

Routing Hijack - Bangladesh

**Presented By :
Simon Sohel Baroi
FGL**



Network Means - Problem

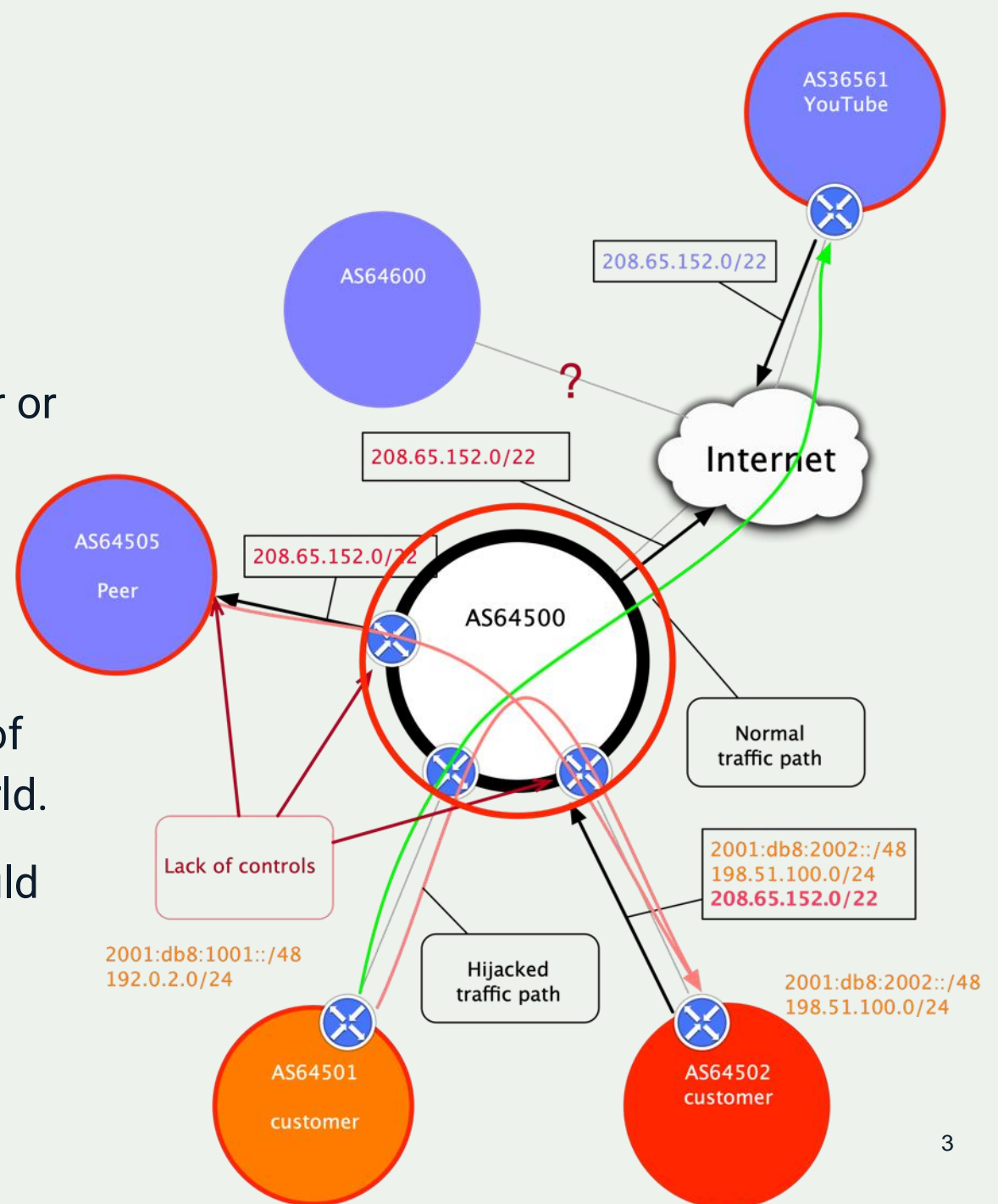


Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking,” is when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that a server or network is their client. This routes traffic to the wrong network operator, when another real route is available.

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.

Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).

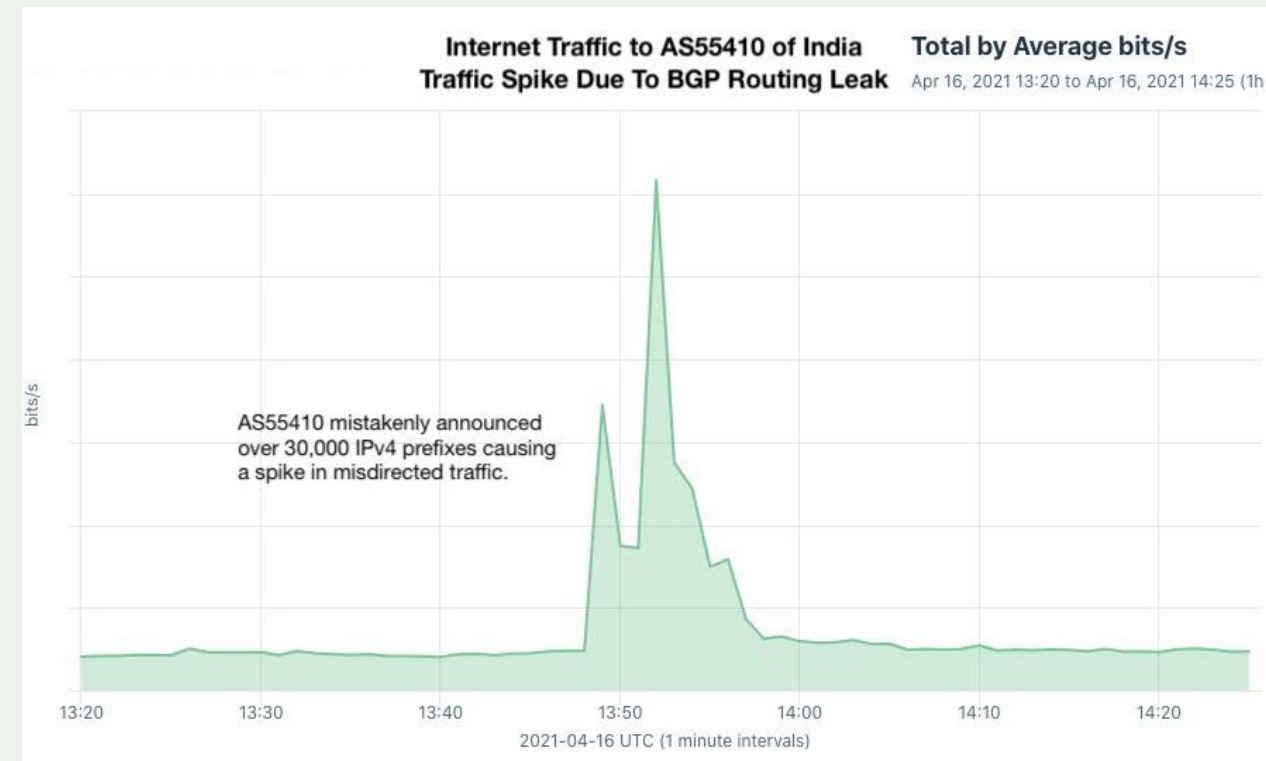


Routing Incidents are increasing (Vodafone Idea AS55410 Hijack)

Vodafone Idea (AS55410) started originating 31,000+ routes which don't belong to them.

Prefixes belonged to Google, Microsoft, Akamai, Cloudflare, Fastly, and many others were affected.

<https://www.manrs.org/2021/04/a-major-bgp-hijack-by-as55410-vodafone-idea-ltd/>



Routing Incidents Cause Real World Problems

MyEtherWallet DNS Hijacked, \$150,000 Worth of Eth Stolen

Routing Leak briefly takes down Google

UK traffic diverted through Ukraine

Massive route leak causes Internet slowdown

Global Collateral Damage of TMnet leak

DDoS Attacks Storm Linode Servers Worldwide

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

BGP routing security flaw caused Amazon Route 53 incident

A BGP routing security flaw enabled unknown threat actors to steal cryptocurrency by hijacking internet routing and rerouting traffic to a phishing site in Russia.

Global Impacts of Re

BGP hijack incident by Syrian Telecommunications Establishment

The Vast World of Fraudulent Routing

Large scale BGP hijack out of India

DDoS attack on BBC may have been biggest in history



Routing Incidents (South Asia) May ~ June 2021

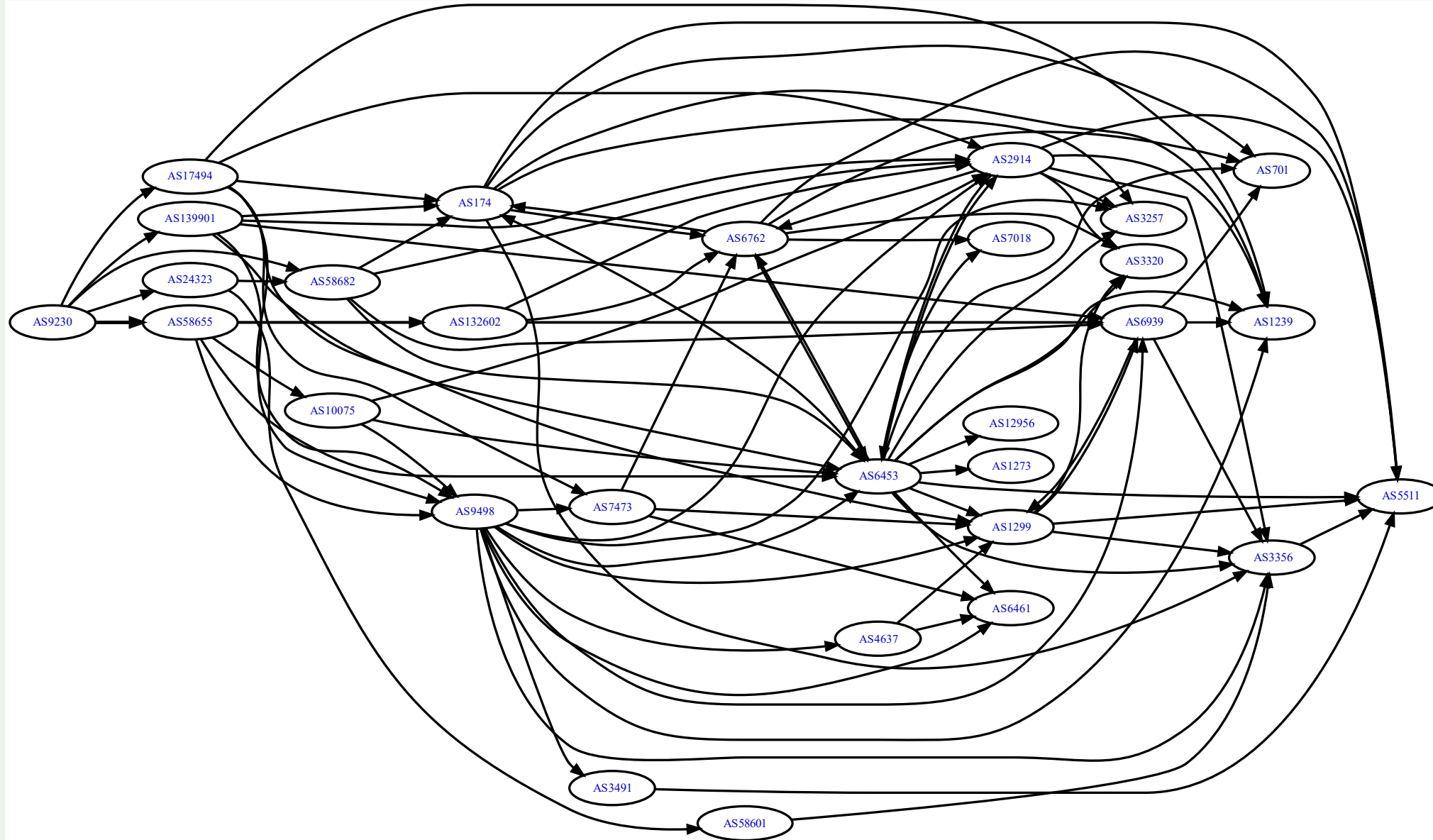
Event Type	Event Details	Prefixes affected
BGP Hijack	Expected Origin: AS45609 BHARTI-MOBILITY-AS-AP Bharti Airtel Ltd Detected Origin: ASN 45069 CNNIC-CTTSDNET-AP China Tietong Shandong net, CN	106.193.255.0/24
BGP Leak	Origin AS: AS 4797 Wipro Spectramind Services Pvt Ltd, IN Leaker AS: AS4775 GLOBE-TELECOM-AS Globe Telecoms, PH Leaked to: AS 4637 (ASN-TELSTRA-GLOBAL Telstra Global, HK)	112.198.30.0/24
BGP Leak	Origin AS: AS132497 DNA-AS-AP DIGITAL NETWORK, IN Leaker AS: AS55644 VIL-AS-AP Vodafone Idea Ltd, IN Leaked to: AS3556 (Level3, US) AS3549 (LVLT-3549, US)	150.242.197.0/24
BGP Hijack	Expected Origin: AS328608 Africa-on-Cloud-AS, ZA Detected Origin: ASN 139879 GALAXY-AS-AP Galaxy Broadband, PK	156.241.0.0/16
BGP Hijack	Expected Origin: AS7018 ATT-INTERNET4, US Detected Origin: ASN18229 CTRLS-AS-IN CtrlS Datacenters Ltd., IN	172.0.0.0/12
BGP Hijack	Expected Origin: AS33567 TELECOM-LESOTHO, LS Detected Origin: ASN 55410 (VIL-AS-AP Vodafone Idea Ltd, IN)	41.203.176.0/20
BGP Leak	Origin AS: AS 132497 DIGITAL NETWORK ASSOCIATES, IN Leaker AS: AS 55644 Vodafone Idea Ltd, IN (AS 55644) Leaked to: AS3356 (LEVEL3, US)	103.245.69.0/24



Lets' Begin



Bangladesh Online Ltd.



AS9230

Bangladesh Online Ltd.

6th Aug, 2022 – Early Morning, NOC Found abnormalities from some clients. Some of them can't access Google, or some random sites.

- The Clients are from a specific prefix
- They thought it's a problem with the upstream.
- It might be routing issue
- They checked with the looking glass, found everything good.

Around 11 AM they found :

The prefix 202.84.36.0/24 is announced from Singtel AS 7473.



AS9230

Bangladesh Online Ltd.

The prefix 202.84.36.0/24 is announced from Singtel AS 7473.

- ROA Check – Found OK
- IRR Check – Found OK.

AS9230

202.84.36.0/24

Observation from different Looking glass:

route-views.isc.routeviews.org> sh ip bgp 202.84.36.0/24 be

BGP routing table entry for 202.84.36.0/24

Paths: (5 available, best #4, table default)

Not advertised to any peer

19151 6461 7473

198.32.176.164 from 198.32.176.164 (66.186.193.17)

Origin IGP, metric 5, valid, external, best (AS Path)

Last update: Tue Jul 26 11:43:49 2022

route-views.isc.routeviews.org>

route-views.optus.net.au>sh ip bgp 202.84.36.0/24

BGP routing table entry for 202.84.36.0/24, version 1440601472

Paths: (2 available, best #2, table default)

Not advertised to any peer

7474 7473

203.202.143.33 from 203.202.143.33 (203.202.143.33)

Origin IGP, localpref 100, valid, external, best

Community: 7474:1202 7474:1222 7474:1403 7474:1527

route-views.optus.net.au>

AS9230

202.84.36.0/24

Observation from APNIC Portal:

Routing Status (202.84.36.0/24)



At **2022-08-06 00:00:00 UTC**, **202.84.36.0/24** was **99%** visible (by **381** of **385** RIS full peers).

🕒 First ever seen announced by **AS9230**, on **2001-07-20 16:00:00 UTC**.

Multi-origin prefix:


AS7473 - RPKI Status: 😞

AS9230 - RPKI Status: 😊 - Route objects: **APNIC** and **RADB**

AS9230

202.84.36.0/24

Observation from HE Portal:



HURRICANE ELECTRIC
INTERNET SERVICES

202.84.36.0/24

Quick Links





- [BGP Toolkit Home](#)
- [BGP Prefix Report](#)
- [BGP Peer Report](#)
- [Exchange Report](#)
- [Bogon Routes](#)
- [World Report](#)
- [Multi Origin Routes](#)

Network Info

Whois

DNS

IRR

Announced By		
Origin AS	Announcement	Description
AS9230	202.84.36.0/24  	Internet Service Provider
AS7473	202.84.36.0/24  	Internet Service Provider



AS9230

202.84.36.0/24

Observation from RIPE Portal:



Prefix Overview (202.84.36.0/24)

Routing

information (RIS)

- ✓ Is visible as exact match
- ✓ 1 more/less-specific prefixes are visible

This prefix is announced by:

AS9230 -RPKI Status: 😊
"BOL-BD-AP Bangladesh Online Ltd."

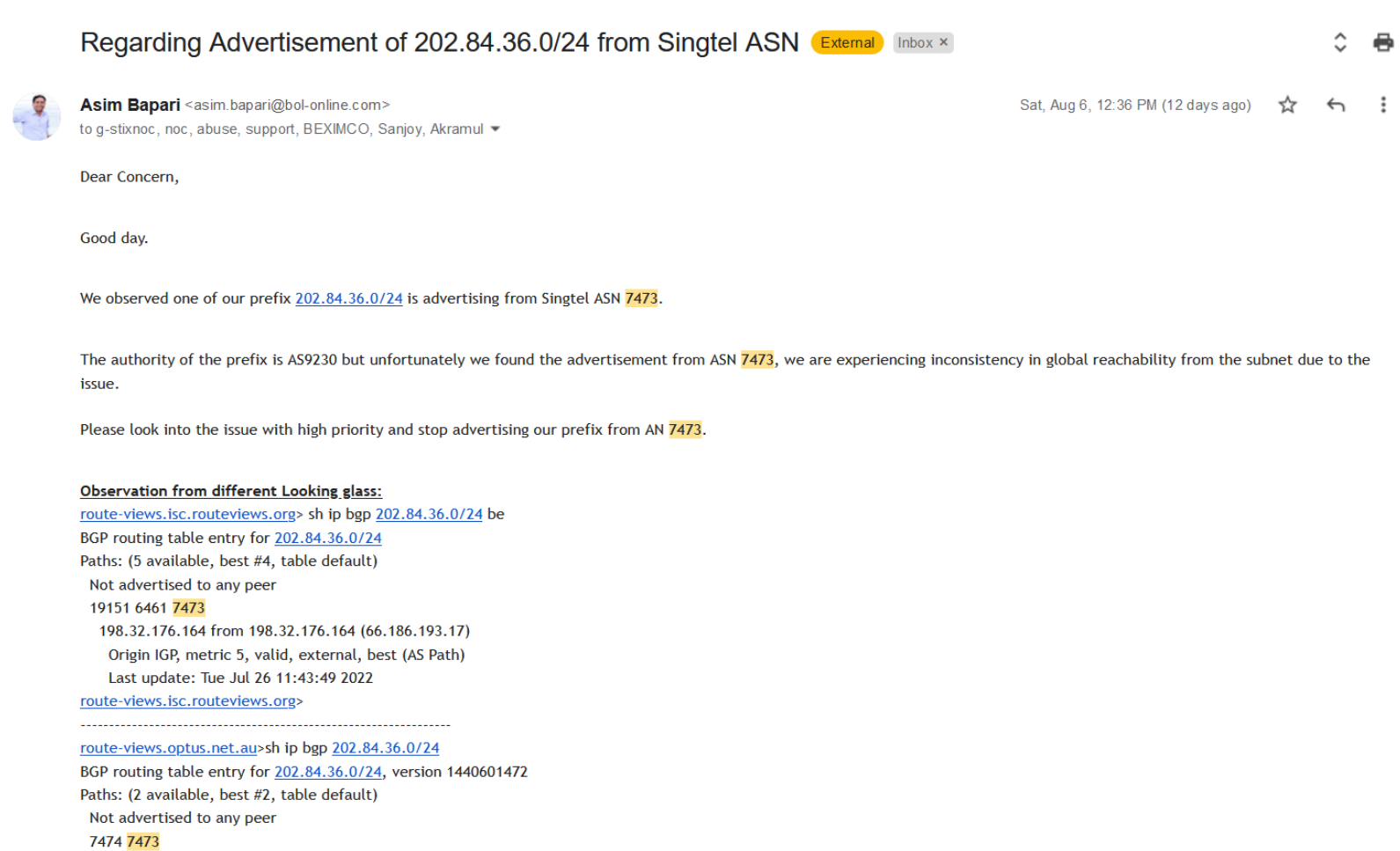
AS7473 -RPKI Status: 😞
"SINGTEL-AS-AP Singapore Telecommunications Ltd"

What to do now ?



Coordination Started :

- First mail to g-stixnoc@singtel.com on 6-Aug-2022, 12:36PM local time



Coordination :

- 1st mail to g-stixnoc@singtel.com on 6-Aug-2022, 12:36PM local time
- 2nd mail to lxxxxxx@singtel.com , cc: g-stixnoc@singtel.com and helpdesk@apnic.net on 6-Aug-2022, 2:04 PM local time
- 3rd mail to Singtel (included some more concern of Singtel) on 10 Aug-2022, 4:14PM

1st Response from Singtel, Asking **SingTel circuit ID** for further process.



Global Customer Support Centre

to manohar.jha@singtel.com, ML-TAC, Kelvin, SVC, keshav.mahadevan@singtel.com, me, stix-noc, Koh, BEXIMCO, Akramul, Sanjoy ▼

Wed, Aug 10, 4:38 PM (8 days ago)



Dear Asim Bapari,

Please assist to provide us the Singtel circuit for further assistance.

Thank you!

Best Regards,



Siti

Technical Assistance Centre (TAC) – Service Desk

Global Delivery - Singtel Enterprise Business

Singapore Telecommunications Limited



Coordination :

2nd Response from Singtel, Asking SingTel circuit ID for further process.



Global Customer Support Centre

to manohar.jha@singtel.com, ML-TAC, Kelvin, SVC, keshav.mahadevan@singtel.com, stix-noc, Koh, BEXIMCO, Akramul, Sanjoy, me ▾

Wed, Aug 10, 5:03 PM (8 days ago)



Dear Asim Bapari,

We will check internally on your below concern.



Thank you!

Best Regards,



Siti

Technical Assistance Centre (TAC) – Service Desk

Global Delivery - Singtel Enterprise Business

Singapore Telecommunications Limited



Coordinating with APNIC :

Mail Sent to APNIC – 6th AUG 2.09 PM



Dear Asim,

Thank you for your email and query.

If you find an incorrect advertisement issue of your IP address prefix by the AS7473, you are welcome to contact the network administrator of AS7473 to report the issue for their further check.

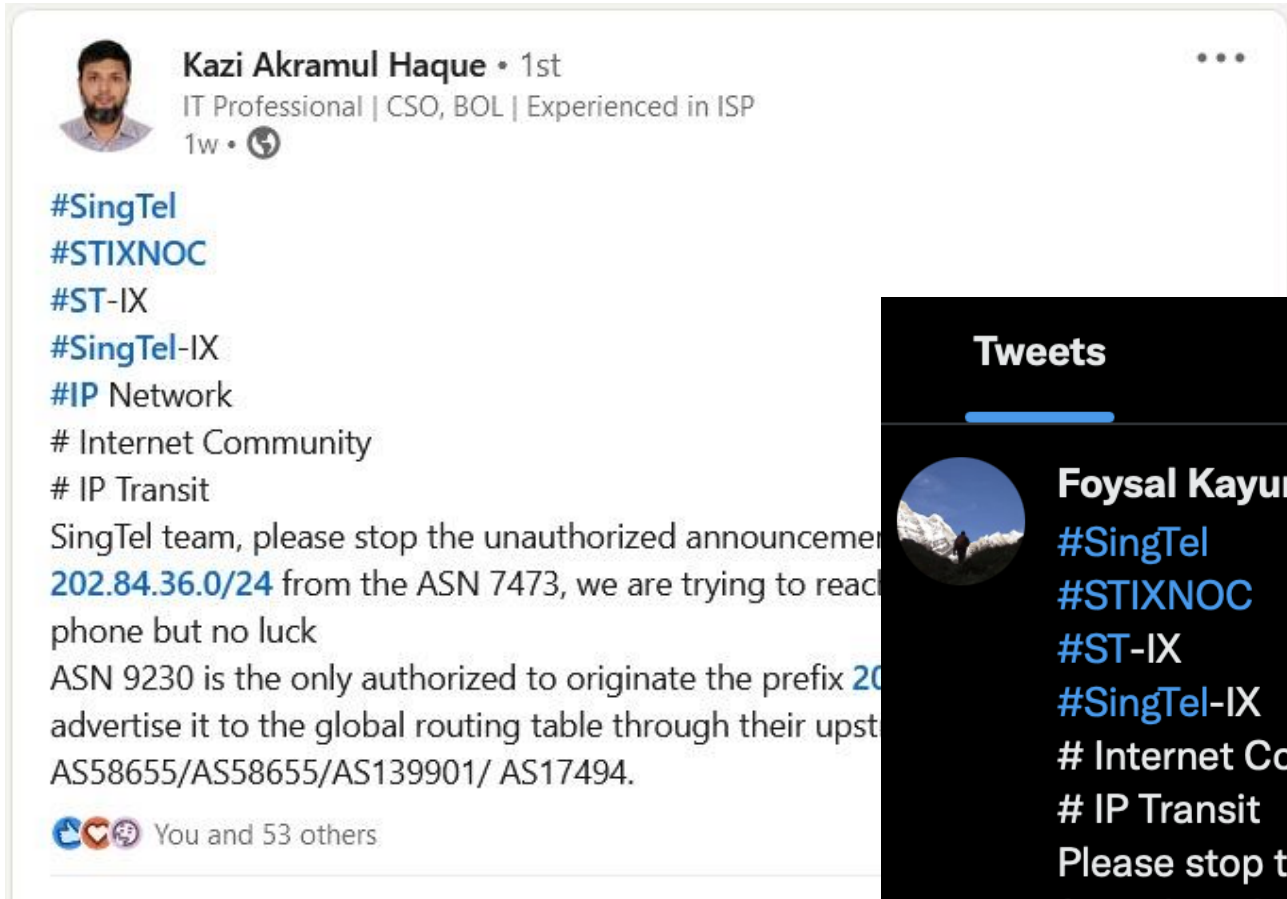
You can find their contact detail, email address and phone number, by querying the AS7473 in the APNIC Whois database below:

<https://wq.apnic.net/apnic-bin/whois.pl>

Regards,



Twitter and Linked-in :



Final Result :

Problem solved from 11-Aug-2022

The ISP noticed it at around 7:00AM



Saturday	Sunday	Monday	Tuesday National Day of Singapore (Holiday)	Wednesday	Thursday	Friday	Saturday
- Holiday in Singapore	- Holiday in Singapore						
6th Aug	7th Aug	8th Aug	9th Aug	10th Aug	11th Aug	12th Aug	13th Aug
Prefix Hijacked - Started Coordinating	<i>Email + Phone</i>	<i>Email + Phone</i>	<i>Email + Phone</i>	Requested through <i>Linkedin & Twitter</i>	Problem Solved		Surprise !!!



What is the Solution ?



MANRS Actions for Network Operators

Action 1: Filtering

Prevent propagation of incorrect routing information

- Implement filters (Inbound/Outbound) on eBGP sessions
- Prevent propagation of incorrect routing information

Action 2: Anti-spoofing

Prevent traffic with spoofed source IP addresses

- Block traffic with spoofed source addresses
- BCP 38 / Unicast reverse path forwarding on interfaces

Action 3: Coordination

Facilitate global operational communication and coordination between network operators

- Communication between network operators
- PeeringDB, route/AS objects, NOC contact details up to date

Action 4: Global Validation

Facilitate validation of routing information on a global scale

- Validation of routing information (IRR)
- Route origination authorization (ROA) and validation



Why and Who will join MANRS -

CTO / CEO / network engineers !!!!



MANRS Observatory

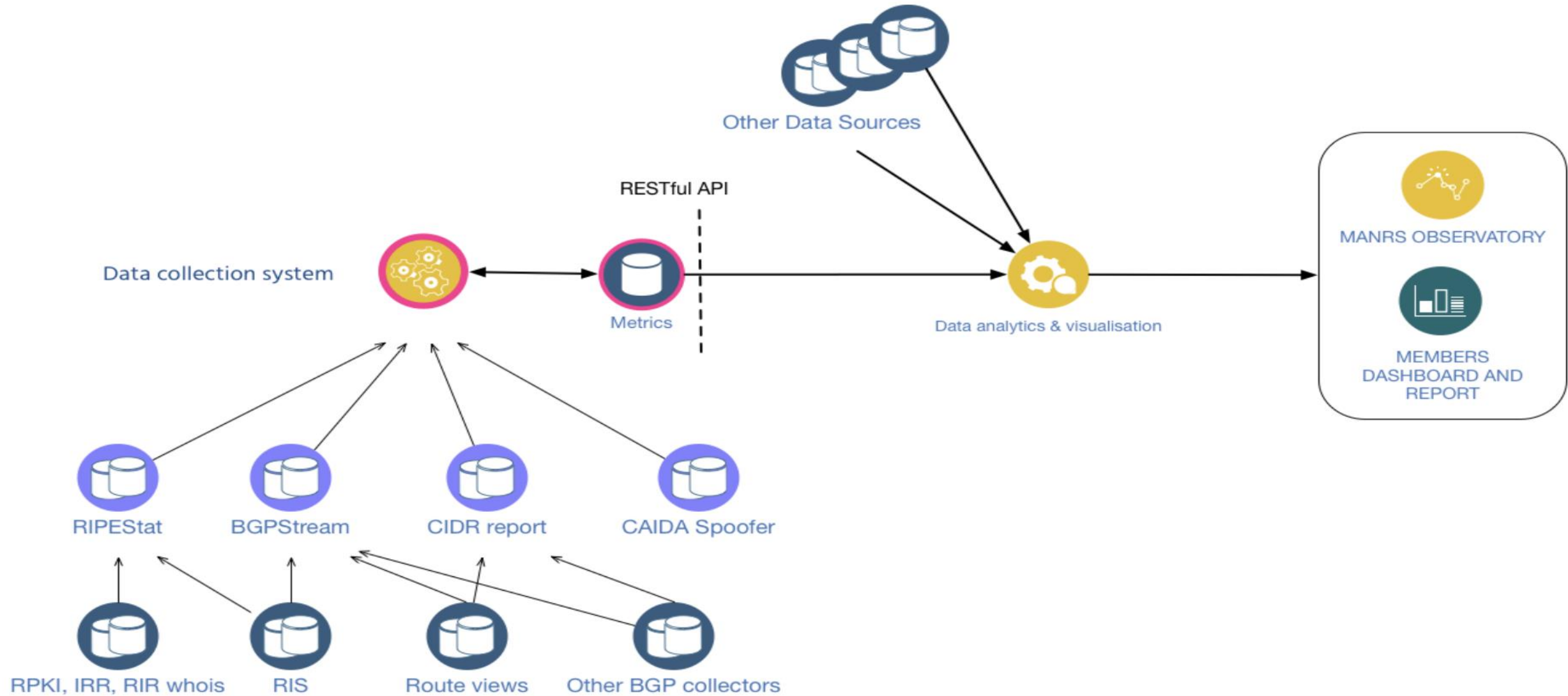
Provide a factual state of security and resilience of the Internet routing system and track it over time

Measurements are:

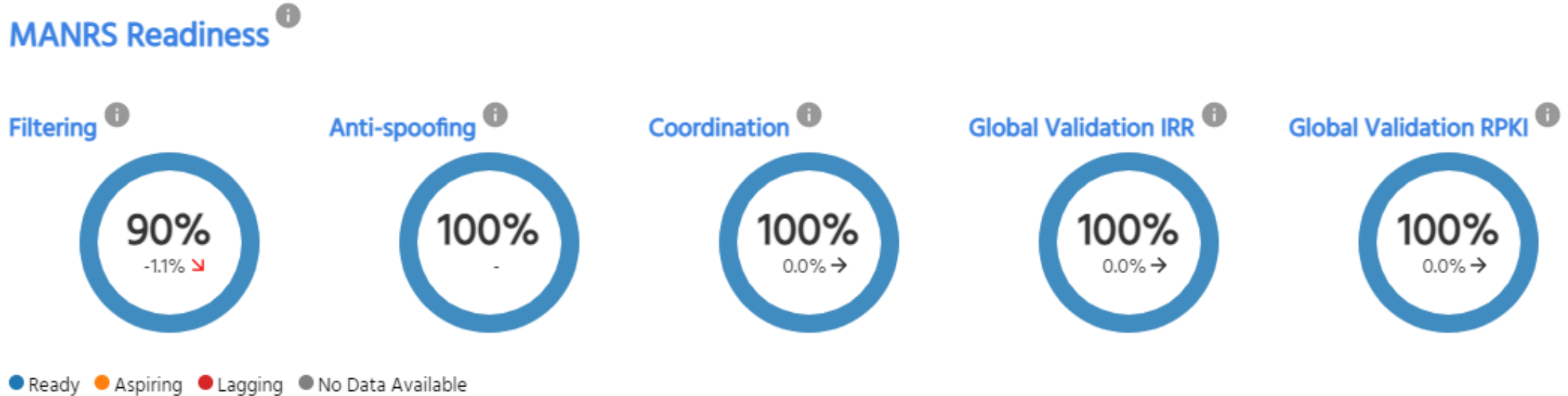
- **Transparent** – using publicly accessible data
- **Passive** – no cooperation from networks required
- **Evolving** – MANRS community decide what gets measured and how



Architecture of the System



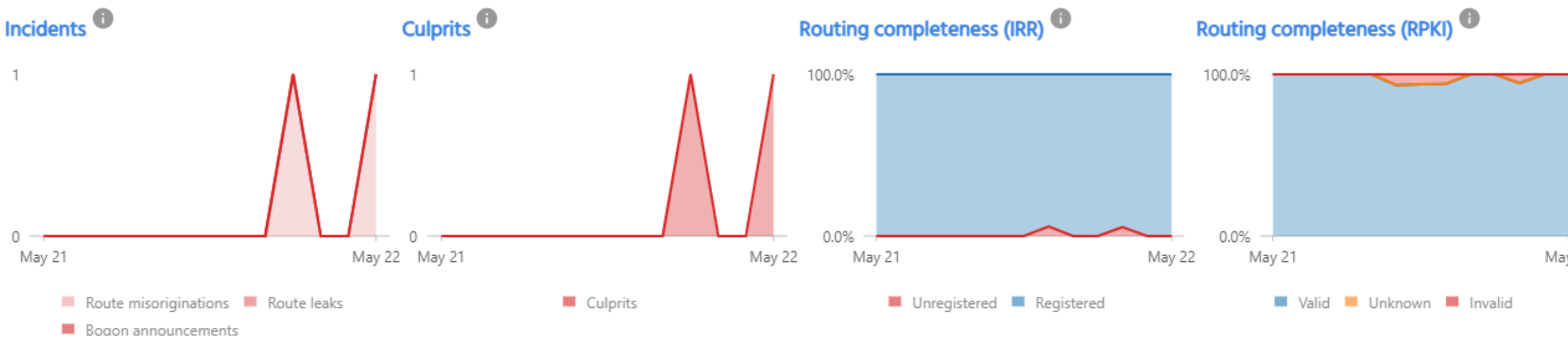
Operator Basis Report (May 2022)



Historical Incidents Data :

History

May 2021 - May 2022



Incidents :

Start Date: 05-04-2022 12-25-00 End Date: 05-04-2022 12-35-00 Duration: 10m, 0s

M2C (GRIP) - Route hijack by a direct customer i



Absolute: 0.5 Normalized: 90% Incident Count: 1

Incident Id: 1 Absolute: 0.5 Start Date: 05-04-2022 12-25-00 End Date: 05-04-2022 12-35-00 Duration: 10m, 0s ⋮ ^

Incident Id	Start Time	End Time	Duration	Prefix	Paths	Weight	Source	Source event
1	2022-04-05 06:25:00	2022-04-05 06:35:00	10m, 0s	103.177.75.0/24	328474 328333 6939 1...	1	grip	moas-1649139900-135597_

Paths

328474 328333 6939 132602 10075 135597
37468 6939 132602 10075 135597



MANRS Conformance Report

2022/05/01 - 2022/05/31

ASN : XXXXXXXXXXXX

MANRS Readiness Scores

Filtering: **90%** ↓
Anti-Spoofing: **100%**
Coordination: **100%**
Global Validation IRR: **100%**
Global Validation RPKI: **100%**

Non-Compliance Incidents

AS Route Misoriginations (GRIP): **1**



Learnings:

- Drop the Invalids.
- Update Whois data periodically.
- Make sure the Call is picked by real person not by any Call Center or IVR.
- Incident/Abuse ticketing should be done for any kind of report (internal/external).
- Inform the Community about the Incident.
- Build secondary coordination channel/community like, MANRS, NOG.



One more thing....



Surprise :

SingTel response on 13-Aug-2022 (problem solved in 11-Aug-2022)

Dear Team,

Please advise if you are still getting an issue on this.

Kindly provide your circuit ID so we can further check.

As of now, we checked from NTT and Singtel looking glass the subnet is no longer advertised from 7473

Have you done any changes from your end?

BGP routing table entry for [202.84.36.0/24](#)

Versions:

Process	bRIB/RIB	SendTblVer
Speaker	336782605	336782605

Last Modified: Aug 12 06:25:28.715 for 1d04h

Paths: (6 available, best #4)

Advertised IPv4 Unicast paths to update-groups (with more than one peer):

0.2 0.3 0.4 0.14

Advertised IPv4 Unicast paths to peers (in unique update groups):

198.64.4.112 4.68.62.129

Path #1: Received by speaker 0

Not advertised to any peer

9498 9498 17494 9230

116.51.31.54 from 116.51.31.54 (203.101.88.34)

Origin IGP, localpref 120, valid, external, group-best

Received Path ID 0, Local Path ID 0, version 0

Community: 2914:370 2914:1405 2914:2406 2914:3400 9498:1 9498:91 9498:9333 9498:9391 9498:17494 34111:9498 34911:9498 40512:9498

Origin-AS validity: valid

Path #2: Received by speaker 0

Not advertised to any peer

9498 9498 17494 9230, (received-only)



Thank You and also thanks to BOL Online

Acknowledgement :

Asim Bapari, Senior Manager, BOL Online,

Indra Raj Basnet, MANRS Fellow

Muhammad Yasir Shamim, MANRS Fellow

