B.P.F

Brasil Peering Forum

MANRS

Introduction to MANRS

Humberto Galiza - Sr. Network Engineer/Architect

Program Comitee - Brasil Peering Forum (BPF)

AONOG/APF 2019

Luanda, Angola, 29 Nov 2019

MANRS

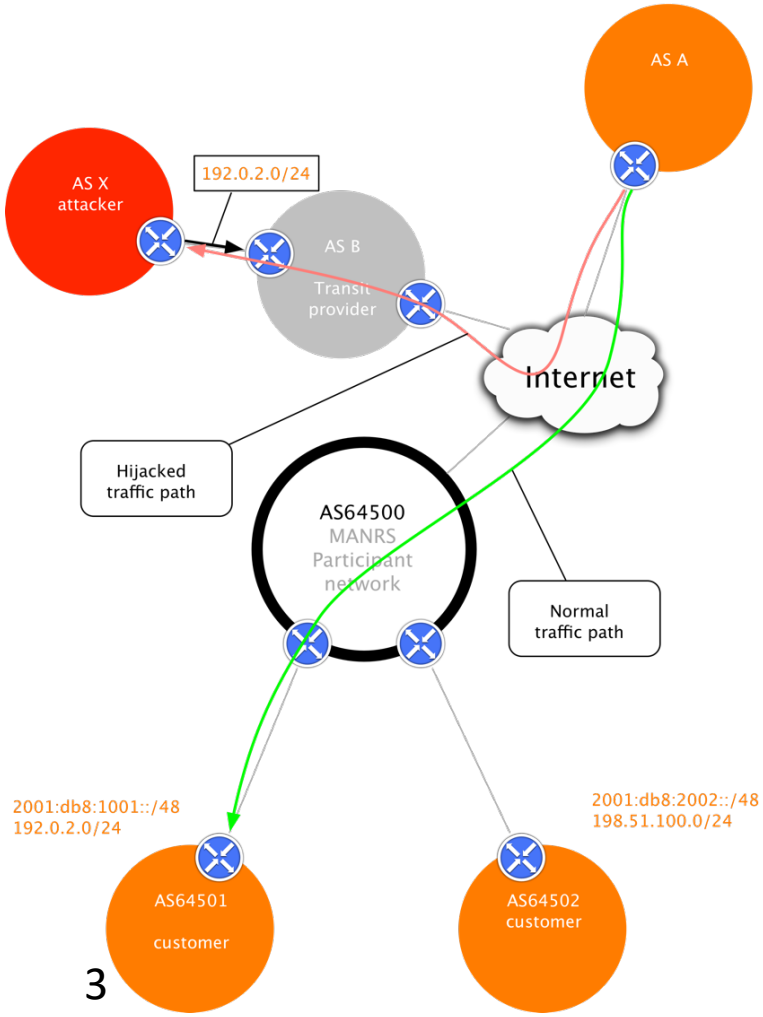
Disclaimer

Opinions expressed are solely my own and do not express the views or opinions of my employer.

Why MANRS

How routing works

- PACKETS
- DESTINATIONS / ANNOUNCEMENTS
- REACHABILITY
- FORWARDING



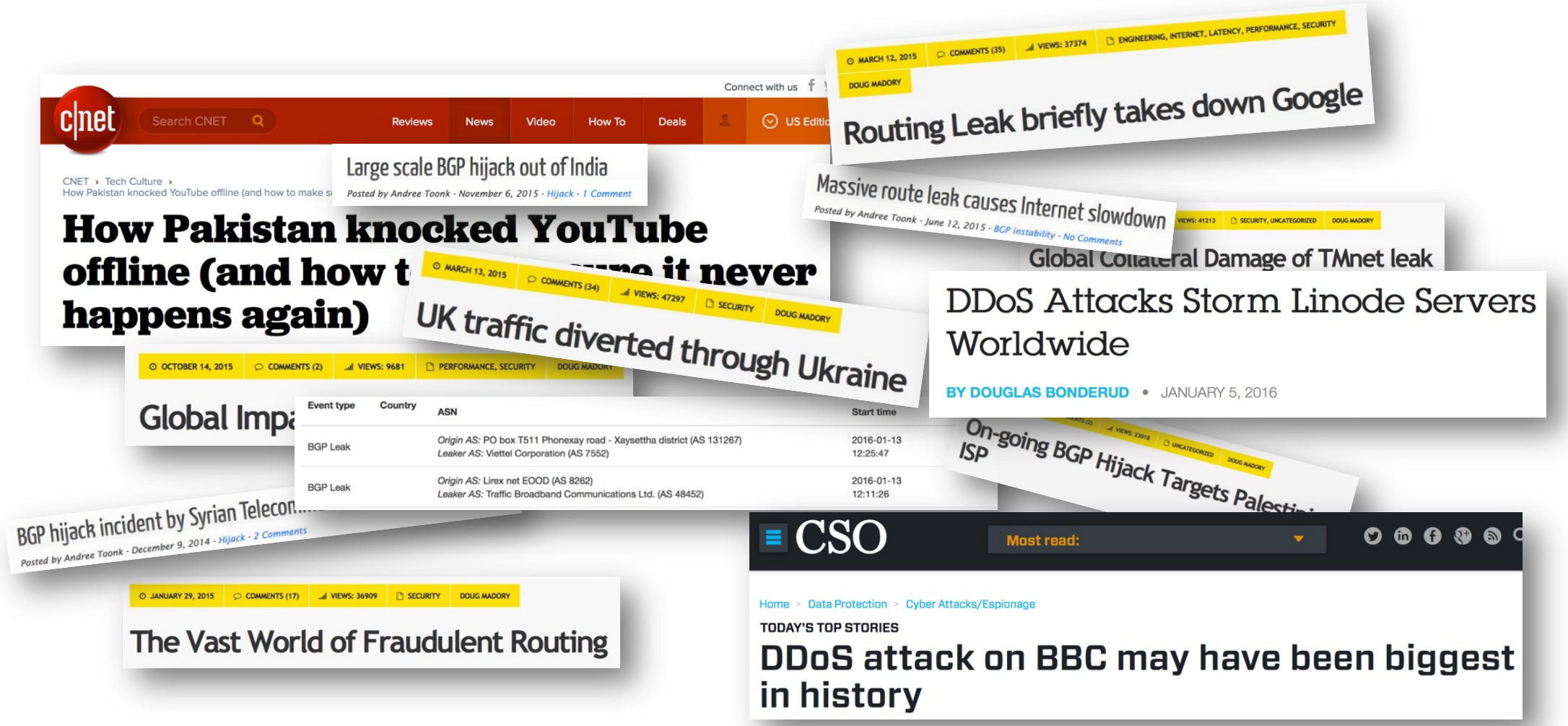
MANRS

What problems are we trying to mitigate: Routing incidents

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*
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 traffic inspection and reconnaissance.	*September 2014. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria.*
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*

MANRS

How users are affected



Event type	Country	ASN	Start time
BGP Leak		*Origin AS:* PO box T511 Phonexay road - Xaysettha district (AS 131267) *Leaker AS:* Viettel Corporation (AS 7552)	2016-01-13 12:25:47
BGP Leak		*Origin AS:* Lirex net EOOD (AS 8262) *Leaker AS:* Traffic Broadband Communications Ltd. (AS 48452)	2016-01-13 12:11:26

B.P.F
Brasil Peering Forum

MANRS

How can MANRS actions prevent incidents:

- MANRS defines four simple but concrete actions that network operators must implement to improve Internet security and reliability.
- The first two operational improvements eliminate the root causes of common routing issues and attacks, while the second two procedural steps improve mitigation and decrease the likelihood of future incidents.

- MANRS builds a visible community of security minded network operators and IXPs

How can MANRS actions prevent incidents: 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

Where are those actions configured and how users are protected?

- Actions 1 BGP configuration
  - core network team
  - network planning & engineering
  - Prevents route leaks & Hijacking
- Action 2 RPF & packet filtering
  - user port configuration
  - service delivery team, process and BCOP implementation
  - DDoS impact
- Action 3 (core team socialization)
- Action 4 core team
  - IRR
  - AFRINIC on RPKI

B.P.F

Brasil Peering Forum

MANRS: Filtering

- 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

- BGP filtering tips:
  - Verify your customer is the owner of the prefix
    - NEVER, EVER, accept any prefixes from your customer!
    - NEVER, EVER, use AS-PATH ACL only
    - 1 customer = 1 prefix list
    - Best practice: prefix-list + as-path checking
    - Use BGP Communities to identify customer prefixes (per location, region, continent, etc)
  - If supported, deploy RPKI for your prefixes

MANRS: Anti-spoofing

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

- Anti-spoofing tips
  - In access networks, use ACLs to block ALL traffic whose source IP DOESN'T belong to your own AS IP addresses
    - Block it as closest as possible of your access customer
  - For transit/peering, filter ALL:
    - Your own prefixes (do not rely only on BGP AS-PATH checking…)
    - ALL BOGONS addresses (RFC1918, RFC6598, RFC1122, RFC2544, RFC5737, etc) from BGP neighbors.

MANRS: Coordination

Coordination

Facilitate global operational communication and coordination between network operators

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

- Coordination tips (for all ASNs)
  - Create (if you still don't have one) and maintain:
    - PeeringDB record: www.peeringdb.com
    - IRR objects: http://www.irr.net/docs/list.html
      - Aut-num, maintainer, route/route6, routing-policy

MANRS: Global Validation

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

- Global Validation tips
  - Join MANRS
    - Submit your data
    - Be engaged, Be part of the community:
      - Join your local/regional/national NOG mailing lists
      - Report misconfigured ASNs so they can take appropriate action!
        - No ones like no MANNERS person, right?

MANRS

WWW.MANRS.ORG

SEARCH

COPY CSV PRINT Show 10 entries

Organization Name	Areas Served	ASNs	Action 1 - Filtering	Action 2 - Anti-Spoofing	Action 3 - Coordination	Action 4 - Global Validation
TDS Telecom	US	4181	✓	✓	✓	✓
Telia Carrier	EU US	1299	✓	✓	✓	✓
TelNet Worldwide, Inc.	US	27553	✓	✓	✓	✓
The George Washington University	US	11039	✓	✓	✓	✓
Three Rivers Optical Exchange (3ROX)	US	5050	✓	✓	✓	✓
TransIP B.V.	NL	20857	✓	✓	✓	
TransWorld Associates Pvt Ltd	PK	38193 45843	✓	✓	✓	✓
Trunk Networks Limited	EU GB	49375	✓		✓	✓
United Information Highway	TH	45796	✓		✓	✓
United Information Highway	TH	38794	✓	✓	✓	✓
Organization Name	**Areas Served**	**ASNs**	**Action 1 - Filtering**	**Action 2 - Anti-Spoofing**	**Action 3 - Coordination**	**Action 4 - Global Validation**

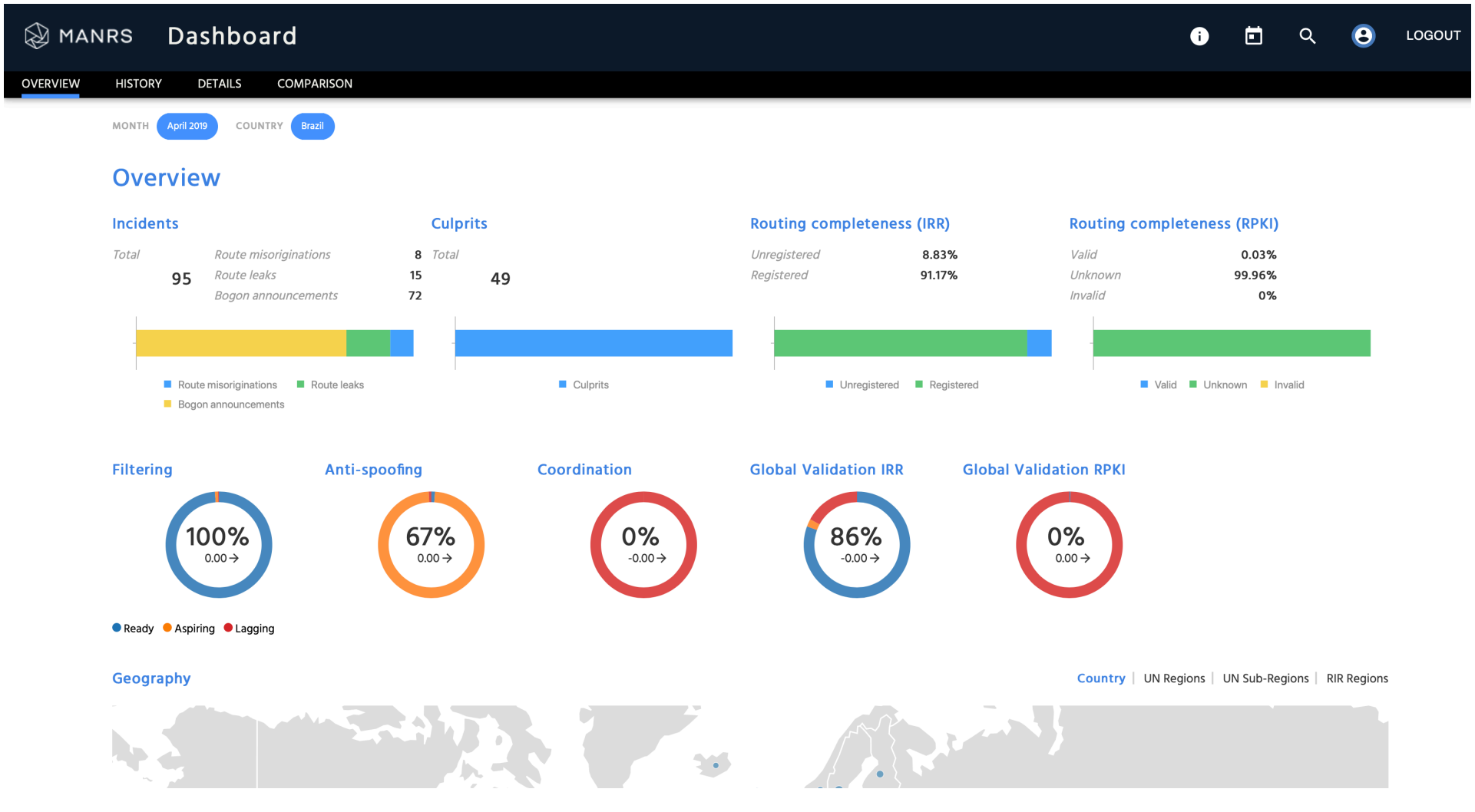
B.P.F
Brasil Peering Forum

MANRS

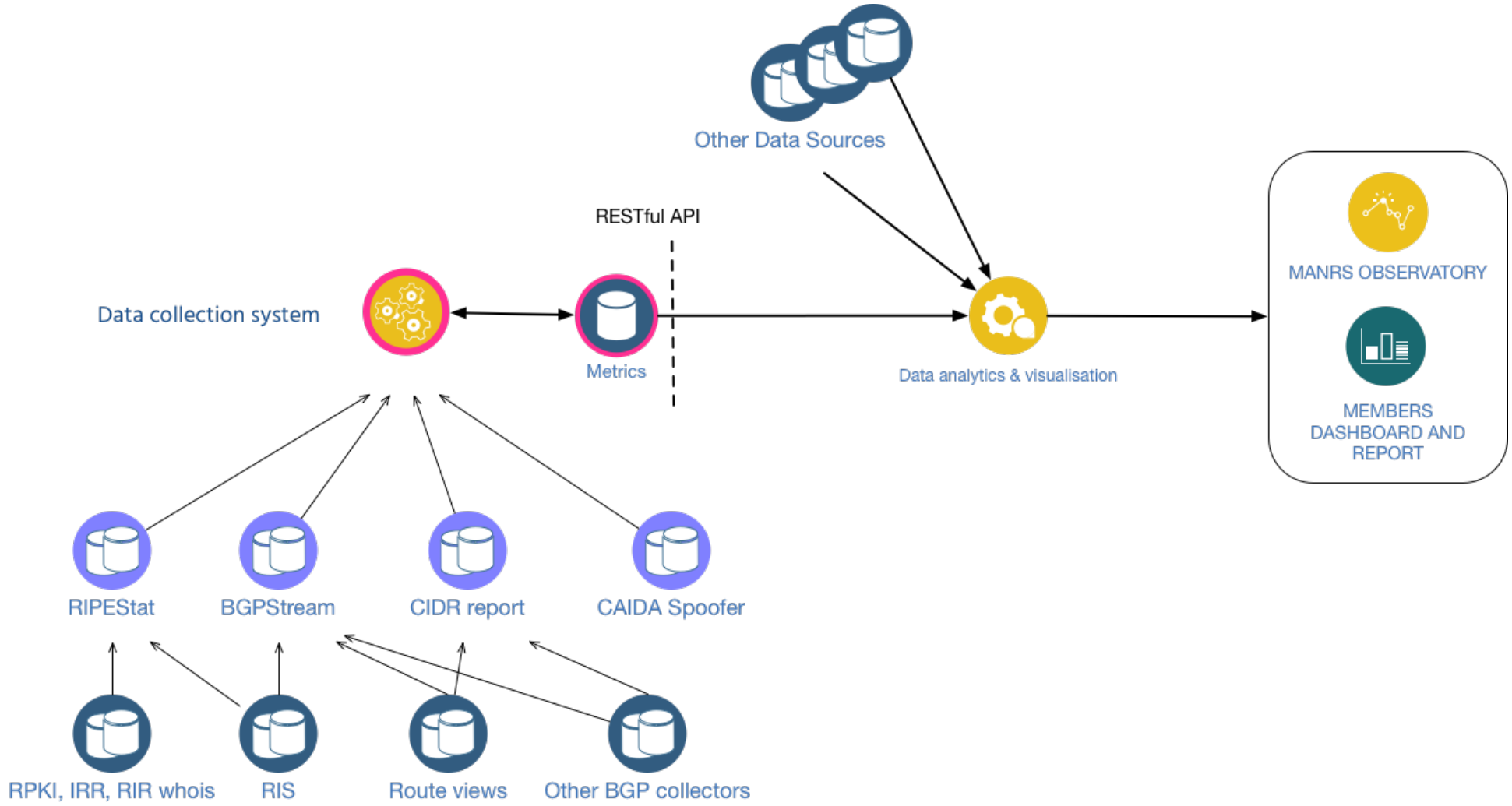
How to use MANRS information for your own benefit

- Where is the information available ?
  - BGP Stream https://bgpstream.com
  - Caida Report http://www.caida.org/data/overview/
  - RIPE Stat
  - CAIDA Spoofer Project https://www.caida.org/projects/spoofer/
  - QRator https://radar.qrator.net/
  - Whois.[RIR].net
  - Afrinic RPKI, IRRs
    - Radb, RIPE, Level3, etc.
    - https://rpki.afrinic.net/
- MANRS observatory https://observatory.manrs.org/

MANRS observatory



MANRS Observatory



MANRS

Practical steps to comply your network with MANRS

- Brazil Peering Forum (BPF) – Author: Marcelo Gondim
  - Published a **PORTUGUESE** ‘how-to’ to guide network operators to easily comply with MANRS – check it out:

    https://wiki.brasilpeeringforum.org/w/MANRS

  - In Brazil we have been working to spread out MANRS word, mainly targeting local/regional ASNs (we have 6000+ only in Brazil!!!)

  - Anyone and any help is really welcome: join our mailing list: https://wiki.brasilpeeringforum.org/w/Participar

B.P.F
Brasil Peering Forum

MANRS

Closing remarks

MANRS is a community effort

CSIRTs can contribute significantly

Message to Network Operators:

”Your security is in someone else’s hands. The actions of others directly impact you and your network security (and vice versa)”

QUESTIONS? CONCERNS? COMMENTS?

B.P.F

Brasil Peering Forum

MANRS

Closing remarks

Special thanks to Christian O'Flearty (ISOC LATAM) and Lucimara Ribeiro (NIC.br) who gently provided some of the material for this presentation.

Thanks for attending AONOG/APF 2019, and see you in 2020!

B.P.F

Brasil Peering Forum