31 July – 1 August 2019
SANOG 34

# Mutually Agreed Norms for Routing Security

## Observing Your MANRS


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

# Background

There are 65,203 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!

MANRS

# How big is the problem?

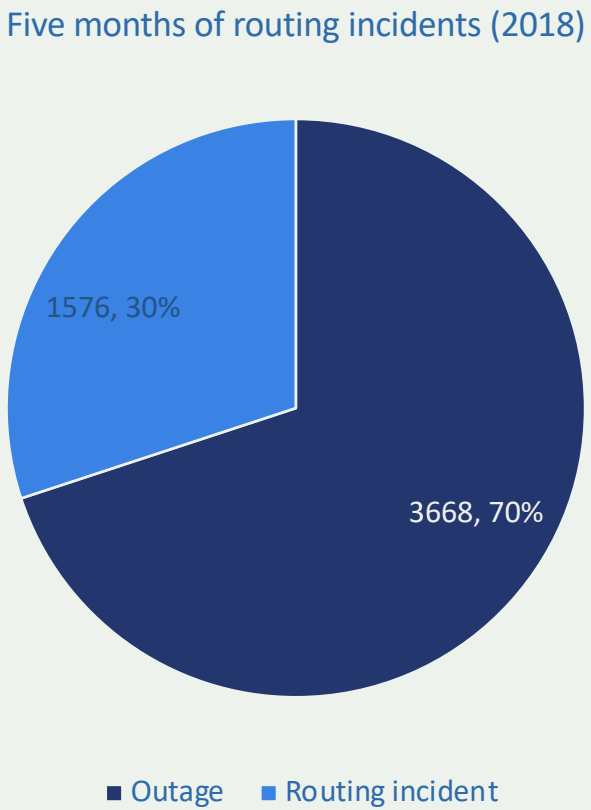
Some Facts & Figures

# 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*<br>*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. | *June 2019. Verizon accepted incorrect routes from DQE Communications that diverted traffic destined for Cloudflare, Facebook & Amazon.* |
| **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 | *March 1, 2018. Memcached 1.3Tb/s reflection-amplificationattack reported by Akamai* |

# The routing system is constantly under attack

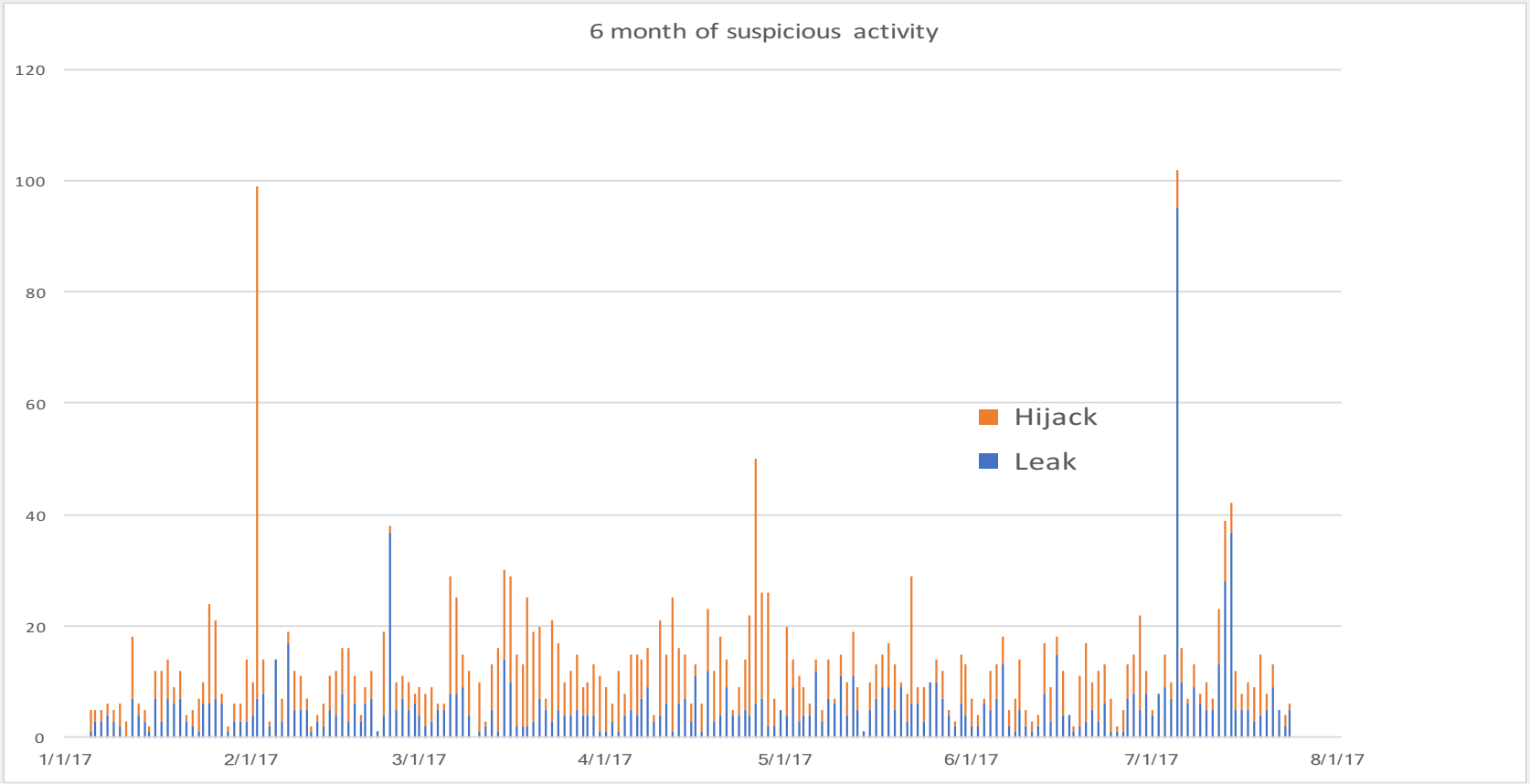
- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- **1,546 networks were responsible for 5304 routing incidents**
- **547 networks were responsible for 1576 routing incidents**




MANRS

Source: https://www.bgpstream.com/

# No Day Without an Incident




http://bgpstream.com/

MANRS

# Mutually Agreed Norms for Routing Security (MANRS)

**Provides crucial fixes 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**

# MANRS Actions

## 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 Participants – as of July 2019

201 Network Operators

328 Autonomous Systems (ASNs)

34 Internet Exchange Points

10 partners (promotion, capacity building etc..)

# MANRS Participants in South Asia


2,686 ASNs advertised in South Asia

1,726 (IN), 674 (BD), 125 (PK), 75 (NP), 47 (AF), 17 (LK), 12 (BT), 10 (MV)

8 ASNs participating in MANRS (0.3%)

| | |
|---|---|
| Cybergate Limited (AS58599) | - 4 actions |
| Link3 Technologies Ltd. (AS23688) | - 4 actions |
| Fiber@Home Limited (AS58587) | - 4 actions |
| Minara Firoz Infotech (AS63980) | - 4 actions |
| Cyber Internet Services (AS9541/24440) | - 3 actions |
| TransWorld Associates (AS38193/45843) | - 4 actions |

Many South Asian ASNs are already MANRS conformant though!

# How to Implement MANRS

Documentation & Tools

# MANRS Implementation Guide

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

Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS

# 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 Dashboard

LOGOUT

OVERVIEW | HISTORY | DETAILS | COMPARISON | ABOUT

MONTH June 2019

# Overview

## State of Routing Security

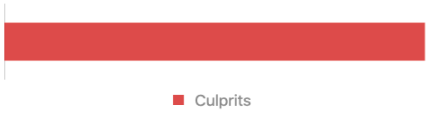
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

### Incidents

| Total | | |
|---|---|---|
| 1'762 | Route misoriginations | 256 |
| | Route leaks | 260 |
| | Bogon announcements | 1'246 |

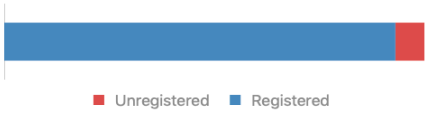

### Culprits

| Total | | |
|---|---|---|
| 866 | Culprits | 866 |



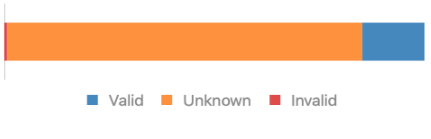

### Routing completeness (IRR)

| Total | | |
|---|---|---|
| 100% | Unregistered | 7% |
| | Registered | 93% |




### Routing completeness (RPKI)

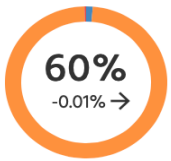
| Total | | |
|---|---|---|
| 100% | Valid | 15% |
| | Unknown | 85% |
| | Invalid | 1% |



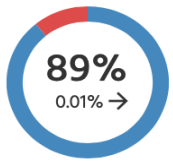

## MANRS Readiness

### Filtering

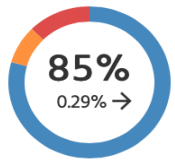

### Anti-spoofing



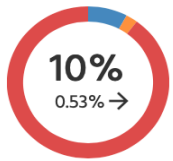

### Coordination




### Global Validation IRR



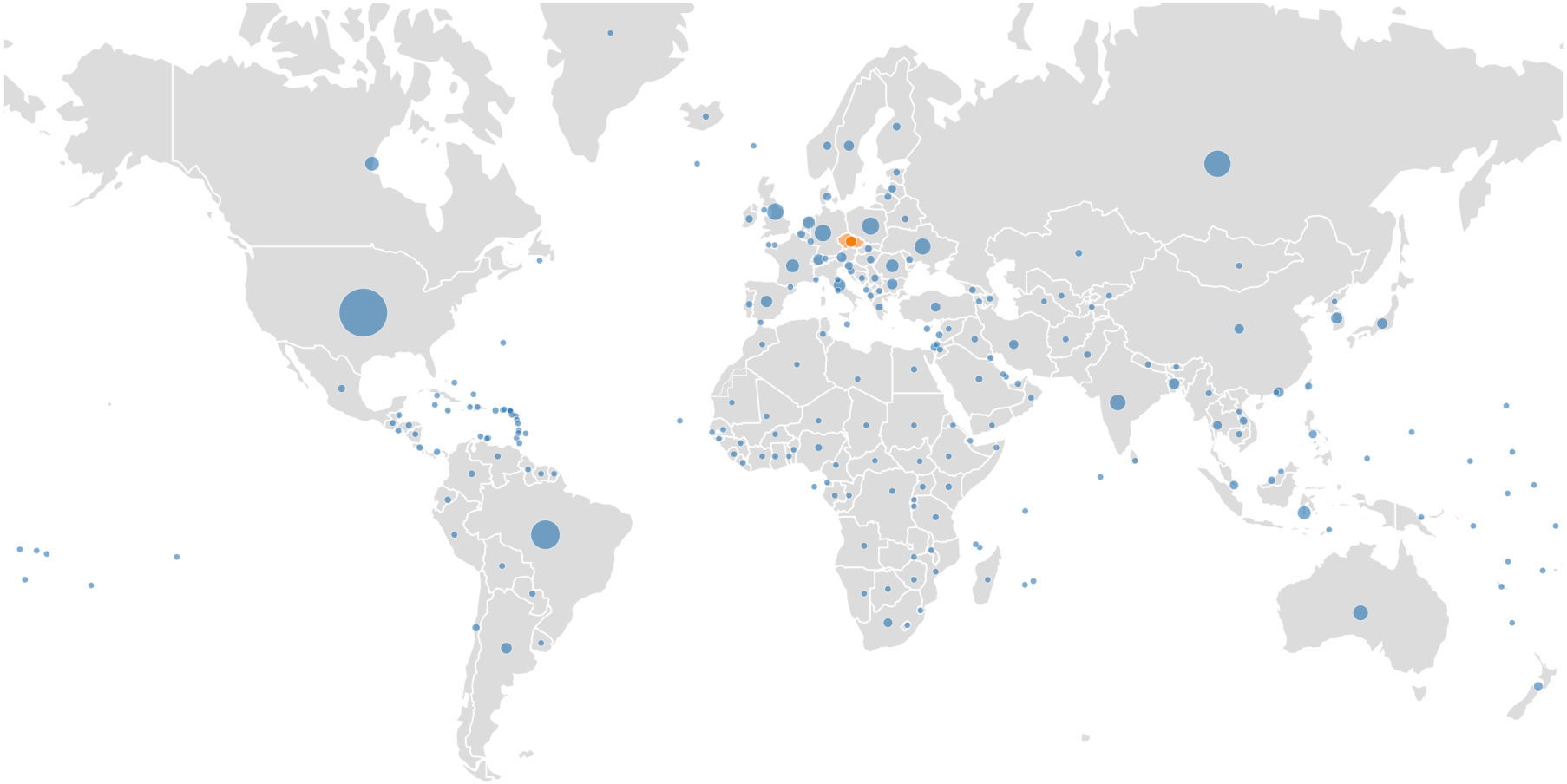

### Global Validation RPKI




Ready Aspiring Lagging

## Global view

Size: **Count** | Incidents | Culprits  Region: **Country** | UN Regions | UN Sub-Regions | RIR Regions



MANRS Dashboard

LOGOUT

OVERVIEW | HISTORY | DETAILS | COMPARISON | ABOUT

MONTH June 2019 COUNTRY India | Pakistan | Bangladesh | Sri Lanka | Nepal | Afghanistan | Maldives | Bhutan

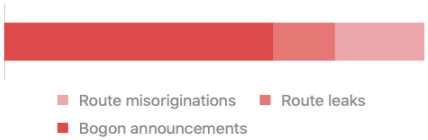
# Overview

## 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

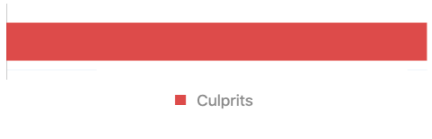
### Incidents

| Total | | |
|---|---|---|
| 89 | Route misoriginations | 19 |
| | Route leaks | 13 |
| | Bogon announcements | 57 |



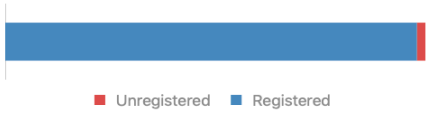

### Culprits

| Total | | |
|---|---|---|
| 40 | Culprits | 40 |



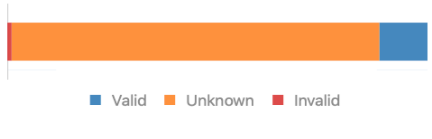

### Routing completeness (IRR)

| Total | | |
|---|---|---|
| 100% | Unregistered | 2% |
| | Registered | 98% |




### Routing completeness (RPKI)

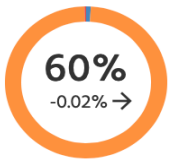
| Total | | |
|---|---|---|
| 100% | Valid | 12% |
| | Unknown | 87% |
| | Invalid | 1% |




## MANRS Readiness

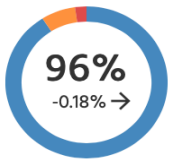
### Filtering


### Anti-spoofing

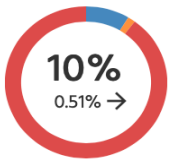



### Coordination


### Global Validation IRR




### Global Validation RPKI




Ready Aspiring Lagging

MANRS Dashboard

LOGOUT

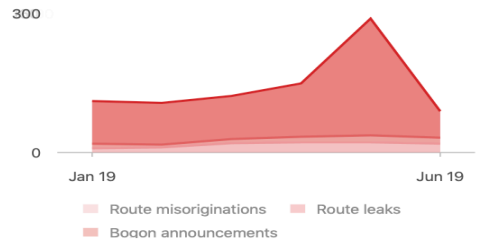
OVERVIEW | HISTORY | DETAILS | COMPARISON | ABOUT

MONTH June 2019 COUNTRY India Pakistan Bangladesh Sri Lanka Nepal Afghanistan Bhutan Maldives

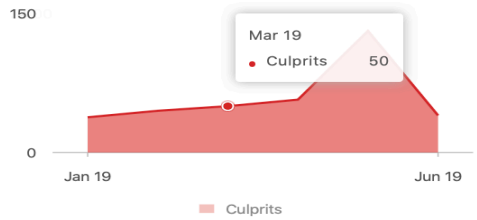
# History

January 2019 - June 2019

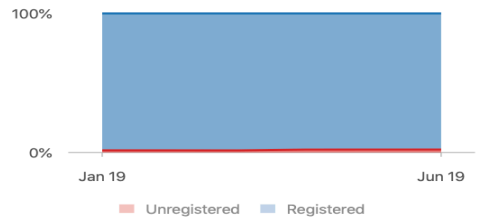
## Incidents



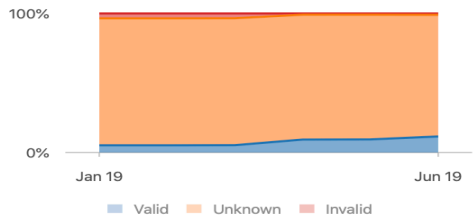

## Culprits




## Routing completeness (IRR)



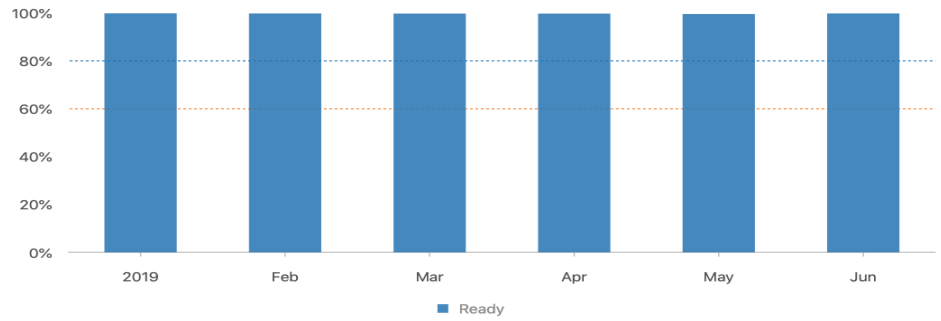

## Routing completeness (RPKI)



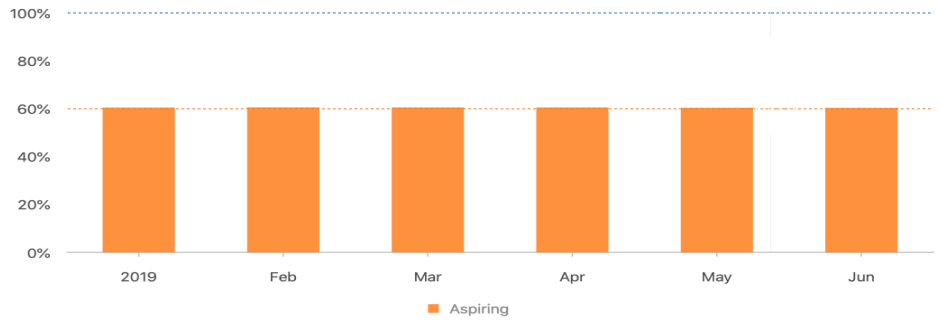

## MANRS Readiness

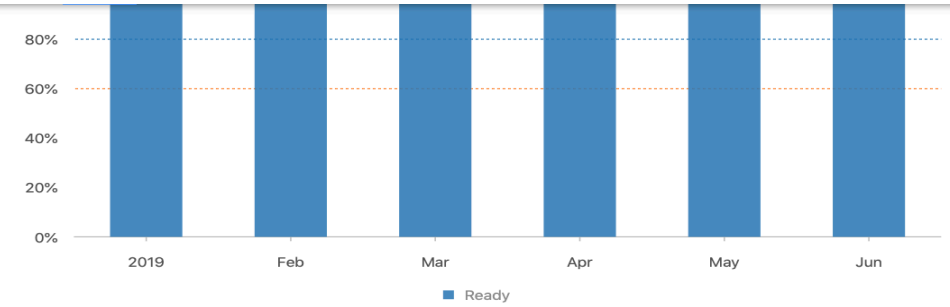
Overall | Metrics

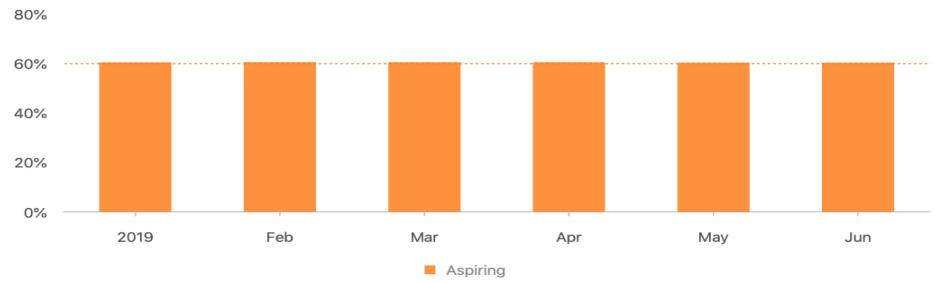
### Filtering



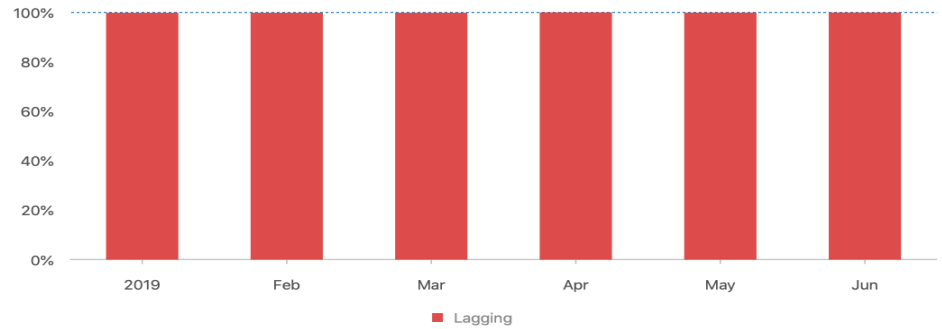

### Anti-spoofing



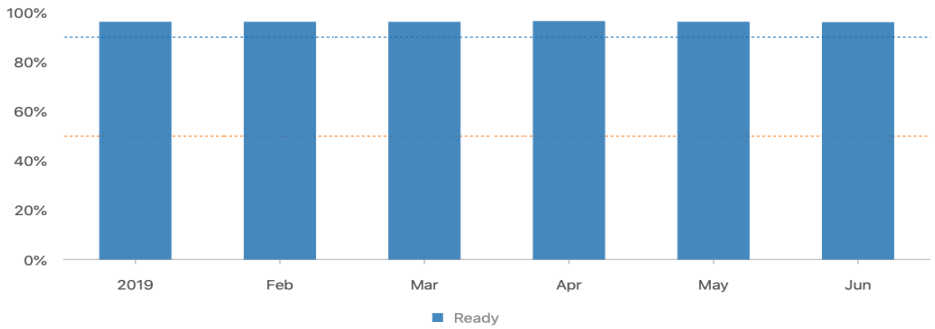


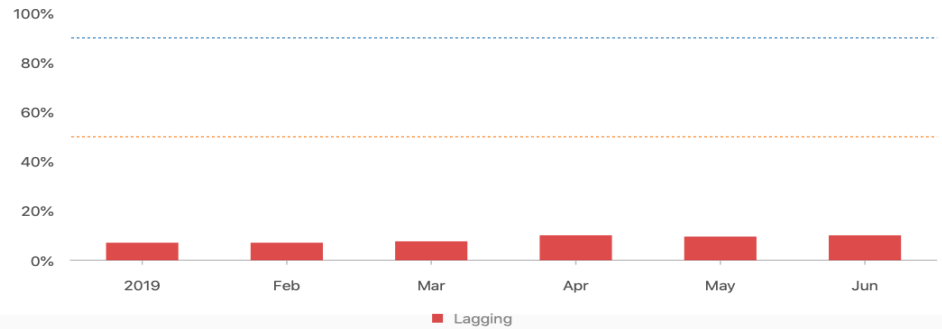

## Coordination




## Global Validation IRR




## Global Validation RPKI



MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

MONTH June 2019 HOLDER BDREN-UGC-AS-AP Banglades...

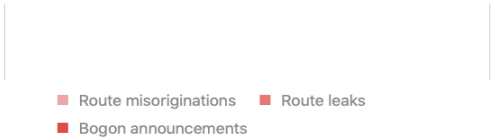
# Overview

## 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 | | |
|---|---|---|
| 0 | Route misoriginations | 0 |
| | Route leaks | 0 |
| | Bogon announcements | 0 |

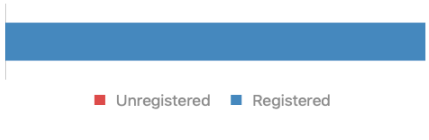



### Culprits

| Total | | |
|---|---|---|
| 0 | Culprits | 0 |

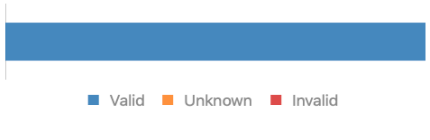

### Routing completeness (IRR)

| Total | | |
|---|---|---|
| 100% | Unregistered | 0% |
| | Registered | 100% |




### Routing completeness (RPKI)

| Total | | |
|---|---|---|
| 100% | Valid | 100% |
| | Unknown | 0% |
| | Invalid | 0% |




## MANRS Readiness

### Filtering


### Anti-spoofing


### Coordination


### Global Validation IRR


### Global Validation RPKI


Ready Aspiring Lagging

MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

MONTH June 2019 HOLDER BDREN-UGC-AS-AP Banglades...

# Details - ASN 63961

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

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

MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

**M5** - Spoofing IP blocks

Absolute: **0.5** Normalized: **60%** Incident Count: **-**

| Has records | Spoofed prefixes |
|---|---|
| False | - |

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

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

| Checked on | Has contact info |
|---|---|
| 2019-06-13 | True |

**M7IRR** - Registered routes (% of routes registered)

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

| Number of prefixes | Number of unregistered prefixes | Unregistered prefixes | Checked on |
|---|---|---|---|
| 15 | 0 | - | 2019-06-13 |

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

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

| Number of prefixes | Number of unknown prefixes | Checked on |
|---|---|---|
| 2 | 0 | 2019-06-13 |

**M7RPKIN** - Invalid routes

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

| Number of prefixes | Number of invalid prefixes | Invalid prefixes |
|---|---|---|
| 2 | 0 | - |

# MANRS Observatory Access

Beta test was launched in June 2019 with MANRS Participants only

Aim to launch publicly in August 2019

Current access policy:

- Public will be able to view Overall, Regional and Economy aggregated data
- Only MANRS Participants will have access to detailed data about their network

Caveats:

- Still some false positives
- There are sometimes good reasons for non-100% conformancy
- BUT, this is all inherently public data anyway!

# MANRS Community

# Is the problem getting better or worse?

# Everyone benefits from improved Routing Security

Joining MANRS means joining a community of security-minded network operators committed to making the global routing infrastructure more robust and secure.

Heads off routing incidents, helping networks readily identify and address problems with customers or peers.

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

# MANRS needs to be community driven

MANRS should be (and is) a collaborative initiative of Internet operators

- Internet operators undertaking MANRS principles need to encourage use of best practices
- MANRS needs to be driven by leaders within their communities who strongly believe that routing security is an essential component for the future well being of the Internet
- Need feedback and recommendations for improving MANRS principles and best practices, e.g. MANRS Actions, MANRS Observatory, MANRS Implementation Guides, and training materials
- Internet Society can help with presentations, informational materials and merchandise (shirts and stickers)

# Join Us

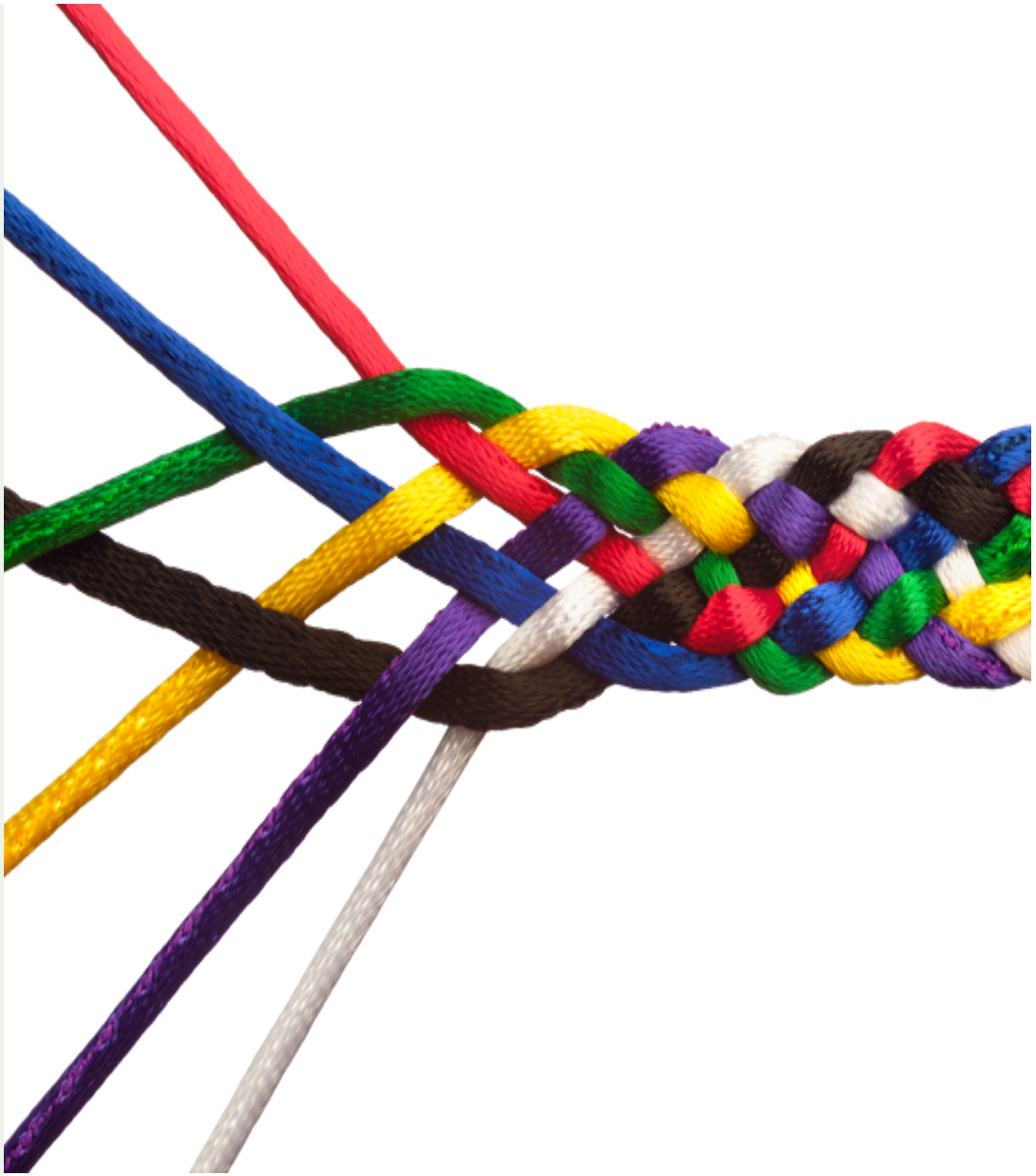
**Visit https://www.manrs.org**

- 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



# Thank you.

Kevin Meynell
meynell@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120