

30 November 2021
RSNOG 7

MANRS Update

Routing Security for the Internet



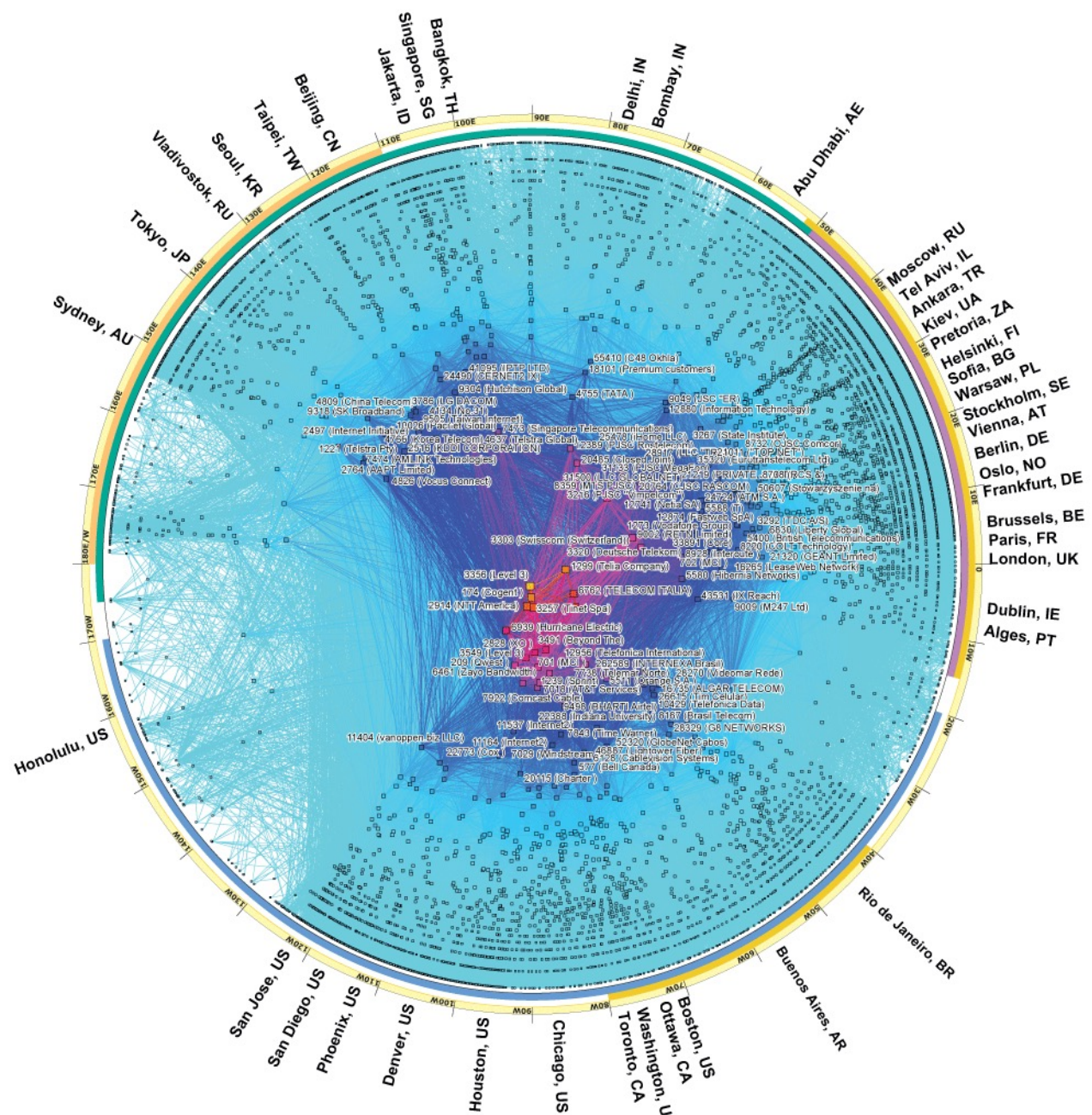
Kevin Meynell
Senior Manager, Technical & Operational Engagement
meynell@isoc.org

Global Routing System Overview

(as of 28 November 2021)

72,629 networks known as Autonomous Systems connected to Internet, each using a unique Autonomous System Number (ASN) for identification

902,184 advertised IP prefixes (routes)



The Routing Problem

The Border Gateway Protocol (BGP) used by the Internet routing system is based entirely on *unverified trust* between networks

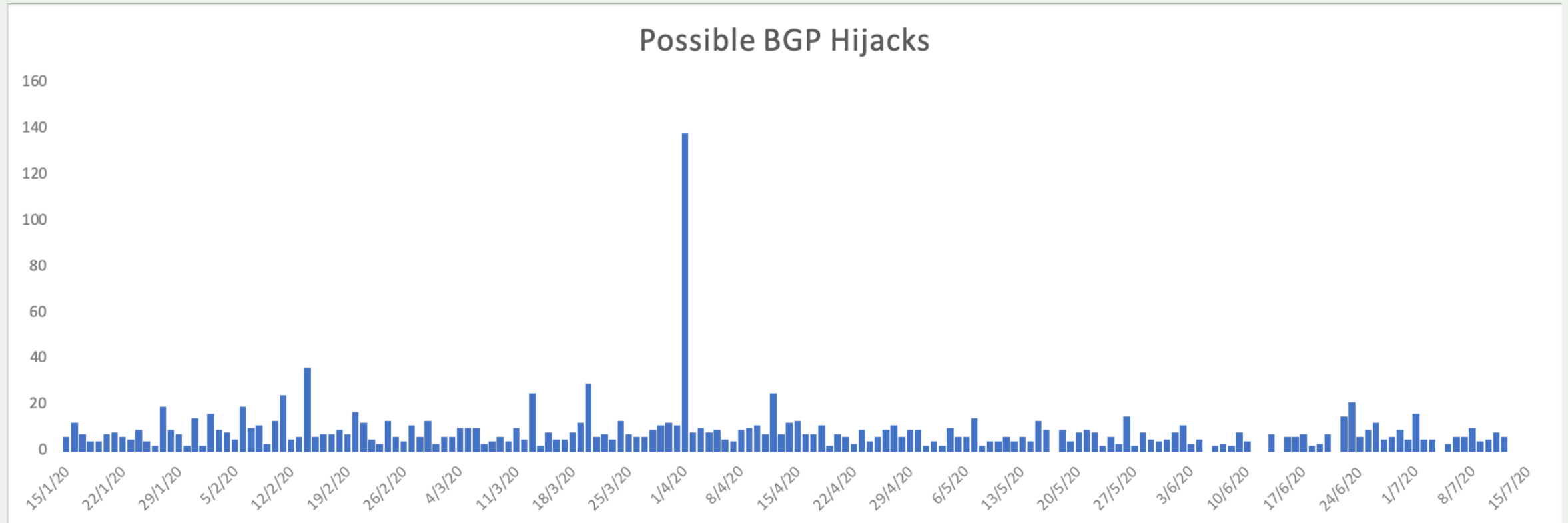
- No built-in validation that updates are legitimate
- Any network can announce any ASN or IP prefix
- Any network can claim to be another network



Routing Incidents Cause Real World Problems

Event	Explanation	Repercussions	Example
Route Leak	A network operator with multiple upstream providers announces to one upstream provider that it has a route to a destination through the other upstream provider. Often due to accidental misconfiguration.	Can be used for a MITM, including traffic inspection, modification and reconnaissance.	<i>June 2019. Verizon accepted incorrect routes from DQE Communications that diverted traffic destined for Cloudflare, Facebook & Amazon.</i>
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.	<i>The 2008 YouTube hijack April 2018 Amazon Route 53 hijack</i>
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	<i>March 1, 2018. Memcached 1.3Tb/s reflection-amplification attack reported by Akamai</i>

The routing system is constantly under attack – incidents every day



<http://bgpstream.com/>

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

4 no-cost programmes for Network Operators, IXPs, CDN/Cloud Providers & Vendors



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

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 conformance

Collates publicly available data sources

- BGPStream / CAIDA GRIP
- CIDR Report
- CAIDA Spoofer Database
- RIPE Database / RIPE Stats
- PeeringDB
- IRRs
- RPKI Validator

MONTH (PARTIAL) November 2021

USE GRIP DATA Info

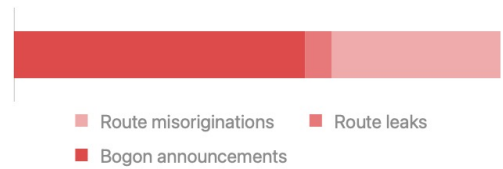
Overview

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

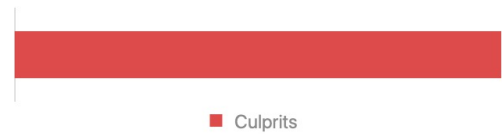
Incidents Info

Route misoriginations	390
Route leaks	61
Bogon announcements	673
Total	1,124



Culprits Info

Culprits 803



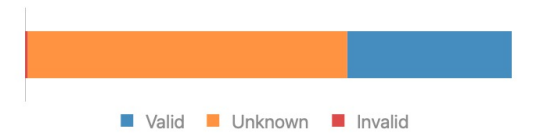
Routing completeness (IRR) Info

Unregistered	132,786	12.4%
Registered	936,453	87.6%



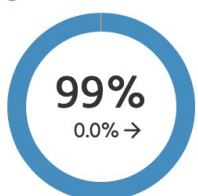
Routing completeness (RPKI) Info

Valid	361,400	33.8%
Unknown	702,471	65.7%
Invalid	5,368	0.5%

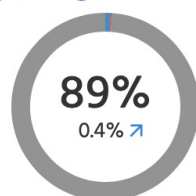


MANRS Readiness Info

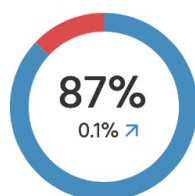
Filtering Info



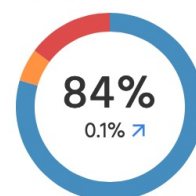
Anti-spoofing Info



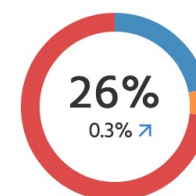
Coordination Info



Global Validation IRR Info



Global Validation RPKI Info



MONTH (PARTIAL)

November 2021

COUNTRY

- Serbia
- Croatia
- Slovenia
- Montenegro
- Macedonia (the former Yugoslav ...)
- Bosnia and Herzegovina
- Romania
- Bulgaria
- Albania
- Greece

USE GRIP DATA

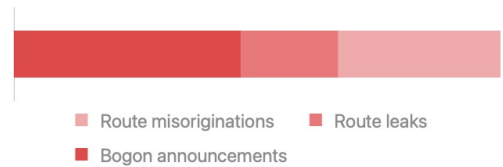
Overview

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

Route misoriginations	5
Route leaks	3
Bogon announcements	7
Total	15



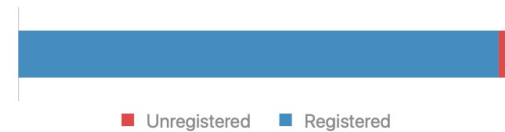
Culprits

Culprits 11



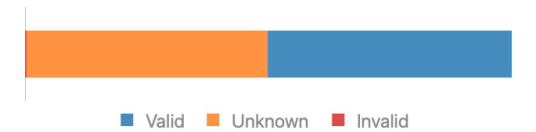
Routing completeness (IRR)

Unregistered	256	1.3%
Registered	19,282	98.7%



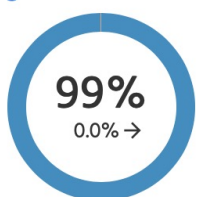
Routing completeness (RPKI)

Valid	9,815	50.2%
Unknown	9,673	49.5%
Invalid	50	0.3%

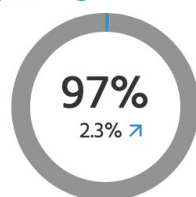


MANRS Readiness

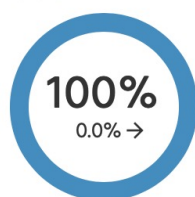
Filtering



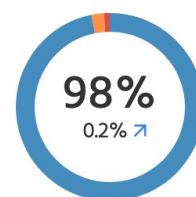
Anti-spoofing



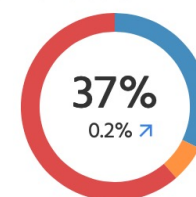
Coordination

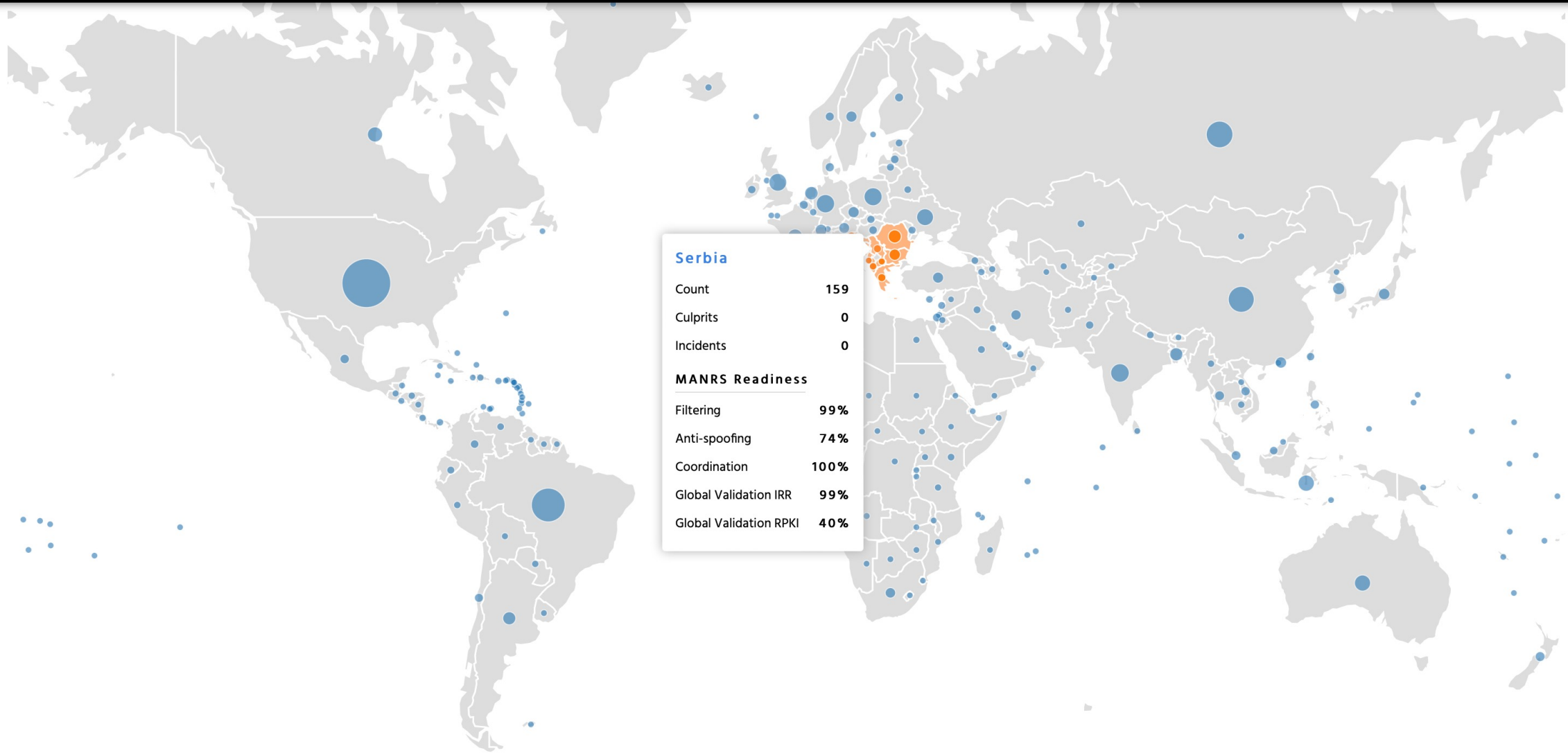


Global Validation IRR



Global Validation RPKI





Serbia

Count	159
Culprits	0
Incidents	0

MANRS Readiness

Filtering	99%
Anti-spoofing	74%
Coordination	100%
Global Validation IRR	99%
Global Validation RPKI	40%

MONTH (PARTIAL) November 2021 COUNTRY Serbia

USE GRIP DATA

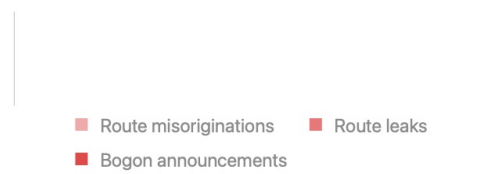
Overview

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

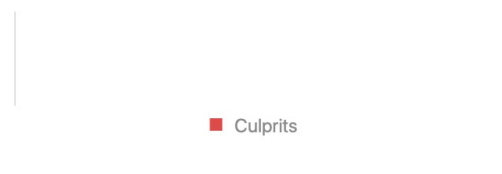
Incidents

Route misoriginations	0
Route leaks	0
Bogon announcements	0
Total	0



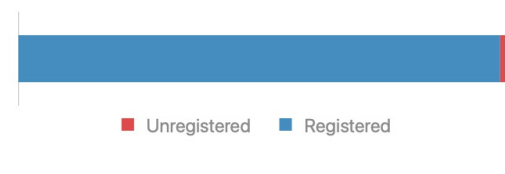
Culprits

Culprits	0
----------	---



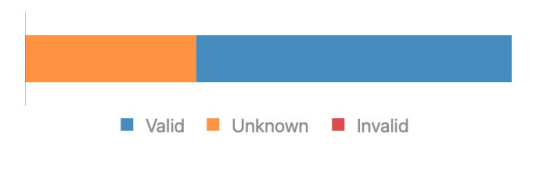
Routing completeness (IRR)

Unregistered	15	1.0%
Registered	1,415	99.0%



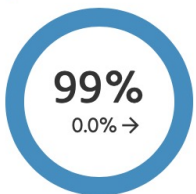
Routing completeness (RPKI)

Valid	928	64.9%
Unknown	501	35.0%
Invalid	1	0.1%

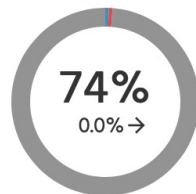


MANRS Readiness

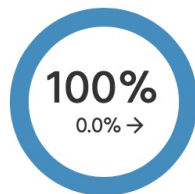
Filtering



Anti-spoofing



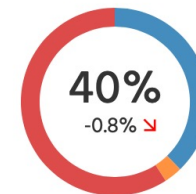
Coordination



Global Validation IRR



Global Validation RPKI



MONTH (PARTIAL) 📅 November 2021
🔍 COUNTRY Serbia

USE GRIP DATA ⓘ

Details

[Download data](#)

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

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

Result Limit: **100** | All


Total 159 [Previous](#) **1** [2](#) [Next](#)

Overview


ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering ^	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
13004	SOX - Serbian Open Exchange D	RS	Europe	Southern Europe	RIPE NCC	91%	-	100%	100%	100%
15958	CETIN_DOO_AS - CETIN Ltd. Bel	RS	Europe	Southern Europe	RIPE NCC	91%	-	100%	100%	0%
35573	MOJASUPERNOVA - Moja Super	RS	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	50%
205786	ZEPTEK - Zepter	RS	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	100%
43281	STEPANOVIC - Privredno drustv	RS	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	100%
31042	SERBIA-BROADBAND-AS - Serbi	RS	Europe	Southern Europe	RIPE NCC	100%	100%	100%	100%	92%
204618	YU-VIDEO - Zoran Marinkovic	RS	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	0%
41897	SAT-TRAKT-AS - Sat-Trakt D.O.O	RS	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	99%
200855	AIKBANKAASN - AIK banka A.D.	RS	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	0%
207068	UZZPPO - Uprava za zajednicke	RS	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	0%
201278	RTV-AS - Javna Medijska Ustanc	RS	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	100%


M2C (GRIP) - Route hijack by a direct customer [↗](#)

Absolute: **2.5** Normalized: **73%** Incident Count: **3**

Incident Id: 1 Absolute: 1.0 Start Date: 01-11-2021 11-00-00 End Date: 02-11-2021 01-15-00 Duration: 2h, 15m, 0s  ^

Incident Id	Start Time	End Time	Duration	Prefix	Paths	Weight	Source	Source event
1	2021-11-01 23:00:00	2021-11-02 01:15:00	2h, 15m, 0s	193.108.17.0/24	199524 6453 3257...	1	grip	moas-1635807600-286_3257_
1	2021-11-01 23:00:00	2021-11-02 01:15:00	2h, 15m, 0s	193.108.17.0/24	199524 6453 3257...	1	grip	moas-1635807600-286_3257_
1	2021-11-01 23:00:00	2021-11-02 01:15:00	2h, 15m, 0s	193.108.17.0/24	199524 6453 3257...	1	grip	moas-1635807600-286_3257_

Incident Id: 2 Absolute: 1.0 Start Date: 02-11-2021 09-55-00 End Date: 02-11-2021 10-55-00 Duration: 1h, 0m, 0s  v

Incident Id: 3 Absolute: 0.5 Start Date: 09-11-2021 12-20-00 End Date: 09-11-2021 12-30-00 Duration: 10m, 0s  v

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

M4 - Bogon ASNs announced by the AS [↗](#)



M4C - Bogon ASNs propagated by the AS i



Absolute: **27.0** Normalized: **20%** Incident Count: **1**

Incident Id: 1 Absolute: 27.0 Start Date: 01-11-2021 12-00-00 End Date: 27-11-2021 12-00-00 Duration: 26d, 0m, 0s ^

Incident Id	Start Time	End Time	Paths	Weight	Source	ASN
1	2021-11-01 00:00:00	2021-11-27 00:00:00	Paths	1	cidr	65200
1	2021-11-01 00:00:00	2021-11-27 00:00:00	Paths	1	cidr	65500
1	2021-11-01 00:00:00	2021-11-27 00:00:00	Paths	1	cidr	65502

Download metrics data

M5 - Spoofing IP blocks i



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

Has records	Spoofed prefixes
False	-

Download metrics data

M8 - Contact registration (RIR, IRR, PeeringDB) i



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

Last changed	Has contact info
--------------	------------------

M7IRR - Registered routes (% of routes registered) i



Absolute: **8%** Normalized: **93%** Incident Count: -

Number of prefixes	Number of unregistered prefixes	Unregistered prefixes	Last changed
40	3	91.150.64.0/18...	2021-11-26

Unregistered prefixes

[Download metrics data](#)

- 91.150.64.0/18
- 178.220.0.0/15
- 91.150.91.0/24



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

Absolute: **18%** Normalized: **83%** Incident Count: -

Number of prefixes	Number of unknown prefixes	Routing consistency	Last changed
40	7	Routing consistency	2021-11-26

[Download metrics data](#)

M7RPKIN - Invalid routes i



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

Number of prefixes	Number of invalid prefixes	Invalid prefixes
40	0	-

[Download metrics data](#)

MANRS Participation

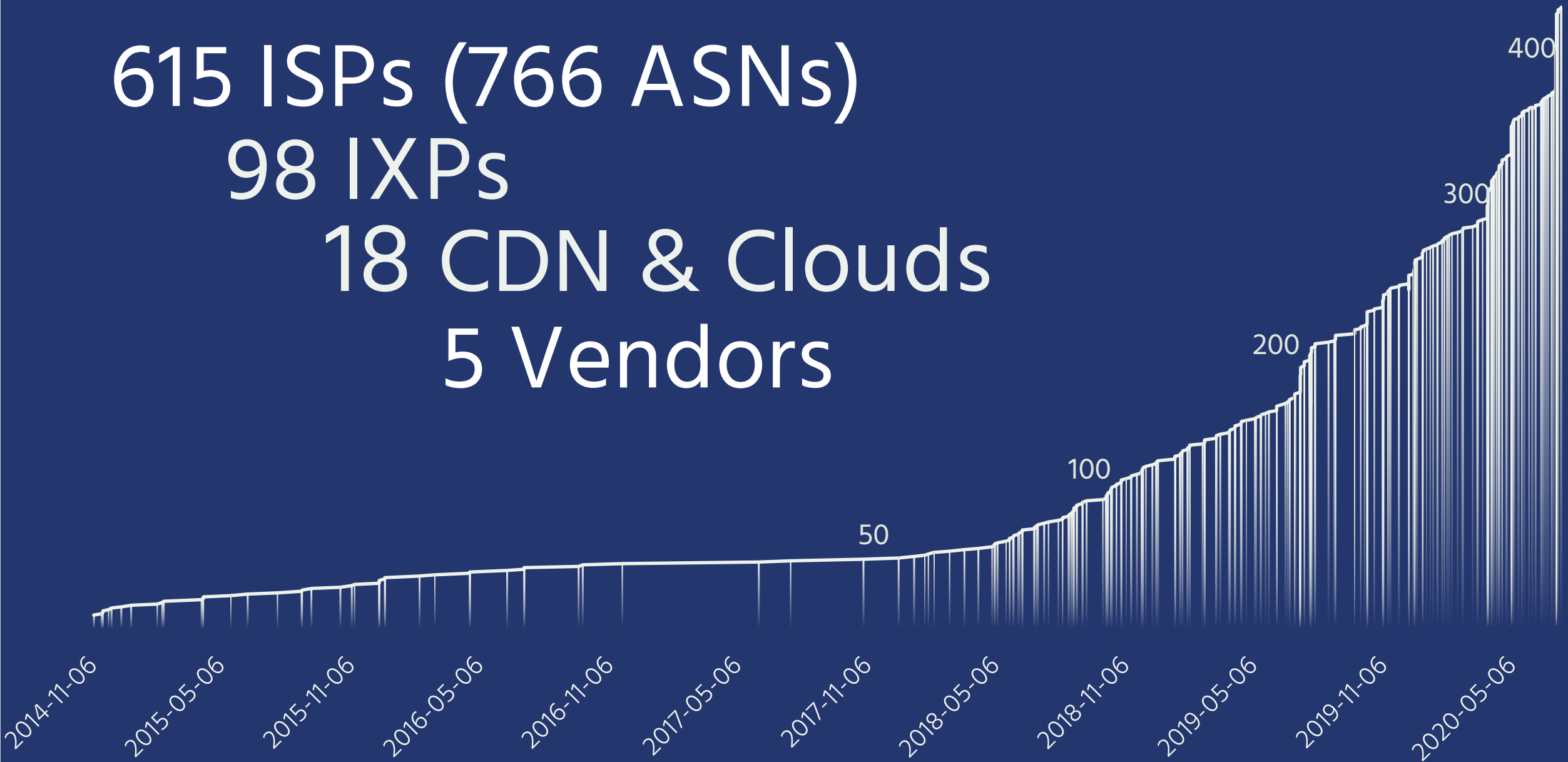


615 ISPs (766 ASNs)

98 IXPs

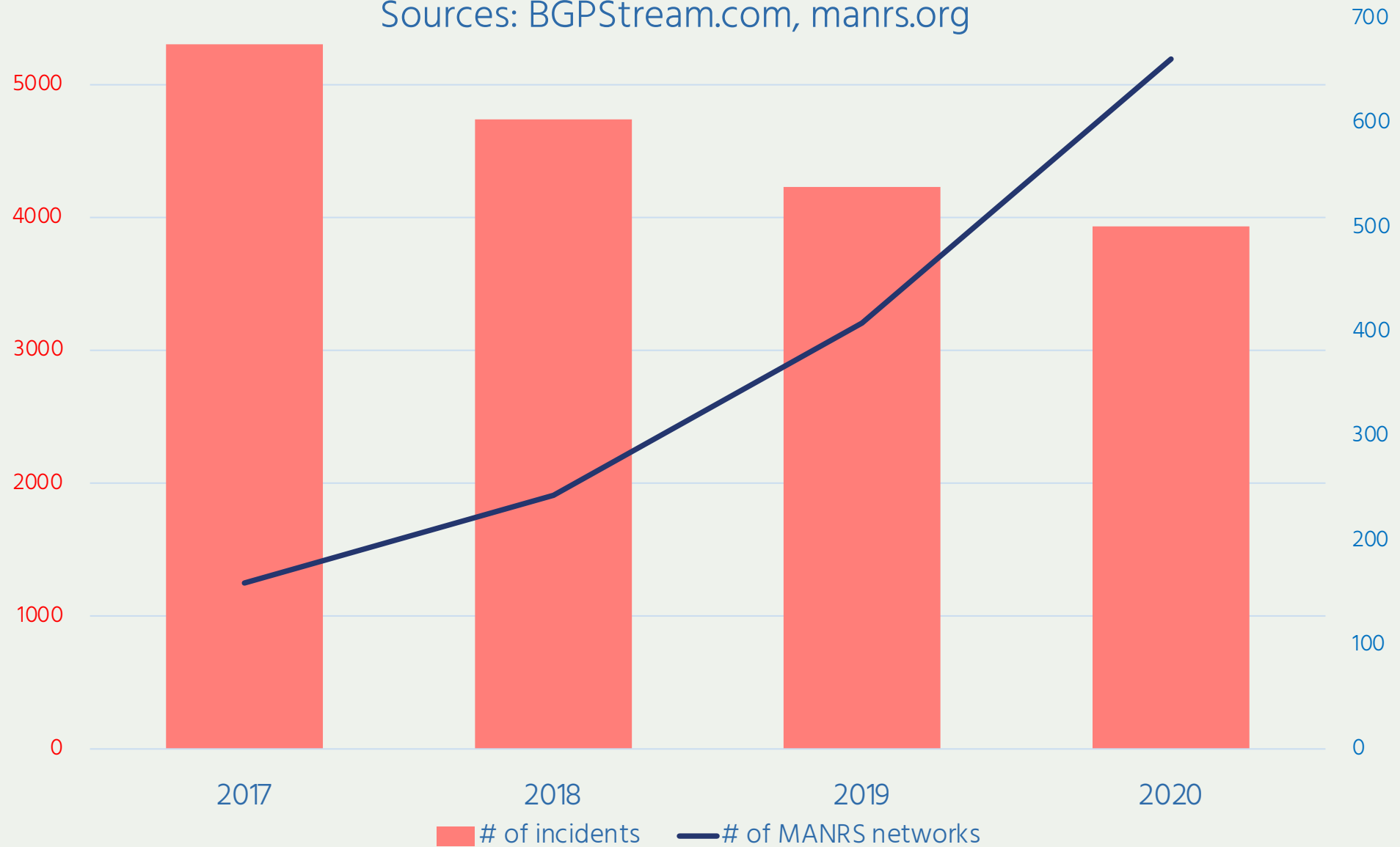
18 CDN & Clouds

5 Vendors



Impact of implementing routing security measures

Sources: BGPStream.com, manrs.org



Join the MANRS Community

Visit <https://www.manrs.org>

- Fill out the sign up form with as much detail as possible
- We will create MANRS Observatory account for your network

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

