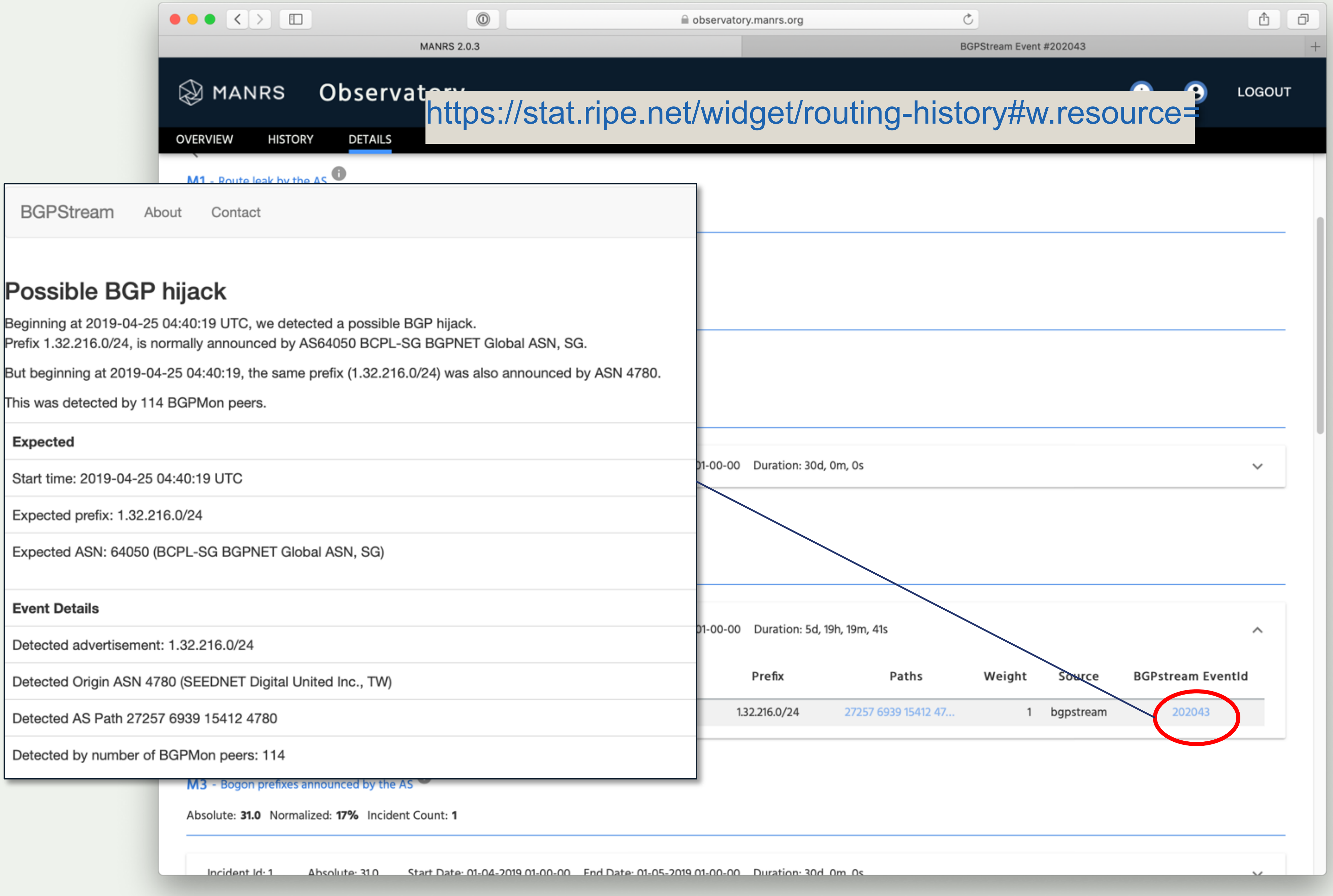
Incident Id: 2 Absolute: 6.0 Start Date: 25-04-2019 05-40-19 End Date: 01-05-2019 01-00-00 Duration: 5d, 19h, 19m, 41s

Incident Id	Start Time	End Time	Duration	Prefix	Paths	Weight	Source	BGPstream EventId
2	2019-04-25 04:40:19	2019-05-01 00:00:00	5d, 19h, 19m, 41s	1.32.216.0/24	27257 6939 15412 47...	1	bgpstream	202043

M3 - Bogon prefixes announced by the AS

Absolute: **31.0** Normalized: **17%** Incident Count: **1**

Incident Id: 1 Absolute: 31.0 Start Date: 01-04-2019 01-00-00 End Date: 01-05-2019 01-00-00 Duration: 30d, 0m, 0s



https://stat.ripe.net/widget/routing-history#w.resource=

M1 - Route leak by the AS

Possible BGP hijack

Beginning at 2019-04-25 04:40:19 UTC, we detected a possible BGP hijack.
Prefix 1.32.216.0/24, is normally announced by AS64050 BCPL-SG BGPNET Global ASN, SG.

But beginning at 2019-04-25 04:40:19, the same prefix (1.32.216.0/24) was also announced by ASN 4780.

This was detected by 114 BGPMon peers.

Expected

Start time: 2019-04-25 04:40:19 UTC

Expected prefix: 1.32.216.0/24

Expected ASN: 64050 (BCPL-SG BGPNET Global ASN, SG)

Event Details

Detected advertisement: 1.32.216.0/24

Detected Origin ASN 4780 (SEEDNET Digital United Inc., TW)

Detected AS Path 27257 6939 15412 4780

Detected by number of BGPMon peers: 114

01-00-00 Duration: 30d, 0m, 0s

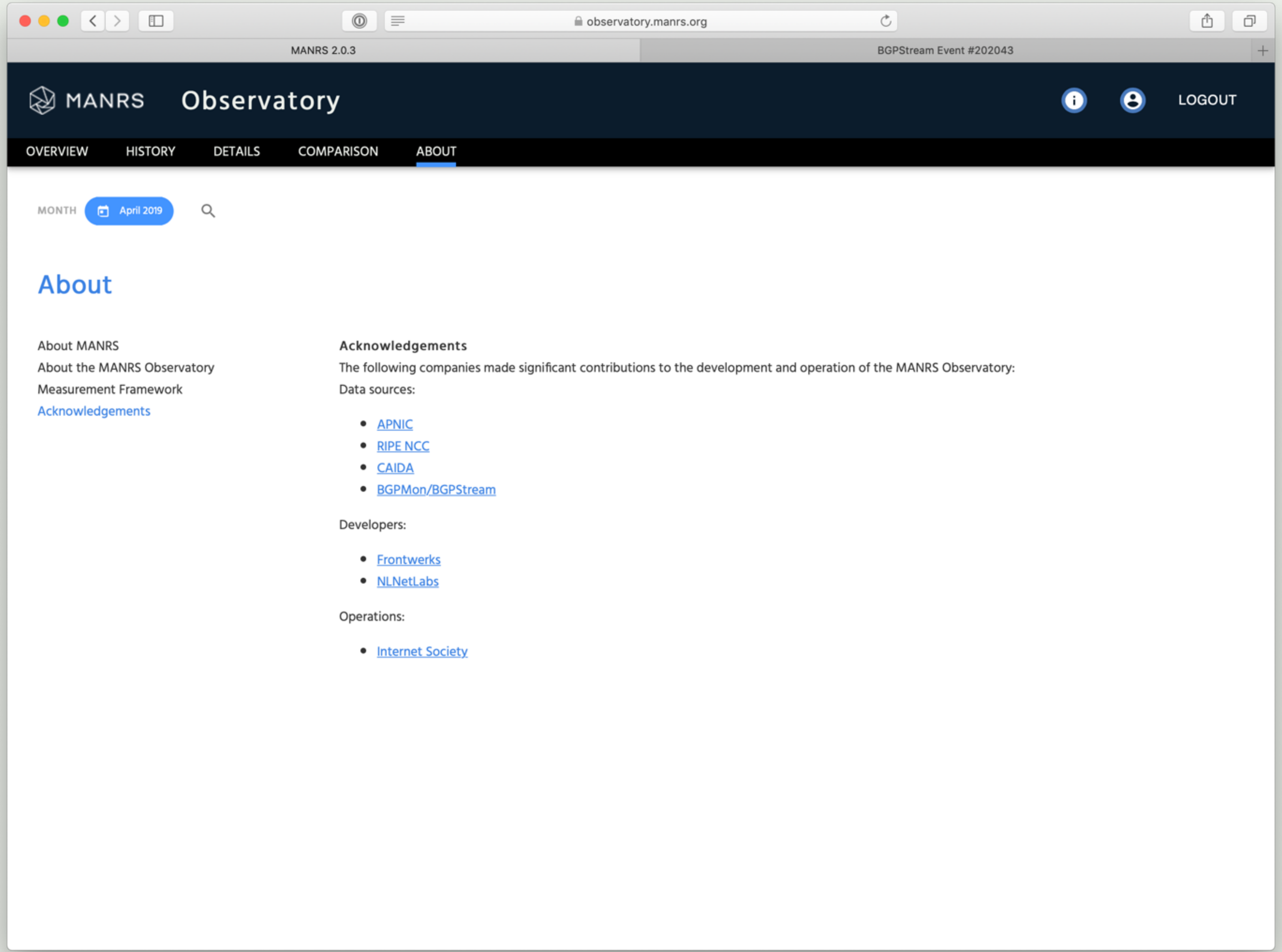
01-00-00 Duration: 5d, 19h, 19m, 41s

Prefix	Paths	Weight	Source	BGPstream EventId
1.32.216.0/24	27257 6939 15412 47...	1	bgpstream	202043

M3 - Bogon prefixes announced by the AS

Absolute: 31.0 Normalized: 17% Incident Count: 1

Incident Id: 1 Absolute: 31.0 Start Date: 01-04-2019 01-00-00 End Date: 01-05-2019 01-00-00 Duration: 30d, 0m, 0s



About

About MANRS
About the MANRS Observatory
Measurement Framework
Acknowledgements

Acknowledgements

The following companies made significant contributions to the development and operation of the MANRS Observatory:

Data sources:

- APNIC
- RIPE NCC
- CAIDA
- BGPMon/BGPStream

Developers:

- Frontwerks
- NLNetLabs

Operations:

- Internet Society

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

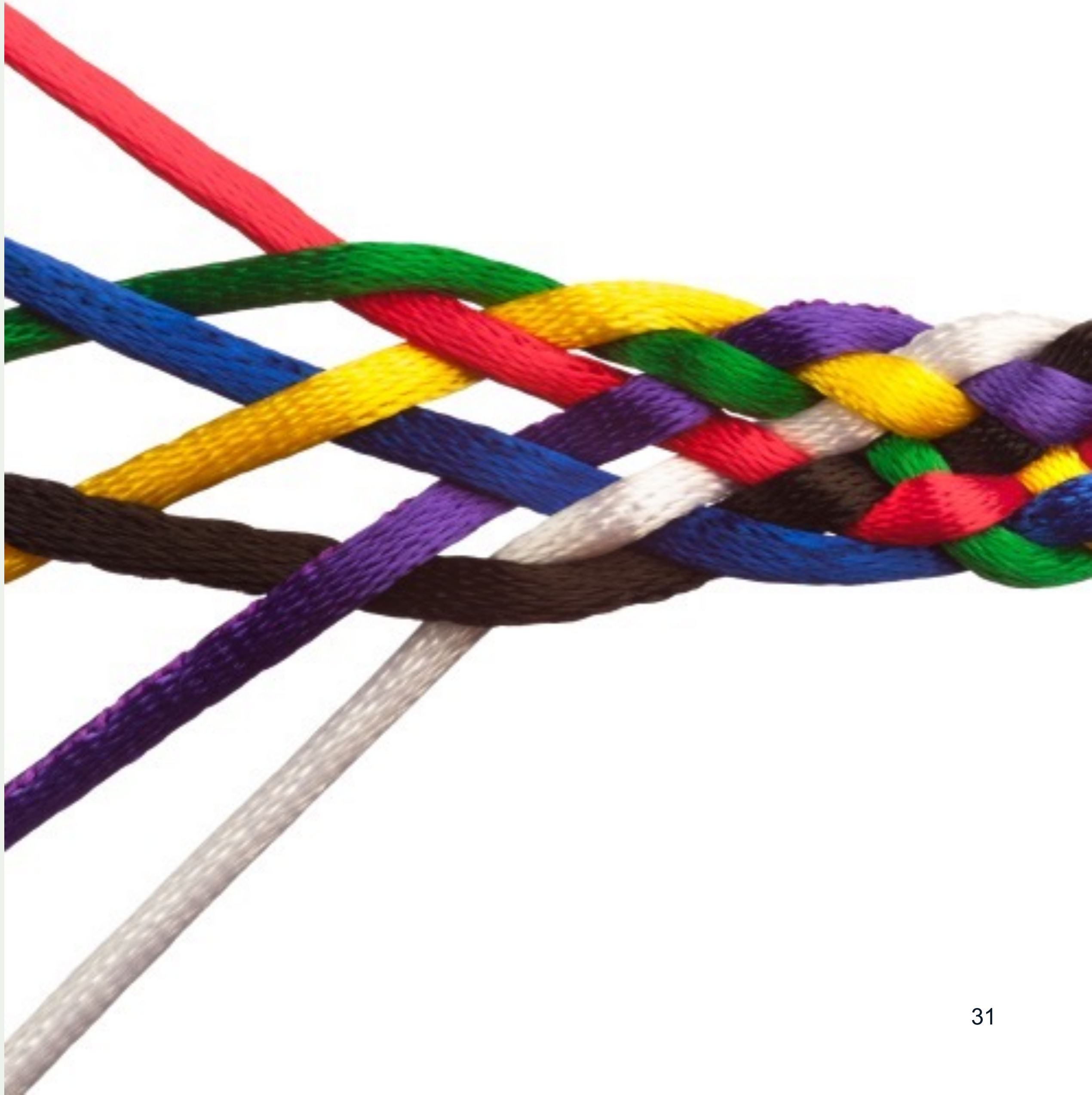
Join MANRS

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and request tests

Get Involved in the Community

- Participants support the initiative and implement the actions in their own networks and encouraging MANRS adoption
- Participants are engaged in substantive activities – developing MANRS requirements and guidance, assisting with capacity and awareness building activities



manrs.org

#ProtectTheCore

Thank you.

MANRS Observatory:

observatory.manrs.org