15 April 2021
UKNOF 47

Observing your MANRS for a more secure Internet

Introducing the MANRS Observatory

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

Internet Society © 1992–2021

Background

There are ~71,000 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

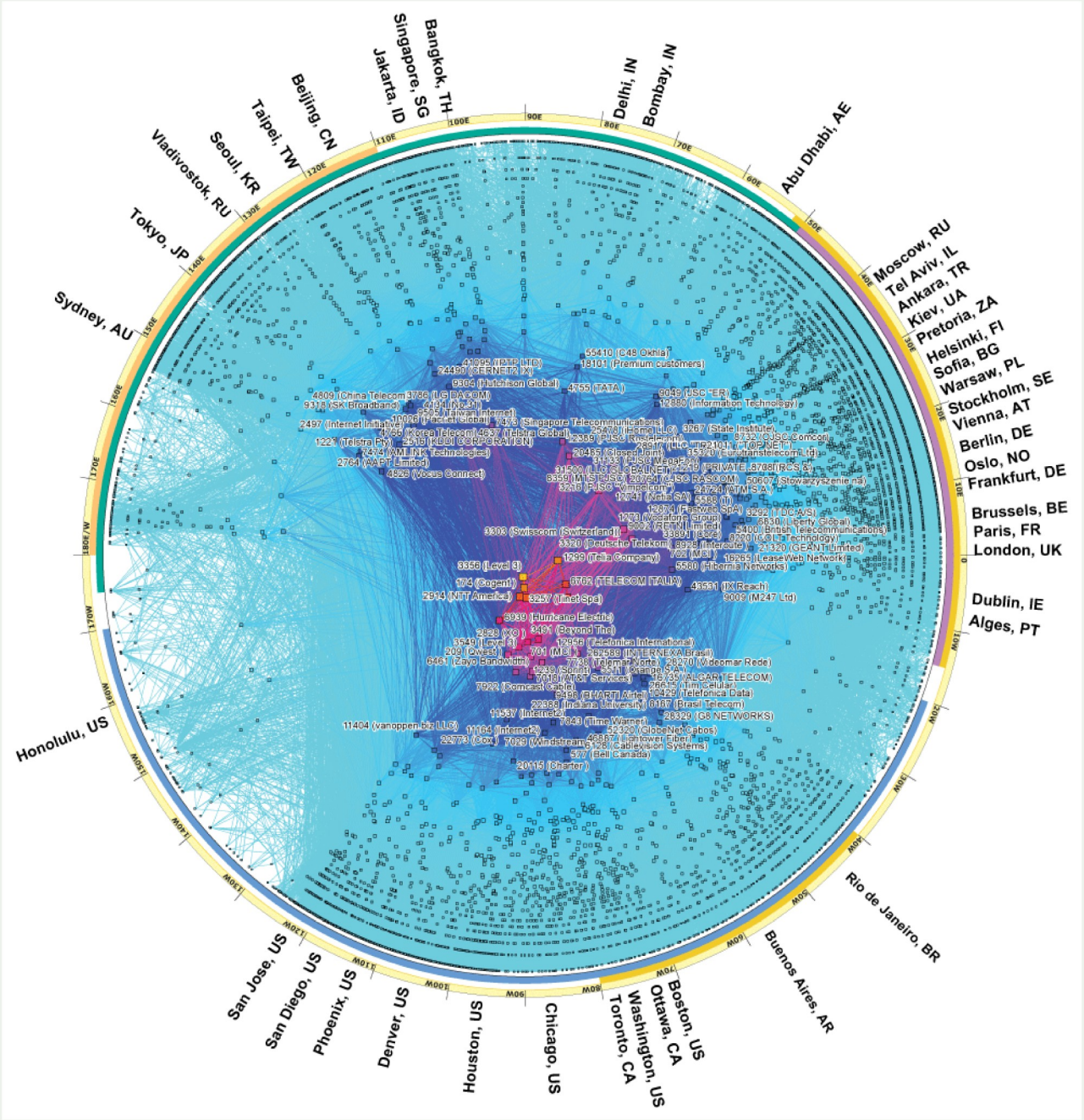
The Routing Problem

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



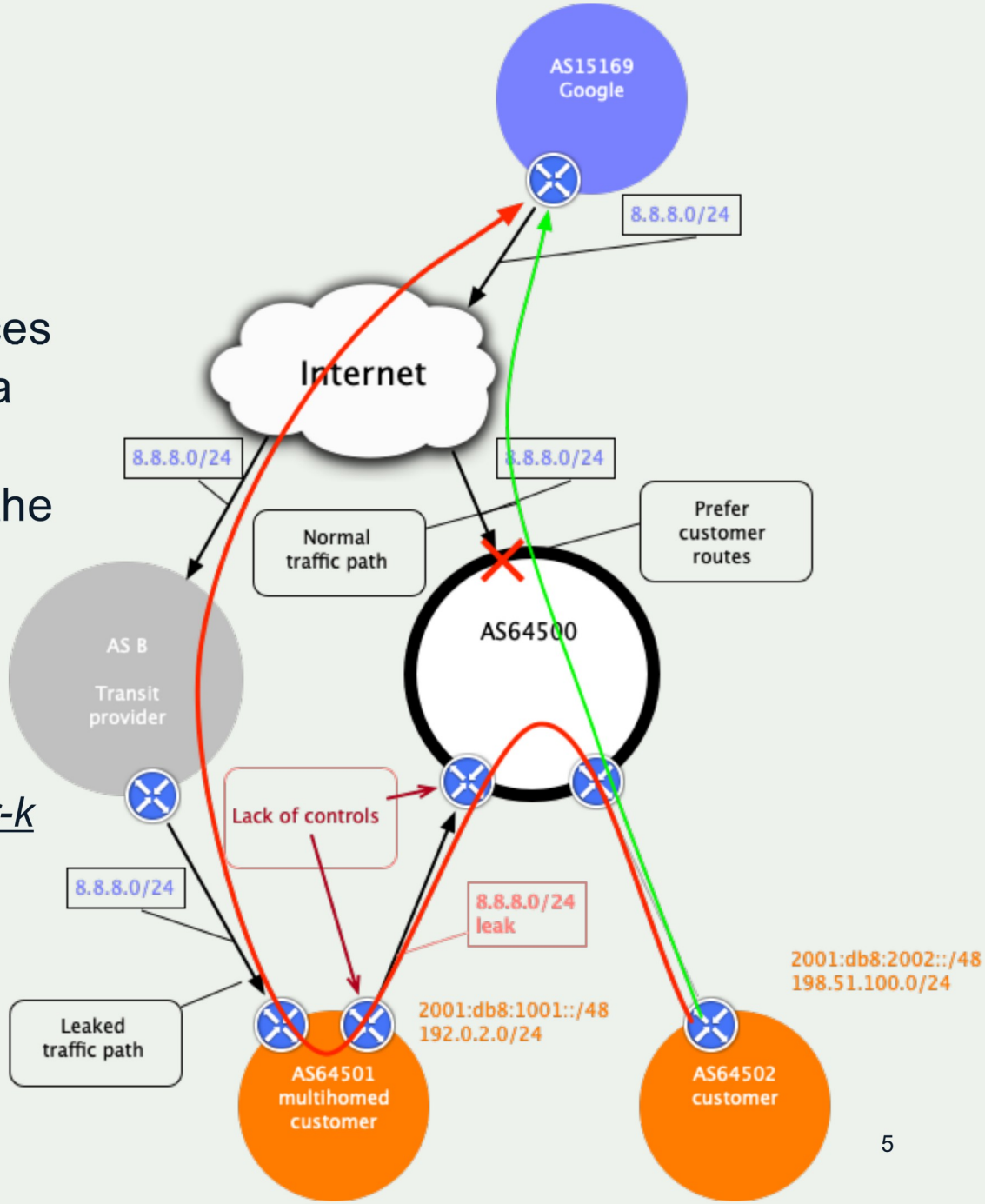
MANRS

https://www.caida.org/

Route Leak

A Route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers. With one sending traffic now through it to get to the other.

Example: *June 2019. Allegheny leaked routes from another provider to Verizon, causing significant outage.* *https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/*

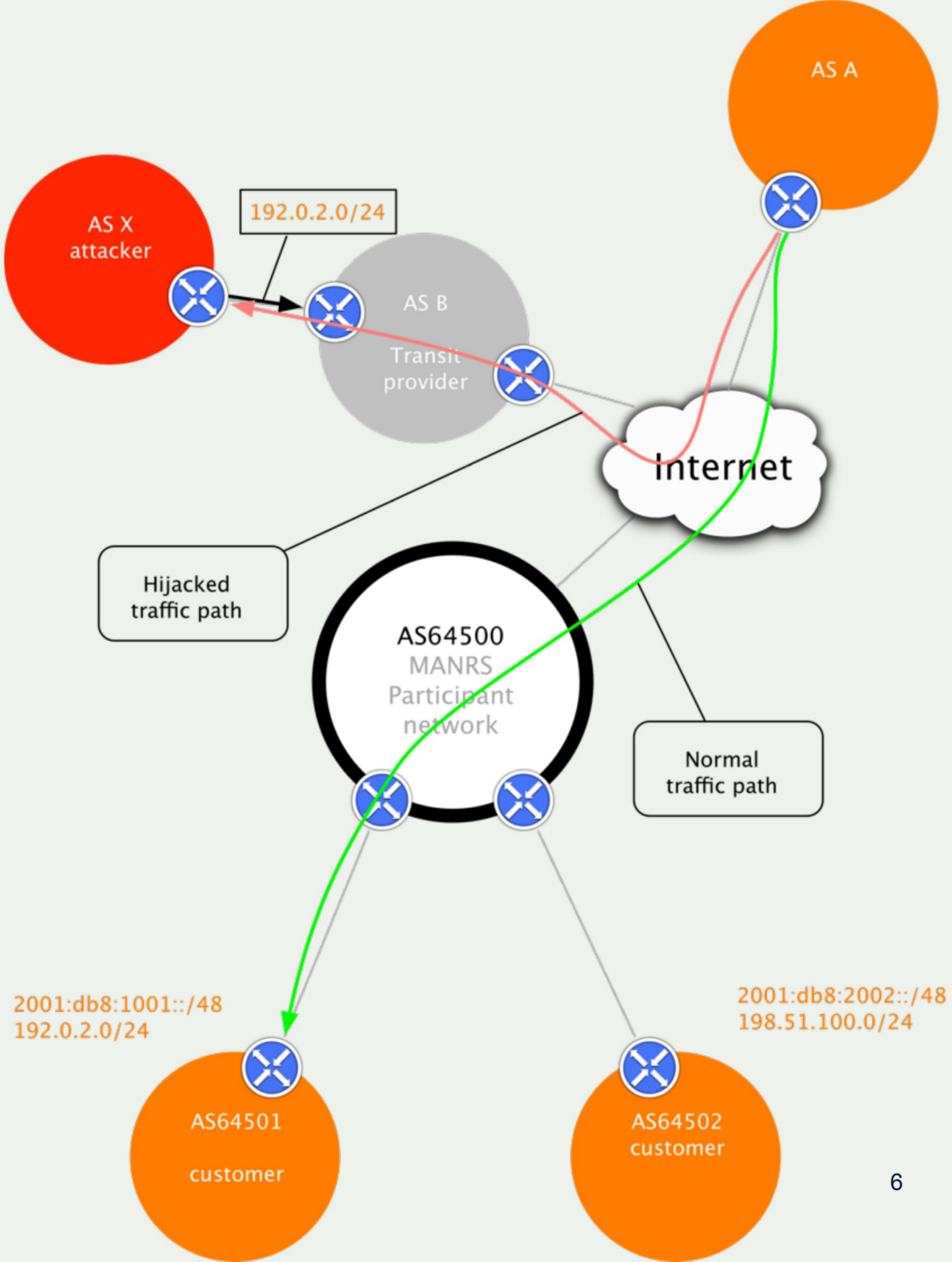


MANRS

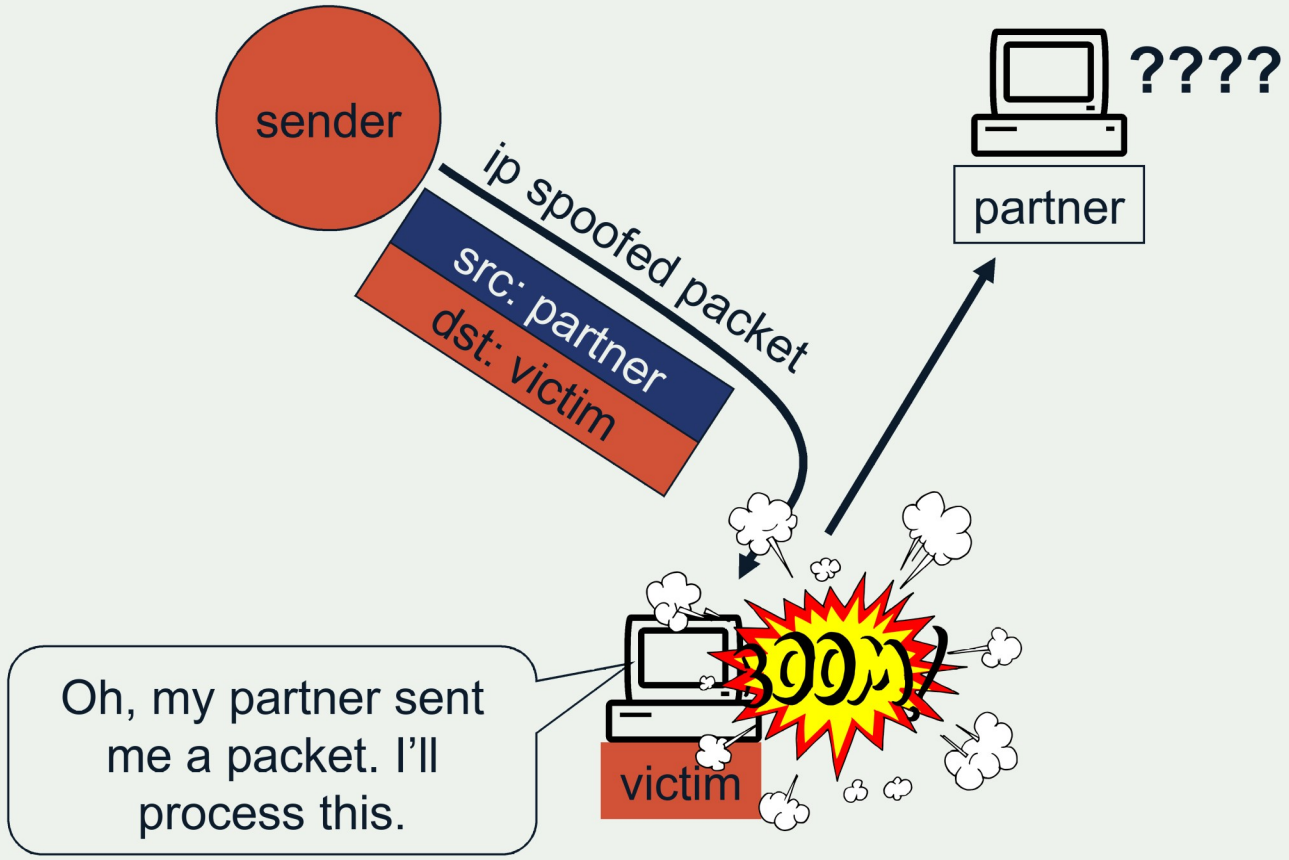
Route Hijacking

Route hijacking, also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that the network is their client. This routes traffic to the attacker, while the victim suffers an outage.

Example: *The 2008 YouTube hijack; an attempt to block Youtube through route hijacking led to much of the traffic to Youtube being dropped around the world (* *https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study* *)*

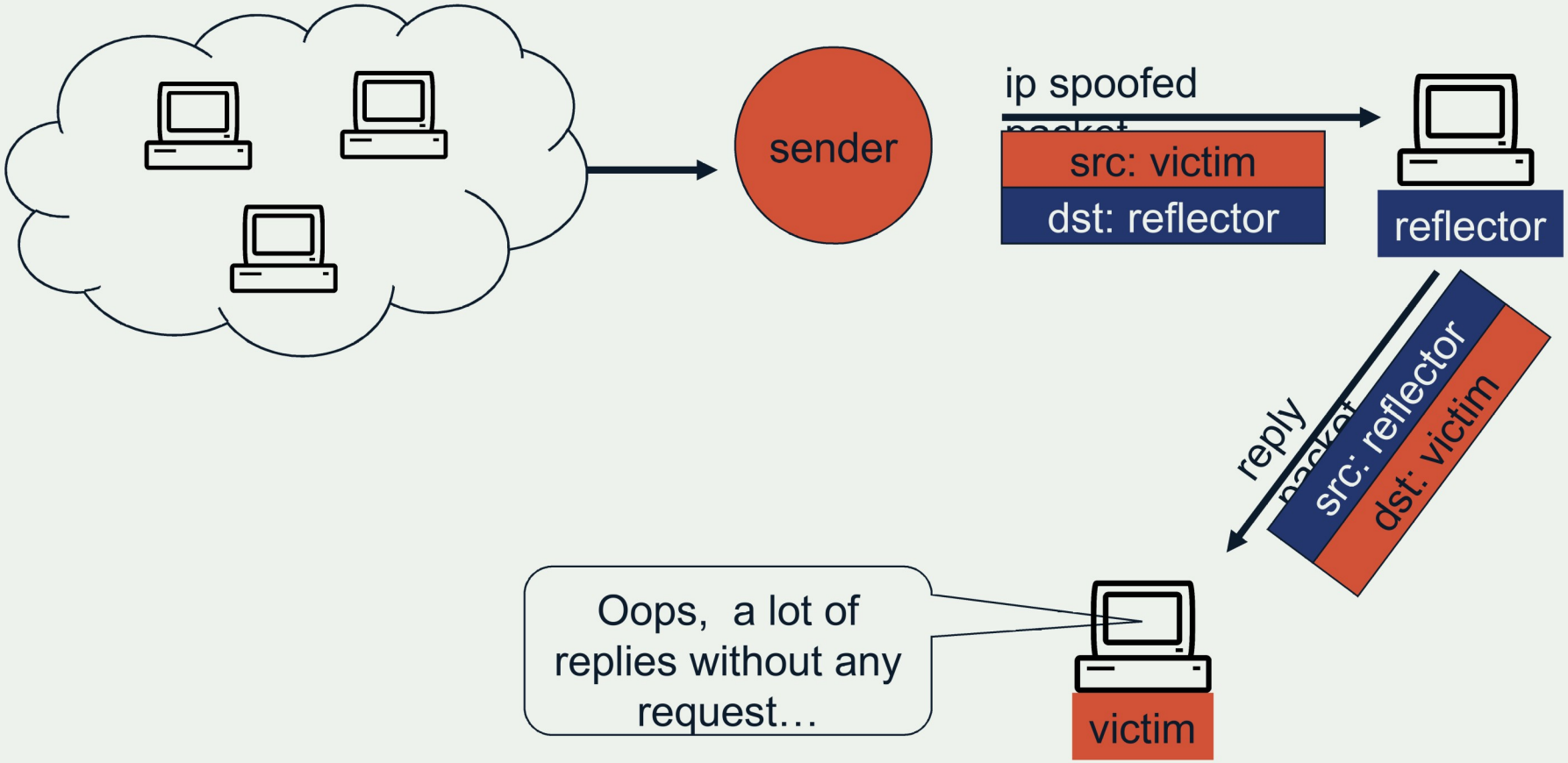


IP Spoofing: Impersonation

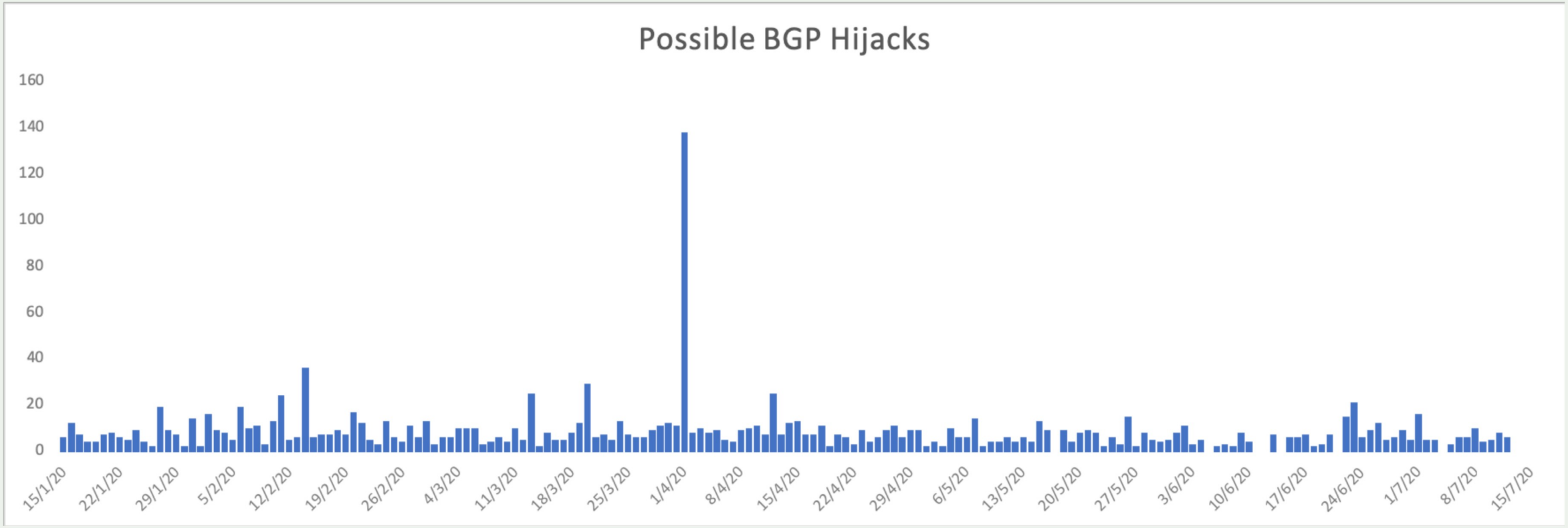


MANRS

IP Spoofing: Reflection



The routing system is constantly under attack – incidents every day



http://bgpstream.com/

MANRS

MANRS: Mutually Assured Norms for Routing Security

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

Three programmes for Network Operators, IXPs & CDN/Cloud Providers

What are we looking to achieve?

- Everyone benefits from improved Routing Security
- Encourage networks to implement routing security best practices + raise customer awareness so they demand this
- Help networks to easily identify and address problems with customers or peers
- The more operators that apply MANRS actions, the fewer incidents there will be, and the less damage they can do
- Develop a database of routing incidents to demonstrate where problems exist + whether things improve over time in response to better routing security measures.
- Build a self-regulating community of security-minded network operators committed to making the global routing infrastructure more robust and secure

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 1 April 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

MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH (PARTIAL) March 2021

Overview

State of Routing Security

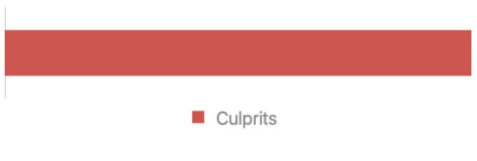
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
967	Route misoriginations	92
	Route leaks	62
	Bogon announcements	813

Culprits

Total		
778	Culprits	778

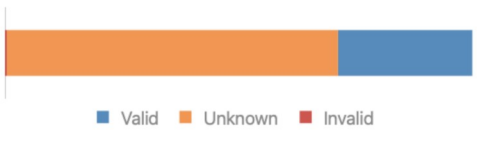


Routing completeness (IRR)

Total		
100%	Unregistered	13%
	Registered	87%

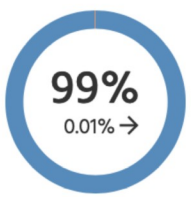
Routing completeness (RPKI)

Total		
99%	Valid	29%
	Unknown	71%
	Invalid	1%

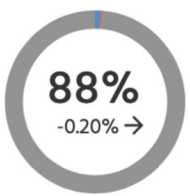


MANRS Readiness

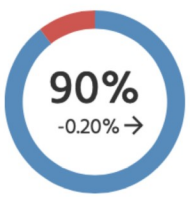
Filtering



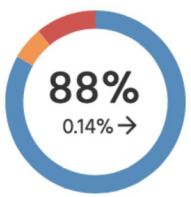
Anti-spoofing



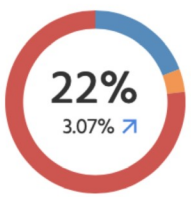
Coordination



Global Validation IRR



Global Validation RPKI



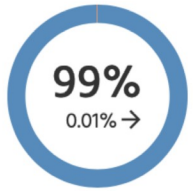
Ready Aspiring Lagging No Data Available

MANRS Observatory

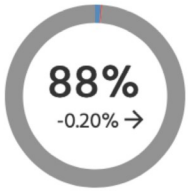
OVERVIEW HISTORY COMPARISON ABOUT

MANRS Readiness

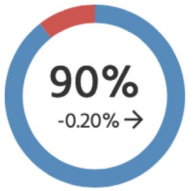
Filtering



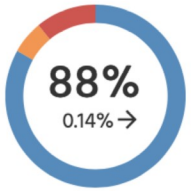
Anti-spoofing



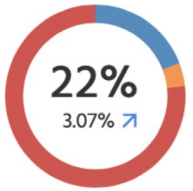
Coordination



Global Validation IRR



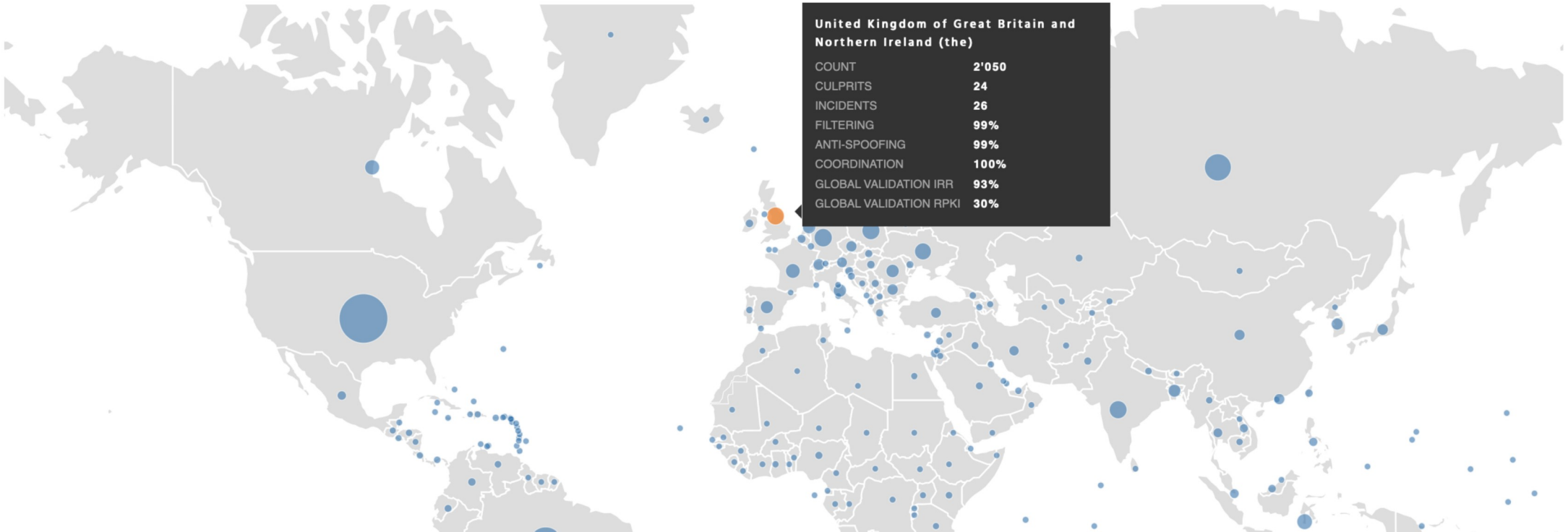
Global Validation RPKI



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) March 2021 RIR REGIONS RIPE NCC

Overview

State of Routing Security

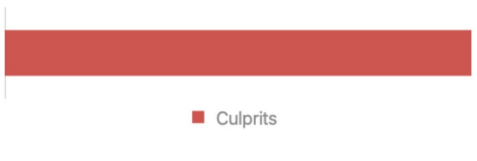
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
196	Route misoriginations	38
	Route leaks	18
	Bogon announcements	140

Culprits

Total		
177	Culprits	177

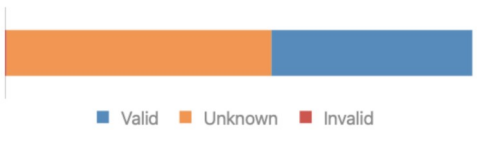


Routing completeness (IRR)

Total		
100%	Unregistered	6%
	Registered	94%

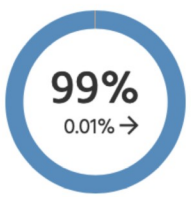
Routing completeness (RPKI)

Total		
100%	Valid	43%
	Unknown	57%
	Invalid	1%

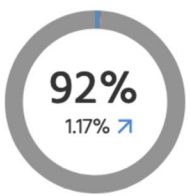


MANRS Readiness

Filtering

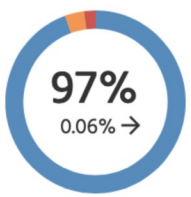


Anti-spoofing

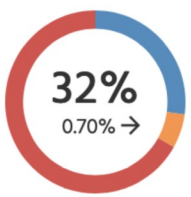


Coordination

Global Validation IRR



Global Validation RPKI



Ready Aspiring Lagging No Data Available

MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH (PARTIAL) March 2021 COUNTRY United Kingdom of Great Britain an...

Overview

State of Routing Security

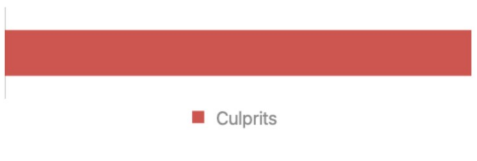
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
26	Route misoriginations	5
	Route leaks	1
	Bogon announcements	20

Culprits

Total		
24	Culprits	24

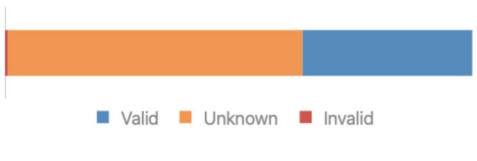


Routing completeness (IRR)

Total		
100%	Unregistered	4%
	Registered	96%

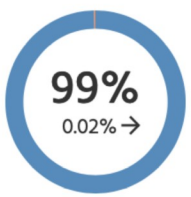
Routing completeness (RPKI)

Total		
100%	Valid	36%
	Unknown	63%
	Invalid	1%

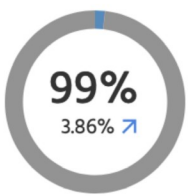


MANRS Readiness

Filtering

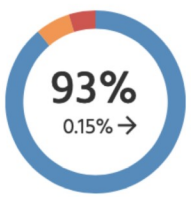


Anti-spoofing

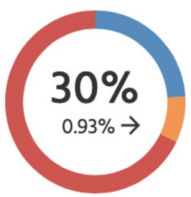


Coordination

Global Validation IRR



Global Validation RPKI



Ready Aspiring Lagging No Data Available

MONTH (PARTIAL) March 2021 COUNTRY United Kingdom of Great Britain an...

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
786	JANET - Jisc Services Limited	GB	Europe	Northern Europe	RIPE NCC	100%	-	100%	99%	5%
2129	HP-EUROPE-AS-TRADE - EntServ	GB	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	0%
2589	WANSTOR - Wanstor Ltd	GB	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	100%
2818	BBC	GB	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	0%
2856	BT-UK-AS - British Telecommunic	GB	Europe	Northern Europe	RIPE NCC	91%	100%	100%	93%	25%
3170	VELOXSERV - Etheroute Ltd	GB	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	69%
3206	AFB-AS - AF Blakemore & Son Ltc	GB	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	0%
3213	BOGONS-ASN - Bogons Ltd	GB	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	0%
3223	VOXILITY - Voxility LLP	GB	Europe	Northern Europe	RIPE NCC	80%	-	100%	99%	65%
3252	FBRX-AS - Fiberax Networking&C	GB	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	0%
3300	BT - British Telecommunications F	GB	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	0%
5089	NTL - Virgin Media Limited	GB	Europe	Northern Europe	RIPE NCC	100%	100%	100%	95%	68%
5378	Vodafone Limited	GB	Europe	Northern Europe	RIPE NCC	100%	100%	100%	100%	0%
5400	BT - British Telecommunications F	GB	Europe	Northern Europe	RIPE NCC	96%	-	100%	100%	35%
5413	AS5413 - Daisy Communications L	GB	Europe	Northern Europe	RIPE NCC	70%	-	100%	100%	8%

MONTH (PARTIAL) March 2021 COUNTRY United Kingdom of Great Britain an...

Details - ASN

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: **5.0** Normalized: **60%** Incident Count: **1**

Incident Id: 1 Absolute: 5.0 Start Date: 22-03-2021 05-10-32 End Date: 27-03-2021 12-00-00 Duration: 4d, 6h, 49m, 28s

Incident Id	Start Time	End Time	Duration	Prefix	Paths	Weight	Source	BGPstream EventId
1	2021-03-22 17:10:32	2021-03-27 00:00:00	4d, 6h, 49m, 28s	51.230.16.0/20	31463 50300 2856 62341...	1	bgpstream	270621
1	2021-03-22 17:10:32	2021-03-27 00:00:00	4d, 6h, 49m, 28s	51.230.112.0/20	49463 13193 34659 1555...	1	bgpstream	270620

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

Incident Id: 1 Absolute: 3.0 Start Date: 10-03-2021 12-00-00 End Date: 12-03-2021 12-00-00 Duration: 2d, 0m, 0s

Incident Id	Start Time	End Time	Paths	Weight	Source	ASN
1	2021-03-10 00:00:00	2021-03-12 00:00:00	Paths	1	cidr	394583

Download metrics data

M4C - Bogon ASNs propagated by the AS

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

M5 - Spoofing IP blocks

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

Has records	Spoofed prefixes
True	-

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: **7%** Normalized: **93%** Incident Count: **-**

Number of prefixes	Number of unregistered prefixes	Unregistered prefixes	Checked on
275	19	147.182.214.0/24...	2021-03-26

Download metrics data

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

Absolute: **75%** Normalized: **25%** Incident Count: **-**

Number of prefixes	Number of unknown prefixes	Routing consistency	Checked on
275	205	Routing consistency	2021-03-26

Download metrics data

M7RPKIN - Invalid routes

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

Number of prefixes	Number of invalid prefixes	Invalid prefixes
275	0	-

Download metrics data

Unregistered prefixes

147.182.214.0/24
2a02:ee80:4176::/47
141.92.8.0/22
91.142.128.0/24
194.32.162.0/24
82.132.144.0/20
194.93.227.0/24
82.132.188.0/22
185.128.205.0/24
85.235.107.0/24
138.108.94.0/24
212.148.1.0/24
193.38.192.0/19
194.62.7.0/24
192.56.233.0/24
141.92.12.0/22
91.227.78.0/24
103.91.117.0/24
170.136.117.0/24

MANRS Dashboard

LOGOUT

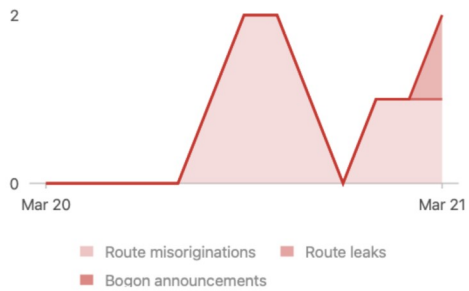
OVERVIEW HISTORY DETAILS COMPARISON ABOUT ADMIN

MONTH (PARTIAL) March 2021 ASN valory

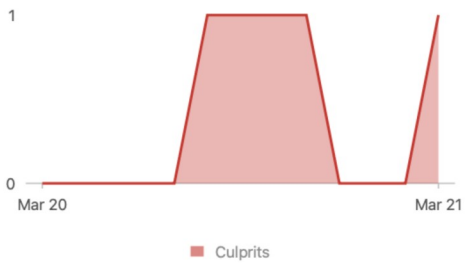
History

March 2020 - March 2021

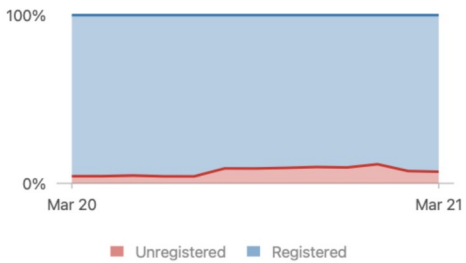
Incidents



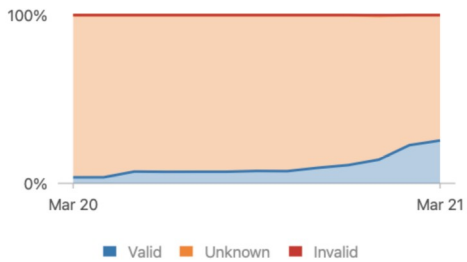
Culprits



Routing completeness (IRR)



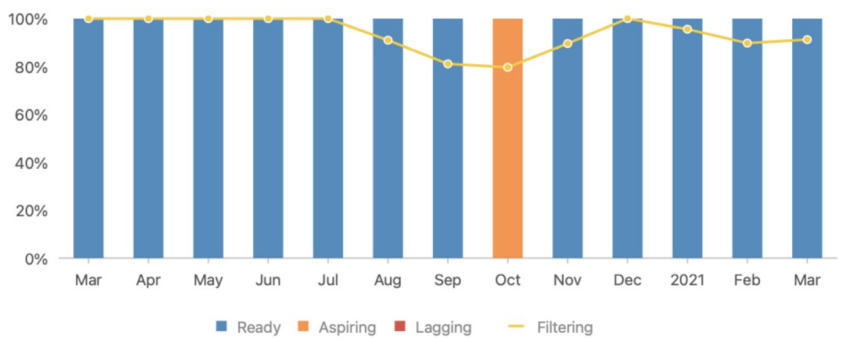
Routing completeness (RPKI)



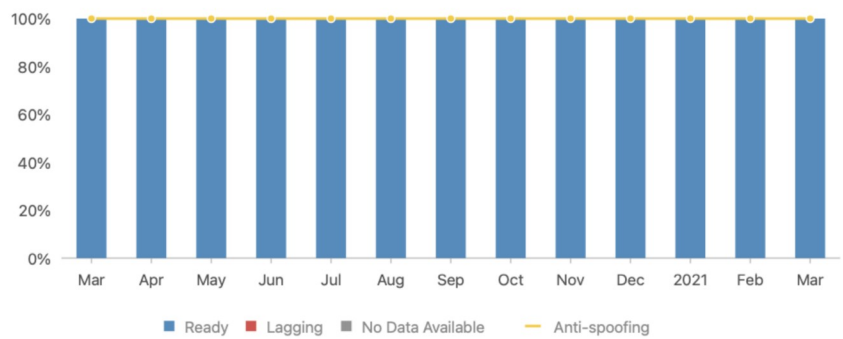
MANRS Readiness

Overall | Metrics

Filtering



Anti-spoofing



MANRS Observatory Access

Publicly launched in August 2019

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
- 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.

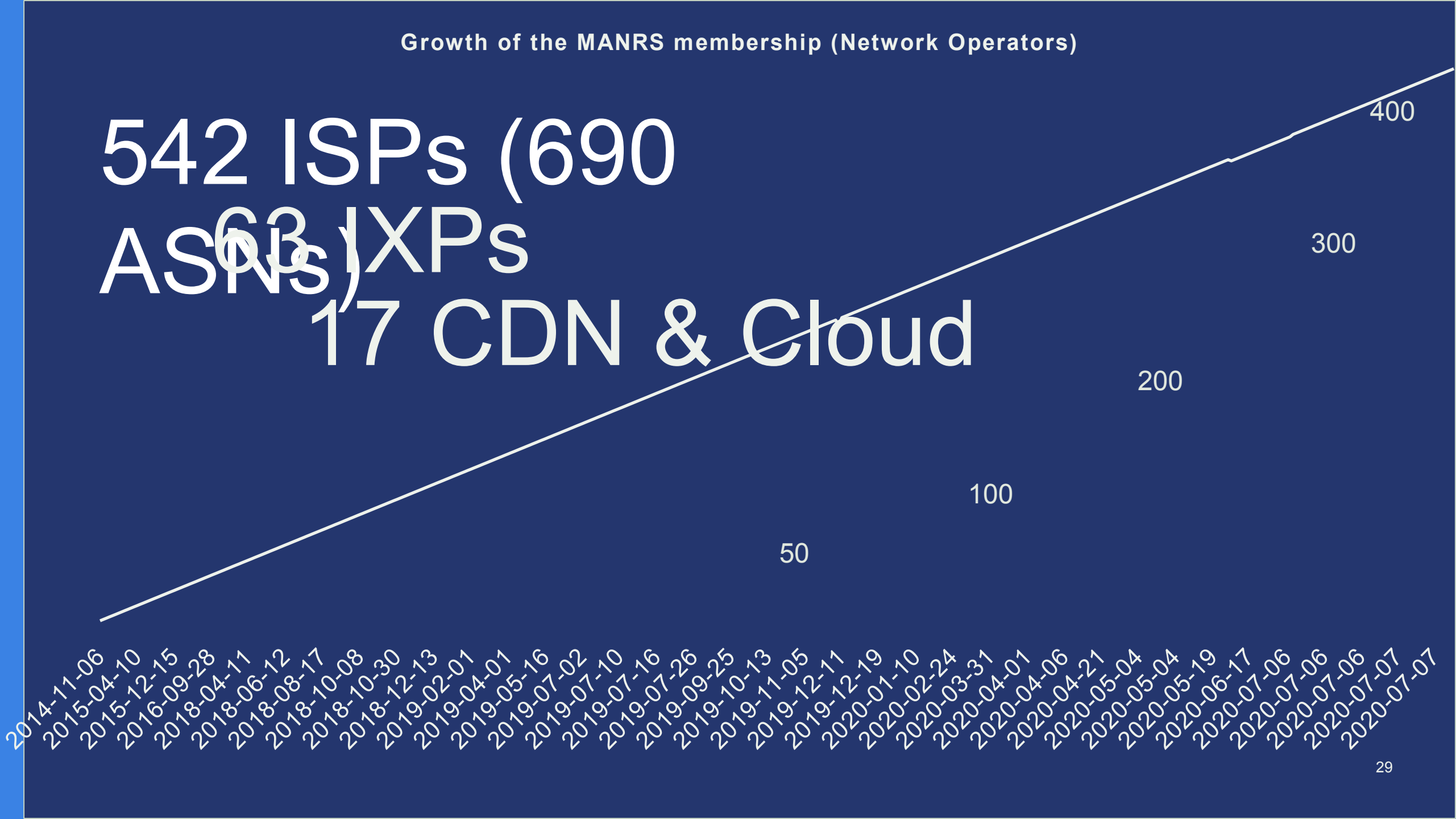
- Based on Best Current Operational Practices deployed by network operators around the world
- Recognition from the RIPE community by being published as RIPE-706
- https://www.manrs.org/bcop/

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

MANRS

Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS Achievements & Impacts


Growth of the MANRS membership (Network Operators)
542 ISPs (690 ASNs)
63 IXPs
17 CDN & Cloud
400
300
200
100
50
2014-11-06
2015-04-10
2015-12-15
2016-09-28
2018-04-11
2018-06-12
2018-08-17
2018-10-08
2018-10-30
2018-12-13
2019-02-01
2019-04-01
2019-05-16
2019-07-02
2019-07-10
2019-07-16
2019-07-26
2019-09-25
2019-10-13
2019-11-05
2019-12-11
2019-12-19
2020-01-10
2020-02-24
2020-03-31
2020-04-01
2020-04-06
2020-04-21
2020-05-04
2020-05-04
2020-05-19
2020-06-17
2020-07-06
2020-07-06
2020-07-06
2020-07-07
2020-07-07

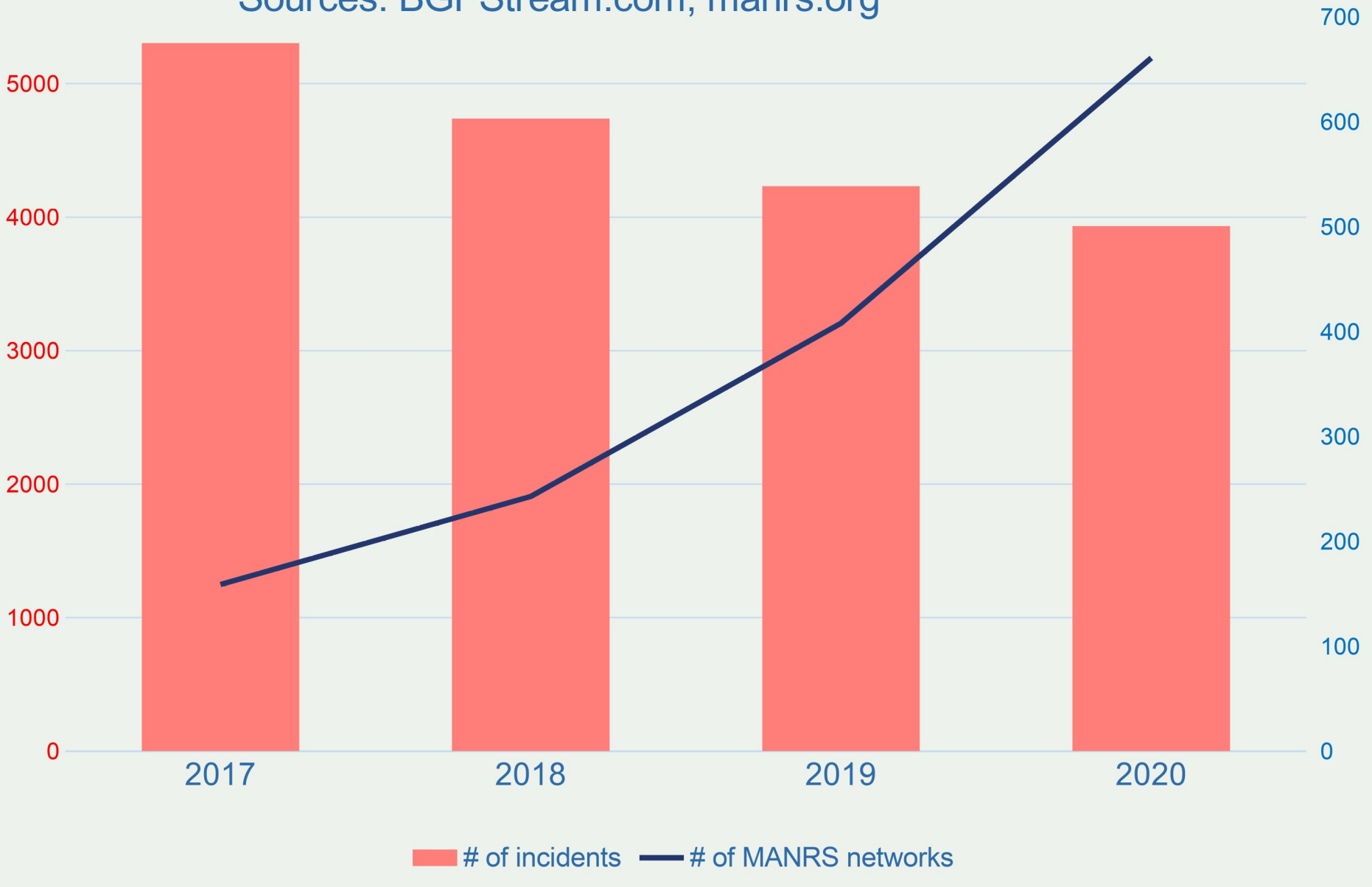
MANRS Participants in UK

2,042 ASNs advertised in UK

28 ASNs participating in MANRS (1.28%)

Most UK ASNs look to be MANRS conformant though!

Impact of implementing routing security measures
Sources: BGPStream.com, manrs.org



MANRS

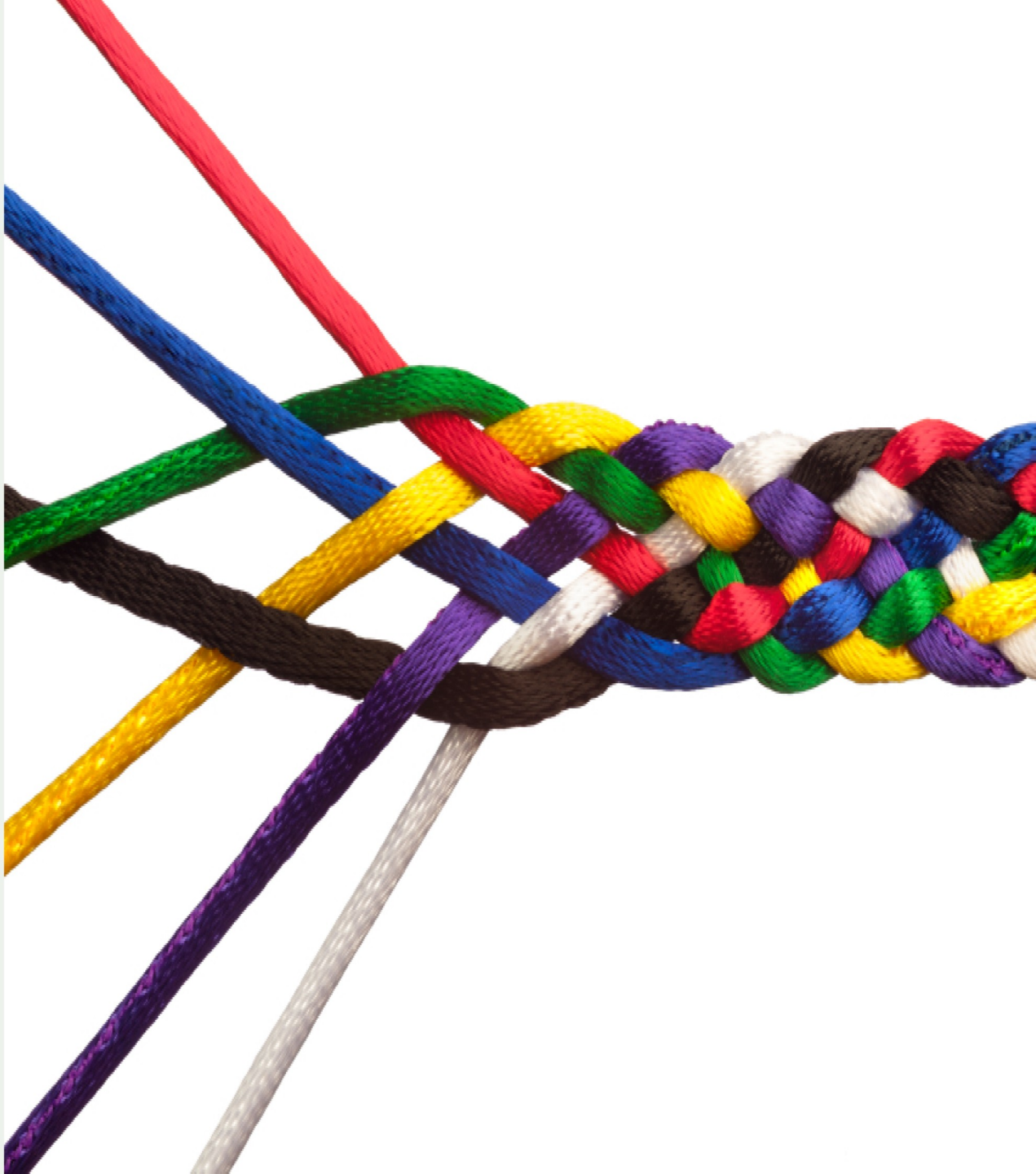
Join the MANRS Community

Visit https://www.manrs.org

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

Get Involved in the Community

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



MANRS