

Routing Security for better Internet Security



Kevin Chege, CISSP, CIPM
Director – Internet Development
chege@isoc.org

Background

The Internet is a large network of interconnected networks. There are ~73,000 networks on the Internet, each using a unique Autonomous System Number (ASN) to identify itself

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” – to know the best route/shortest path to other networks

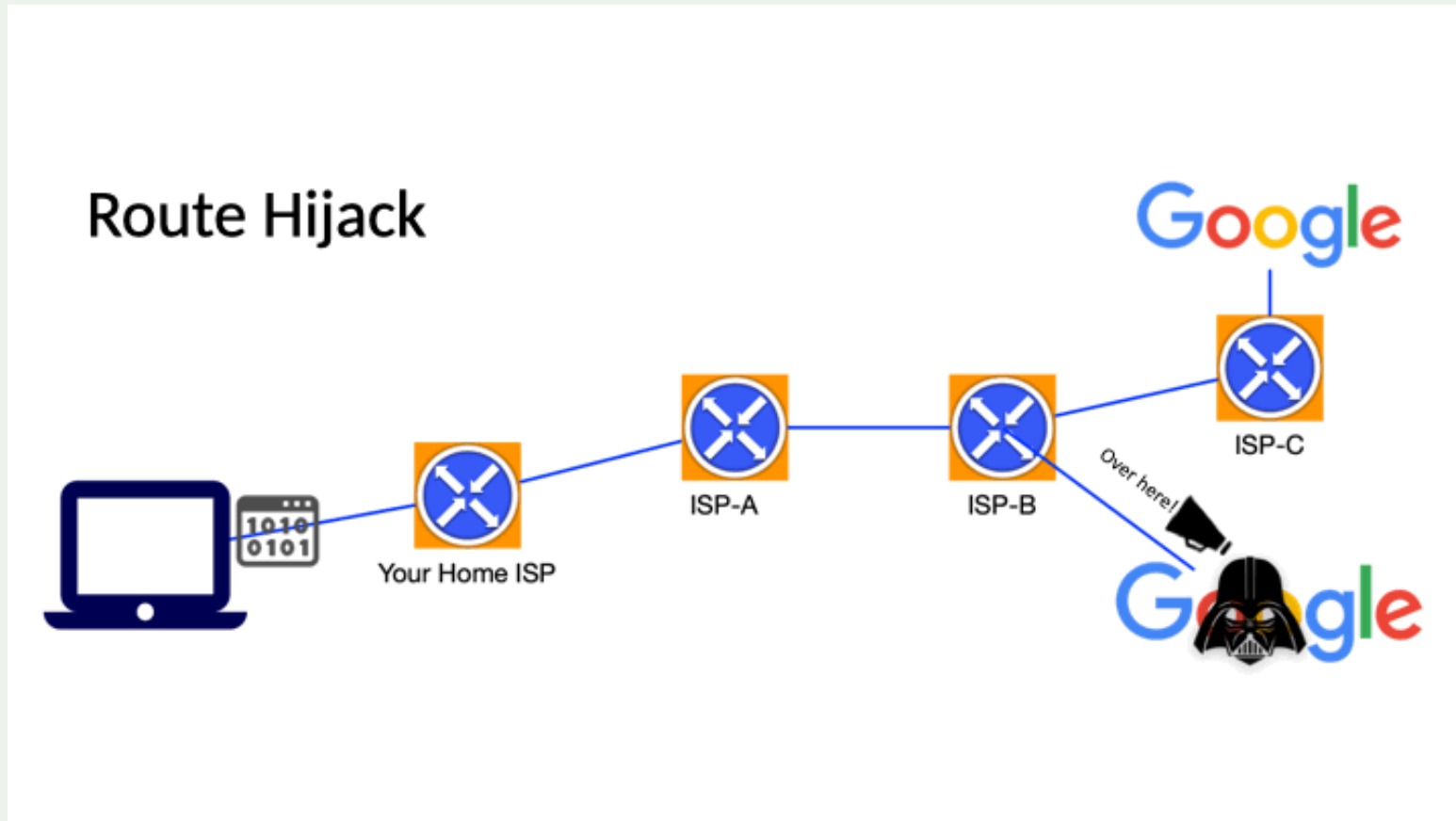
The Border Gateway Protocol (BGP) used by the Internet routing system is based entirely on *unverified trust* between networks

- 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

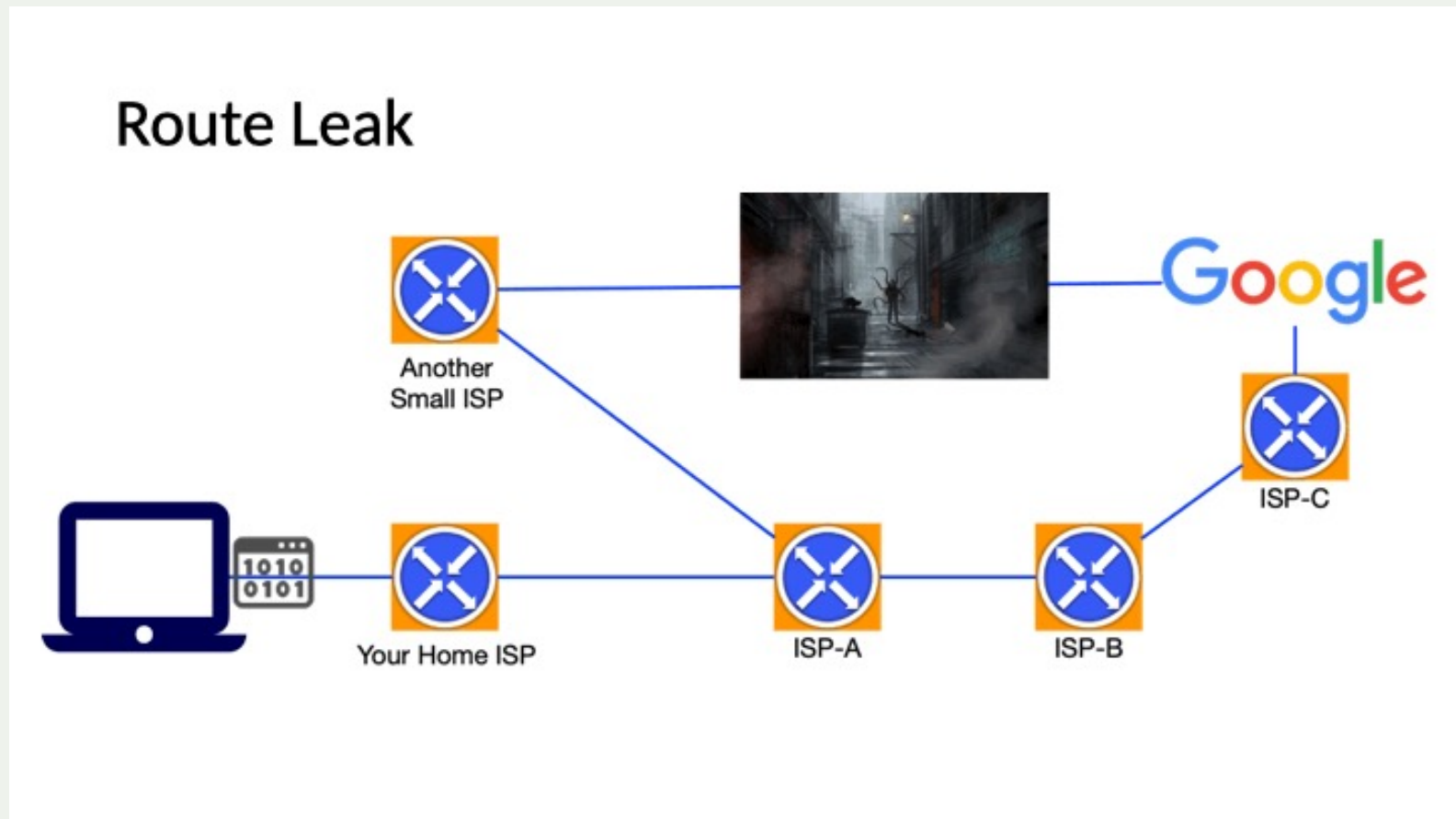
Event	Explanation	Repercussions	Example
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that it has a route to a destination through the other upstream provider.	Can be used for a MITM, including traffic inspection, 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>

Routing Security



Routing Security

Route Leak



Routing Incidents.. They are not going away

< KENTIK BLOG SUBSCRIBE

What can be learned from recent BGP hijacks targeting cryptocurrency services

by [Doug Madory](#) • Director of Internet Analysis
SEPTEMBER 22, 2022 • [INTERNET ANALYSIS](#), [NETWORK SECURITY](#), [CRYPTOCURRENCY](#)

[Twitter](#) [LinkedIn](#) [Facebook](#)

Security Blogwatch

BGP hijack steals AWS IP range; cryptocurrency theft ensues

[Richi Jennings](#)
Your humble blogwatcher, dba RJA



BORDER GATEWAY PROTOCOL INSECURITY —

How 3 hours of inaction from Amazon cost cryptocurrency holders \$235,000

For 2nd time in 4 years, Amazon loses control of its IP space in BGP hijacking.

DAN GOODIN - 9/23/2022, 9:04 PM



Routing security – impact on online privacy

- **Man in the Middle (MITM) attacks** - Online traffic inspection, modification and or reconnaissance without consent
- **Traffic Hijacks** - Data being sent to the wrong destination by a malicious actor who hijacks network traffic.
- **Impersonation** - via spoofing where a malicious actor impersonates a genuine online resource thereby facilitating the collection of user data from unsuspecting users.

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.



MANRS sets a new norm for routing security.



Currently: 4 MANRS Programs



Network
Operators (2014)

765 members about
950 ASNs



Internet Exchange Points (2018)

108 members



Content Delivery Networks (CDNs) and
Cloud Providers (2020)

23 members



Network Equipment Vendors (2021)

6 members

Summary of the MANRS actions



Filtering

Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity



Anti-Spoofing

Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure



Coordination

Maintain globally accessible up-to-date contact information



Global Validation

Publish your data, so others can validate routing information on a global scale



Tools

Provide monitoring and debugging tools to help others



Promotion

Actively encourage MANRS adoption among peers, customers, and partners

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



Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

MANRS outlines four simple but concrete actions that network operators should take:

Filtering – Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing – Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure

Coordination – Maintain globally accessible up-to-date contact information

Global Validation – Publish your data, so others can validate routing information on a global scale

<https://www.manrs.org>

MANRS – Tools for routing security

MANRS Observatory – <https://observatory.manrs.org>

A lot of work to improve the MANRS Observatory:

- MANRS Observatory collates data from third-party data sources BGPStream, GRIP, CIDR Report, RIR databases, PeeringDB, and CAIDA Spoofer
- BGPStream is no longer actively maintained
- Started to use GRIP (Global Routing Intelligence Platform) but this tends to generate false positives so needs improvements to tune and improve accuracy
- More automated processing of MANRS applications to improve response times

MONTH (PARTIAL) October 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

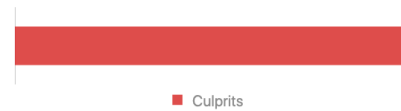
Incidents

Total		
1'016	Route misoriginations	178
	Route leaks	91
	Bogon announcements	747



Culprits

Total	Culprits	822
-------	----------	-----



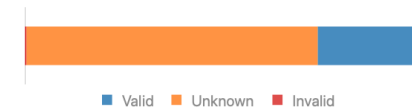
Routing completeness (IRR)

Total	Unregistered	14%
100%	Registered	86%



Routing completeness (RPKI)

Total	Valid	25%
100%	Unknown	74%
	Invalid	1%

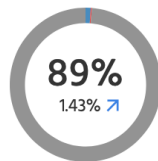


MANRS Readiness

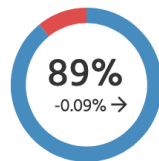
Filtering



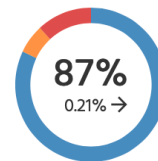
Anti-spoofing



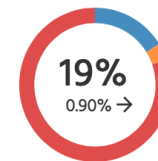
Coordination



Global Validation IRR

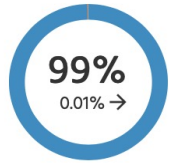


Global Validation RPKI

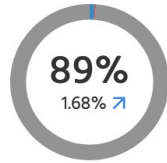


● Ready ● Aspiring ● Lagging ● No Data Available

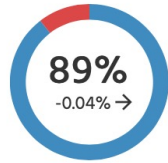
Filtering ⁱ



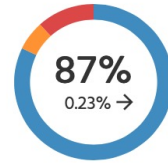
Anti-spoofing ⁱ



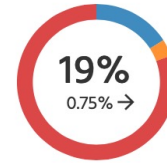
Coordination ⁱ



Global Validation IRR ⁱ



Global Validation RPKI ⁱ



● Ready ● Aspiring ● Lagging ● No Data Available

Global view

Size: [Count](#) | [Incidents](#) | [Culprits](#) Region: [Country](#) | [UN Regions](#) | [UN Sub-Regions](#) | [RIR Regions](#)

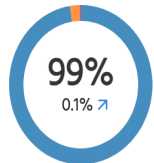


RPKI- AFRINIC region Observatory data

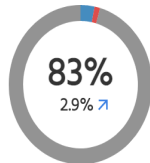
January 2022

MANRS Readiness ⁱ

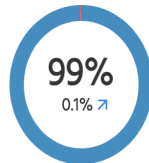
Filtering ⁱ



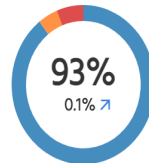
Anti-spoofing ⁱ



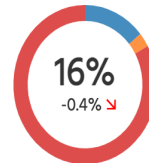
Coordination ⁱ



Global Validation IRR ⁱ



Global Validation RPKI ⁱ



● Ready ● Aspiring ● Lagging ● No Data Available

Routing completeness (RPKI) ⁱ

Valid	4,723	13.8%
Unknown	29,456	86.1%
Invalid	43	0.1%

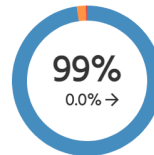


■ Valid ■ Unknown ■ Invalid

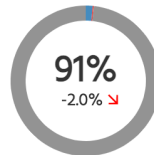
January 2023

MANRS Readiness ⁱ

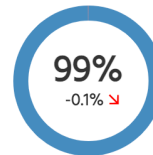
Filtering ⁱ



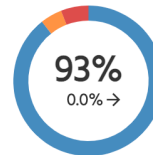
Anti-spoofing ⁱ



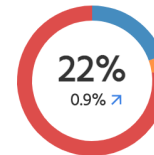
Coordination ⁱ



Global Validation IRR ⁱ



Global Validation RPKI ⁱ



● Ready ● Aspiring ● Lagging ● No Data Available

Routing completeness (RPKI) ⁱ

Valid	8,021	21.6%
Unknown	28,976	77.8%
Invalid	227	0.6%



■ Valid ■ Unknown ■ Invalid

MANRS Observatory – API

API access is available to the MANRS Observatory. This will enable everyone to view and use this data for research or to make sense of the state of routing on the Internet.

You do not need to be a MANRS participant to get access, but you do need an Observatory account. You can get access by:

- Being a MANRS participant, you get access to all MANRS scores and detailed information on your ASN(s).
- Applying to be a partner, you get access to a certain selection of ASN(s).
- Registering as an API-only user, you get no access to any non-public part of the Observatory.

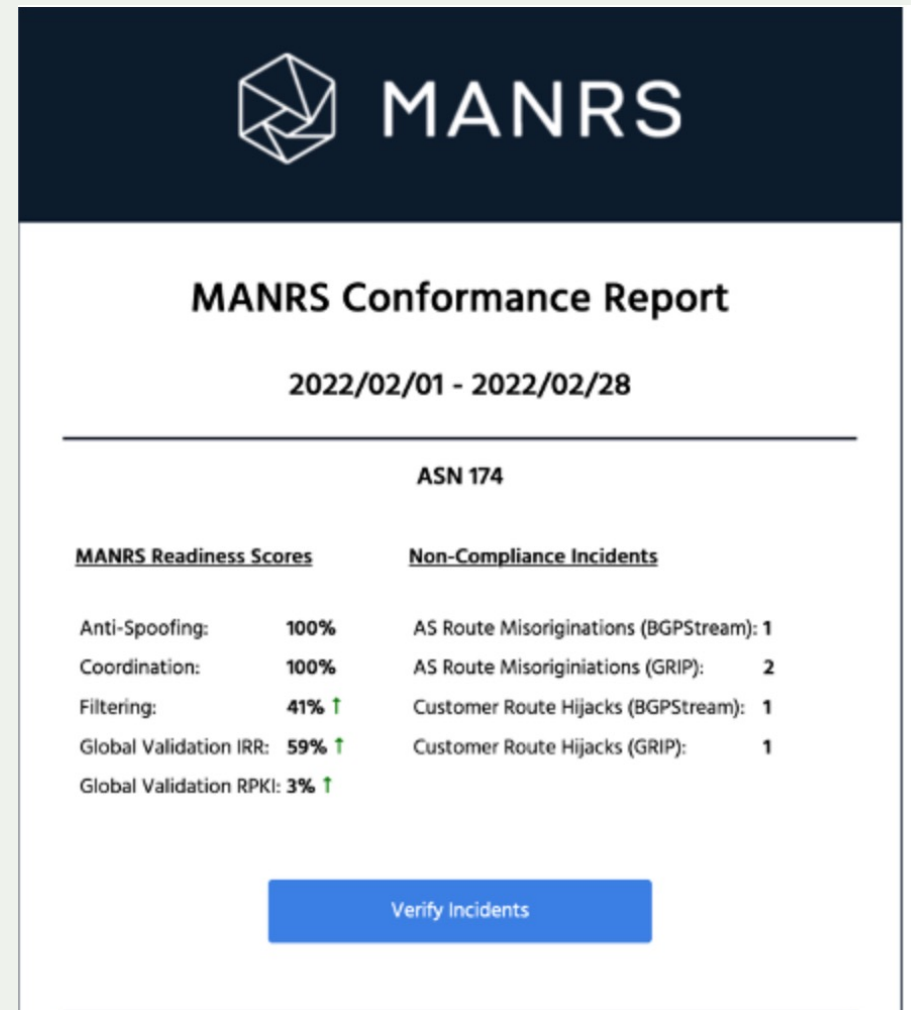


MANRS Conformance Reports

Monthly reports on MANRS participant conformance

Opportunity to verify any incidents picked up on the MANRS Observatory that involved your network

May indicate a need to look at your network security controls, especially those that require MANRS conformance.



MANRS

MANRS Conformance Report

2022/02/01 - 2022/02/28

ASN 174

<u>MANRS Readiness Scores</u>	<u>Non-Compliance Incidents</u>
Anti-Spoofing: 100%	AS Route Misoriginations (BGPStream): 1
Coordination: 100%	AS Route Misoriginations (GRIP): 2
Filtering: 41% ↑	Customer Route Hijacks (BGPStream): 1
Global Validation IRR: 59% ↑	Customer Route Hijacks (GRIP): 1
Global Validation RPKI: 3% ↑	

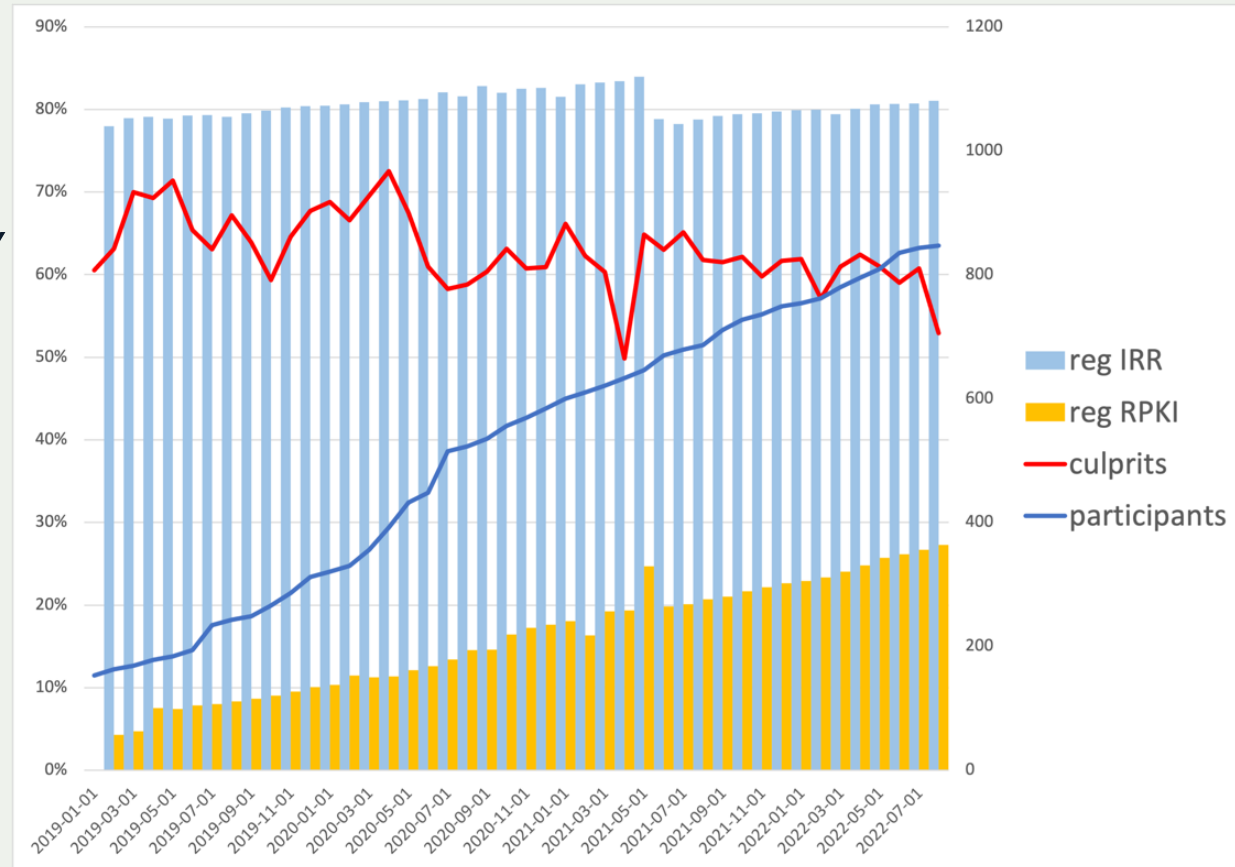
[Verify Incidents](#)

Progress in routing security

81% of all ASNs have their routes registered in the IRR and 27% in RPKI, and these numbers steadily grow.

Number of “culprits” – ASNs implicated in one or more suspicious routing events – declines

Data sources: MANRS Observatory, BGPStream, GRIP.



The Future of MANRS

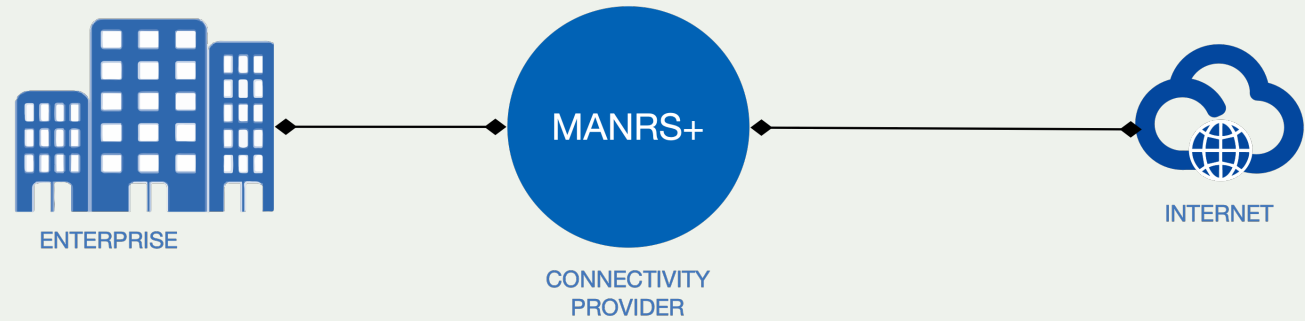


MANRS+ - Elevated tier of MANRS participation

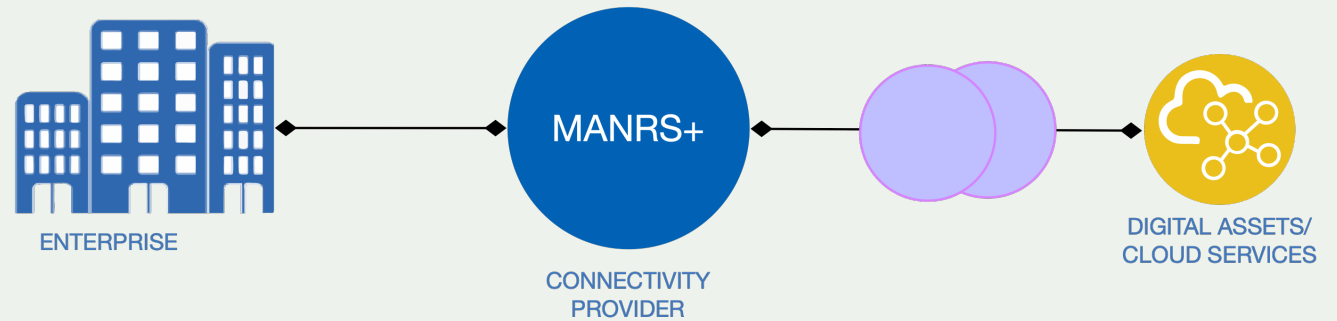
- Established by network operators, service providers and their customers who require higher levels of routing security assurance
- Aims to develop a quality mark, certification, and possibly standards that can be incorporated into procurement recommendations and policies.
- MANRS+ WG is developing set of requirements around path security, DDoS attack protection, anti-spoofing protection, and validated routing information (e.g. ROAs and AS-SETs), plus auditing approaches to assure high levels of conformance
- Network operators (Connectivity Providers) and their customers (Relying Parties) setting the requirements of the future quality mark for traffic security with the goal of eventually incorporating it in procurement policies and recommendations

Use Cases for MANRS+

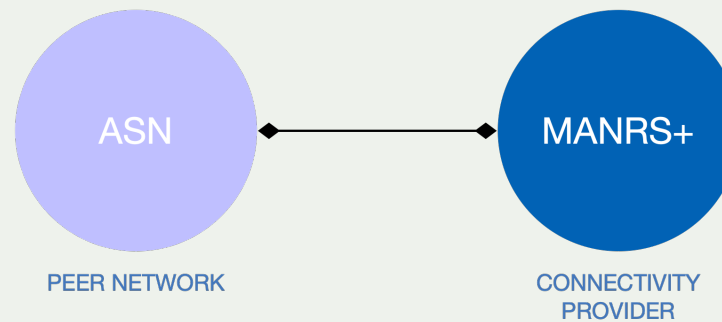
Traffic Security



Value Chain Security



Peering Security



MANRS+ Sample Requirements

- **Path Security** - Connectivity provider has detection capabilities and can mitigate the risk that traffic will be hijacked or detoured as a result of a mistake or an attack.
- **DDoS Attack Protection** - Connectivity provider has detection and mitigating capabilities reducing the risk of a (volumetric) DoS attack.
- **Anti-Spoofing Protection** – Connectivity provider detects and prevents traffic from their direct customers or peers with spoofed source IP addresses
- **Routing Information** - Connectivity provider has accessible complete and up-to-date documentation of the intended routing announcements (e.g. RPKI ROAs) and other information on its routing policy (e.g AS-SET) that is necessary for deploying effective security controls by the Network.



Current status of MANRS+

MANRS+ WG setup

WG landing page: <https://www.manrs.org/about/manrs-working-group/>

WG calls every two weeks, alternating between 1200UTC and 1700UTC

WG mailinglist: <manrs-plus-wg@elists.manrs.org>

Work focus: MANRS+ Requirements, survey to validate the requirements

2023: Opportunities for ISPs in Botswana



MANRS Trainings

- Internet Society moderated courses (<https://www.isoc.org/learning/manrs/>)
- Hands-on workshops (both directly and via our Mentors and Ambassadors Program)
- Training labs for network engineers and administrators to learn how to configure routing security features
- Implementation Guides provide step-by-step instructions to implement MANRS Actions



MANRS Lab Manager
Dashboard: MANRS-Vers1 for manrs

Logged in as manrs (chege@isoc.org)
[Home](#) | [Admin interface](#) | [Change password](#) | [Log out](#)

Instructions AS64500 **AS64501** AS64502 AS64510 AS64511 Online

The customer (AS64501)

Customer 64501 should announce the following prefixes to you:

- 2001:db8:1001::/48
- 192.0.2.0/24

For testing purposes you can ping them on addresses 2001:db8:1001::1 and 192.0.2.1.

Looking glass from this router's viewpoint

Received traffic (last change at 8:17:09)

Expected	Currently seen
10.0.0.1 to 192.0.2.1	These packets are missing
198.51.100.1 to 192.0.2.1	These packets are missing
2001:db8::1 to 2001:db8:1001::1	These packets are missing
2001:db8:2002::1 to 2001:db8:1001::1	These packets are missing
2001:db8:3000::1 to 2001:db8:1001::1	These packets are missing

MANRS Mentors & Ambassadors Program 2023

formerly known as MANRS Ambassadors & Fellows Program

Aims to extend outreach and involve the wider Internet community in routing security

- Applications will open on 6 April 2023
- **Mentors** are individuals well established in the MANRS Community who provide mentorship, guidance, and feedback to others in the routing security community
- **Ambassadors** are emerging leaders who can enthusiastically bring knowledge and skills about routing security to their communities
- **Three Tracks:** Training, Research and Policy
- CSIRTs are invited to apply and participate

Participation in the MANRS Steering Committee

The Steering Committee is comprised of individuals elected by the MANRS community to coordinate and develop the MANRS initiative. It holds quarterly meetings, and its duties include:

- Reviewing and making recommendations to the MANRS community about the MANRS Actions
- Appointing MANRS Advisors, Ambassadors, and Mentors
- Supervising the auditing process for new applicants
- Making recommendations to the MANRS community on the suspension/termination

Anyone is eligible to serve on the Steering Committee. Nominations are held annually in October.

Participating in the MANRS+ Working Group

MANRS+ WG setup

WG landing page: <https://www.manrs.org/about/manrs-working-group/>

WG calls every two weeks, alternating between 1200UTC and 1700UTC

FIRST NetSec SIG: <https://www.first.org/global/sigs/netsec/>

Why join MANRS?

- **Improve your security posture and reduce the number and impact of routing incidents**
- Improve your privacy posture
- **Meet the expectations of the operator community**
- Join a community of security-minded operators working together to make the Internet better
- **Use MANRS as a competitive differentiator**



Thank You!

Join the MANRS Community

<https://www.manrs.org>

Kevin Chege
chege@isoc.org

