7 December 2021
FIRST & AfricaCERT Virtual Symposium 2021

The MANRS Observatory

Monitoring Routing Security on the Internet

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

The Routing Problem

72,629 ASNs connected to Internet

902,184 advertised IP prefixes (routes)

Border Gateway Protocol (BGP) is based entirely on *unverified trust* between these 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

MANRS

MANRS: What do we need to observe?

- MANRS provides fixes to eliminate the common threats - route leaks/hijacks & spoofed traffic
- Brings together established industry best practices
- Based on collaboration among participants and shared responsibility for the Internet infrastructure
- 615 Network Operators, 98 IXPs, 18 CDN/Cloud Providers, 5 Vendors, 18 Partners

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

Maintain globally accessible up-to-date contact information in common routing databases

(RIR Whois or PeeringDB)

Global Validation

Facilitate validation of routing information on a global scale

Publish your data so others can validate

(IRR and/or RPKI)

MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH (PARTIAL) November 2021 UN REGIONS Africa USE GRIP DATA

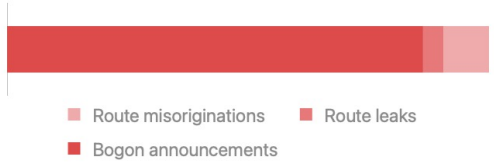
Overview

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

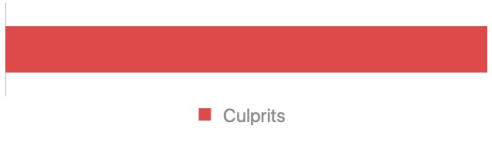
Incidents

Route misoriginations	9
Route leaks	4
Bogon announcements	82
Total	95



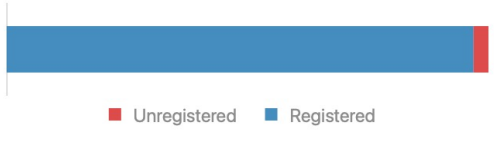
Culprits

Culprits	59



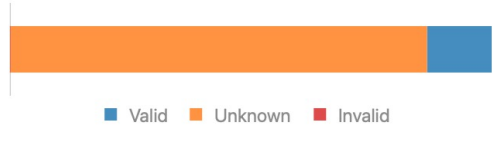
Routing completeness (IRR)

Unregistered	1,048	3.1%
Registered	32,698	96.9%



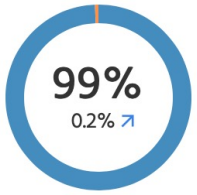
Routing completeness (RPKI)

Valid	4,526	13.4%
Unknown	29,184	86.5%
Invalid	36	0.1%

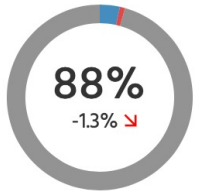


MANRS Readiness

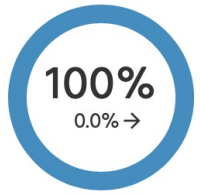
Filtering



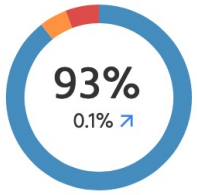
Anti-spoofing



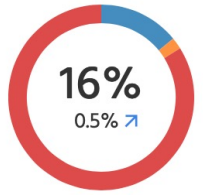
Coordination



Global Validation IRR



Global Validation RPKI



Ready Aspiring Lagging No Data Available

MONTH (PARTIAL) November 2021 UN REGIONS Africa 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 | 200 | 500 | 1000

Total 1,662 Previous 1 2 3 4 5 ... 17 Next

Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
24757	EthioNet-AS	ET	Africa	Sub-Saharan Africa	AFRINIC	100%	100%	100%	99%	0%
26422	ABOUTIT-ONLINE	ZA	Africa	Sub-Saharan Africa	AFRINIC	100%	-	100%	100%	0%
204934	CLOUD-LAYER-LIMITED-AS - Clou	SC	Africa	Sub-Saharan Africa	AFRINIC	100%	-	100%	100%	0%
22572	INFOSAT-IP	ZA	Africa	Sub-Saharan Africa	AFRINIC	100%	-	100%	100%	100%
207740	AMIRGT-AS - Youssef Hamed	EG	Africa	Northern Africa	AFRINIC	100%	-	100%	100%	100%
201118	INTELCOM - Intelcom Group Ltd	SC	Africa	Sub-Saharan Africa	AFRINIC	100%	-	100%	100%	0%
25543	FasoNet-AS	BF	Africa	Sub-Saharan Africa	AFRINIC	100%	100%	100%	100%	3%
29918	IMPOL-ASN	ZA	Africa	Sub-Saharan Africa	AFRINIC	100%	-	100%	100%	100%
29340	AFOL-	GH	Africa	Sub-Saharan Africa	AFRINIC	100%	-	100%	100%	0%
16800	NBS90	ZA	Africa	Sub-Saharan Africa	AFRINIC	100%	-	100%	100%	0%
21739	T-SOL	ZA	Africa	Sub-Saharan Africa	AFRINIC	100%	-	100%	100%	100%

How can CSIRTs get involved?

- Raise awareness of routing security issues within your constituencies, as well as into national critical infrastructure activities
- Add routing security incident monitoring and handling to your service portfolios
- Help organise practical routing security workshops and/or develop routing security curriculums in the context of training-the-trainers and/or network forensics capacity building programmes
- Add routing security to network security auditing programmes
- Inclusion of routing security activities in cyberdrills
- **Utilise the MANRS Observatory monitoring tool** (can offer account)