WHY MANRS IS IMPORTANT

Warrick Mitchell
warrick.mitchell@aarnet.edu.au

Introduction to MANRS

Using repositories IRR / RPKI / Peering DB

Facilitate validation of routing information at a global scale

Prevent propagation of incorrect routing information

Prevent traffic with spoofed source IP addresses

Facilitate global operational communication and coordination

WHAT IS MANRS?

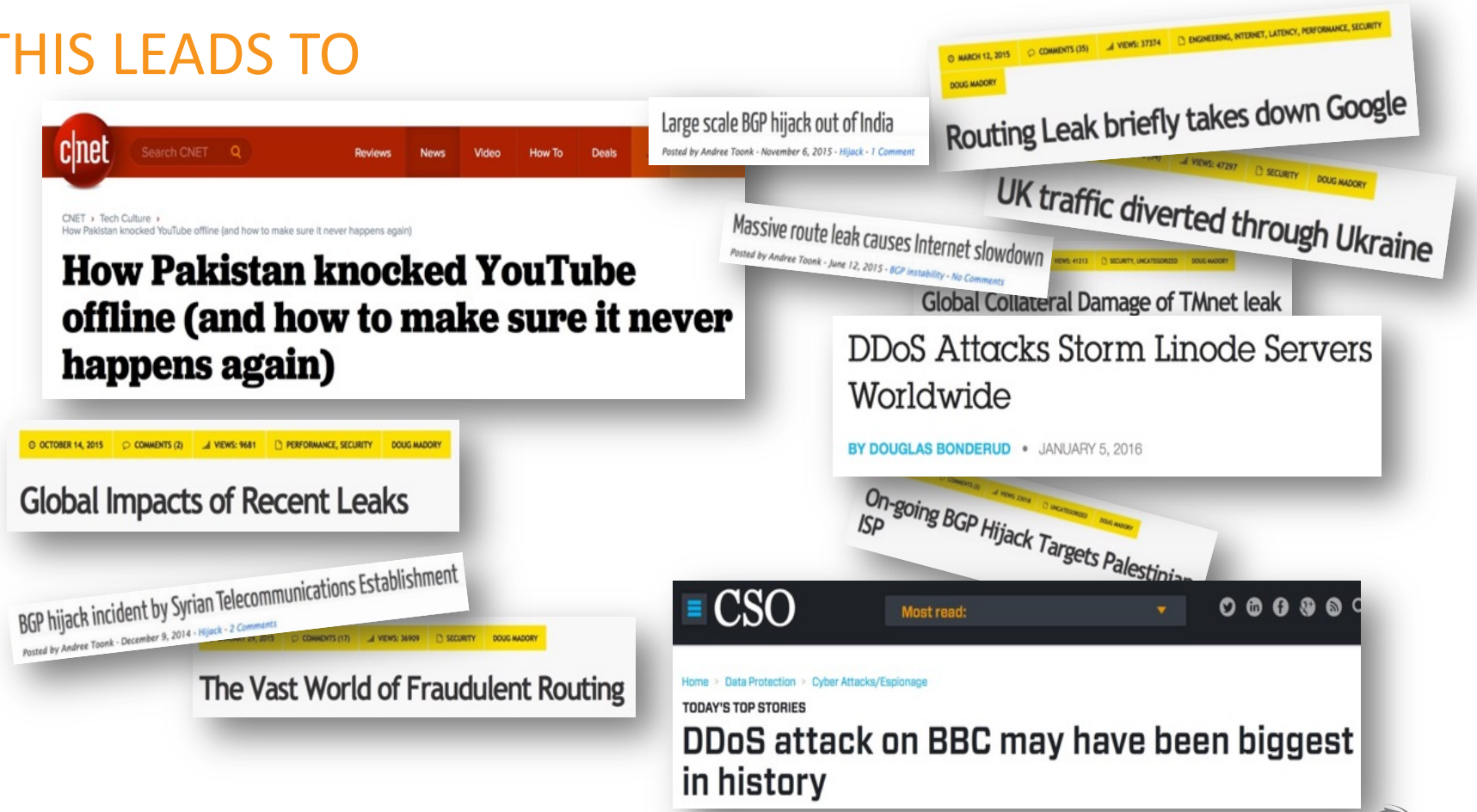
- The Internet's routing foundation has cracks, and they're growing.
- Not a single day goes by without dozens of incidents affecting the routing system.
- Route hijacking, route leaks, IP address spoofing, and other harmful activities can lead to DDoS attacks, traffic inspection, lost revenue, reputational damage, and more.
- These incidents are global in scale, with one operators routing problems cascading to impact others.
- Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society and a number of NRENs like AARNet, that provides crucial fixes to reduce the most common routing threats.

BGP – AN HONOUR SYSTEM

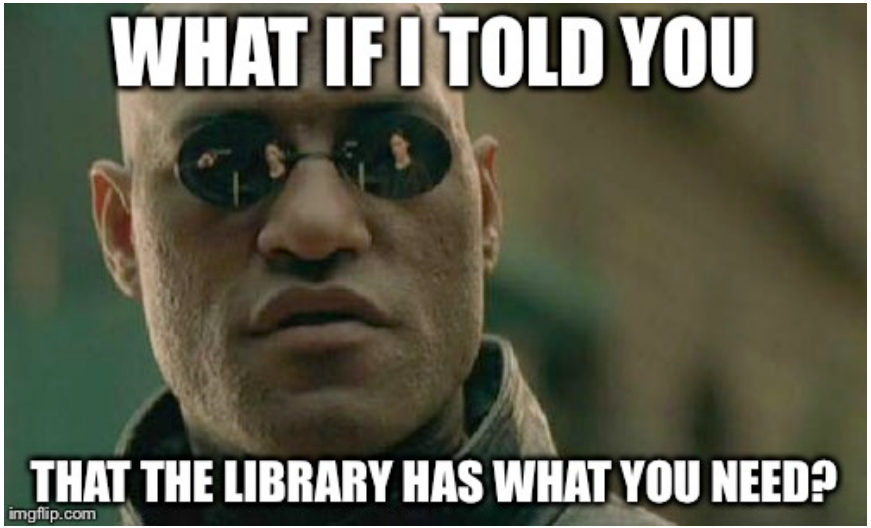
BGP is based on an inherent trust system. I trust you, you trust me, together we exchange routes.

- The protocol was created before security of routes was a considered issue.
- There is an assumption that all routes presented are true and valid
- No built-in validation that updates are legitimate
- The trust chain spans the globe
- Lack of reliable consistent data on the route, its origin etc…

THIS LEADS TO



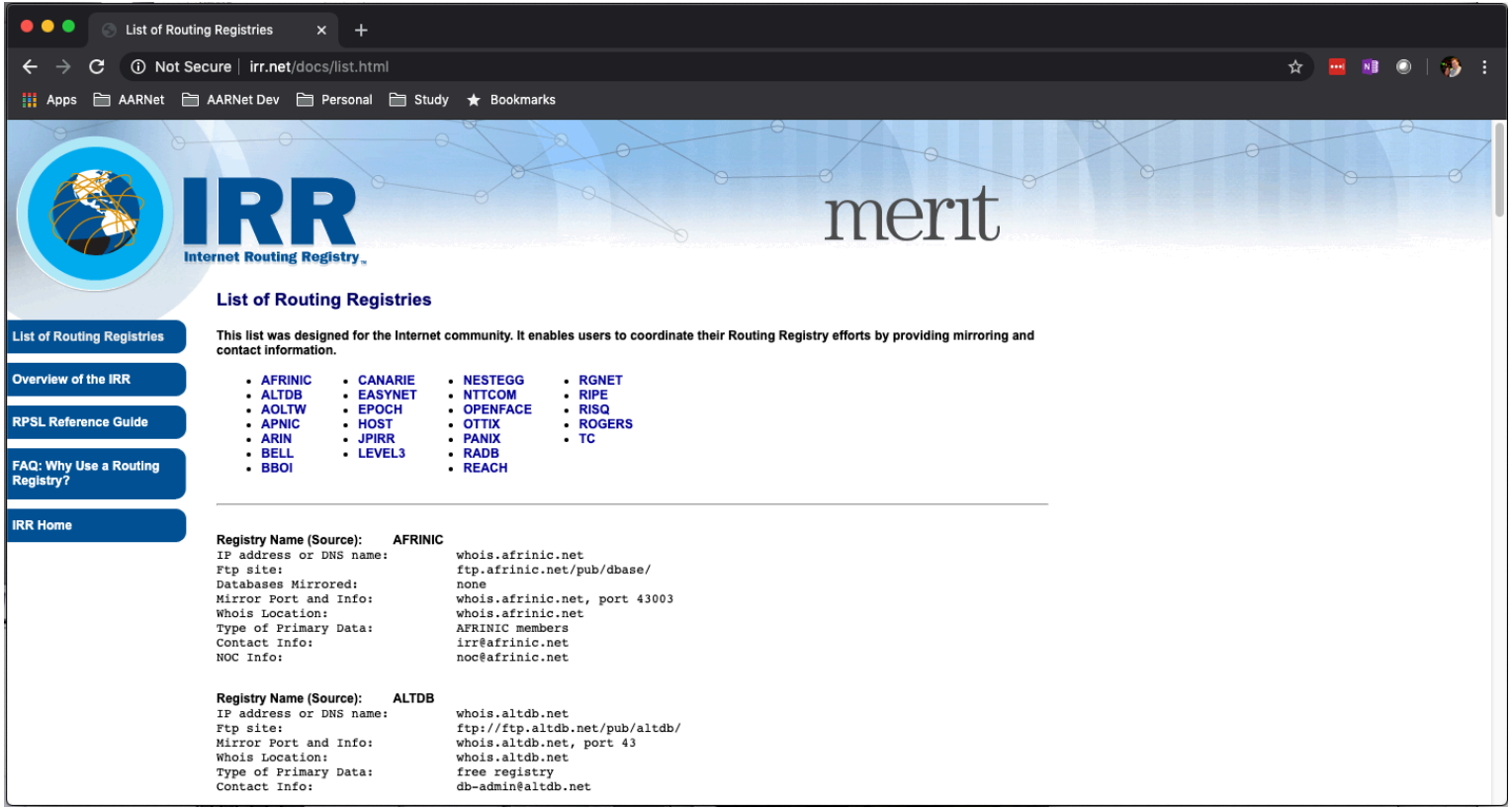
Source: https://www.manrs.org/wp-content/uploads/2018/09/MANRS-Ambassador-Presentation.pptx



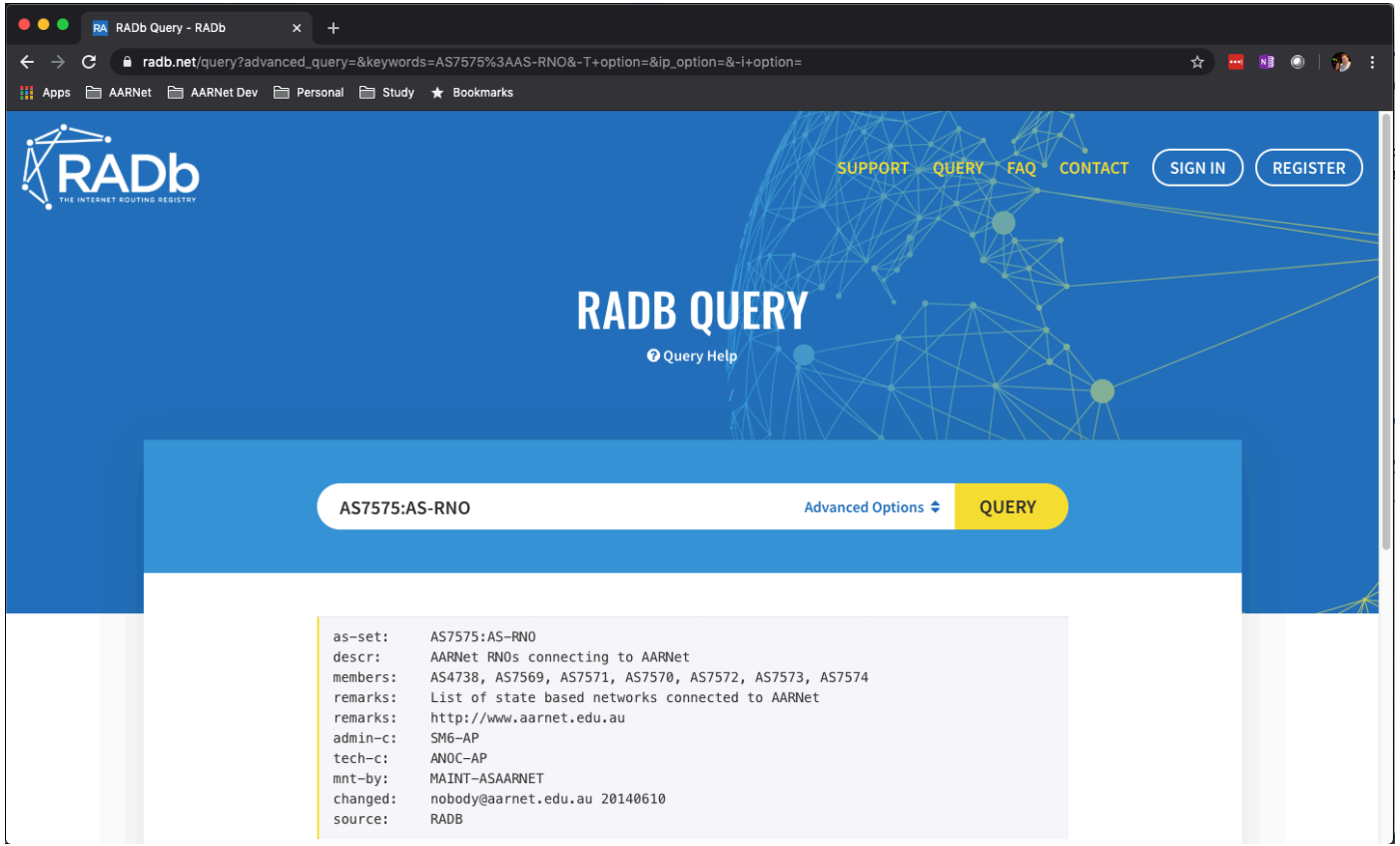
REPOSITORIES OF INFORMATION

Source: https://www.pinterest.com.au/pin/42502790217129995

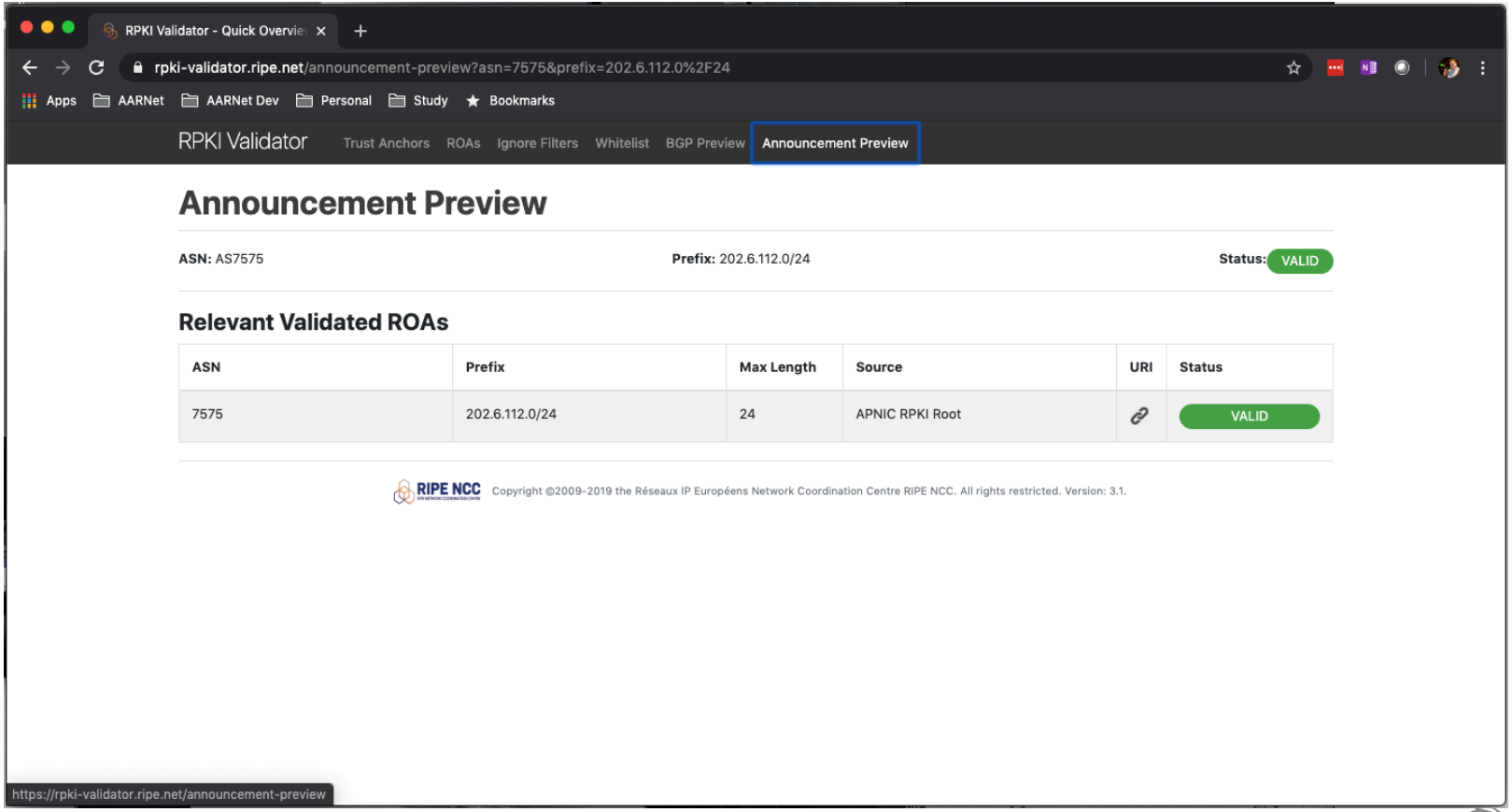
IRR


List of Routing Registries
Not Secure
irr.net/docs/list.html
Apps
AARNet
AARNet Dev
Personal
Study
Bookmarks
IRR
Internet Routing Registry
merit
List of Routing Registries
List of Routing Registries
Overview of the IRR
RPSL Reference Guide
FAQ: Why Use a Routing Registry?
IRR Home
This list was designed for the Internet community. It enables users to coordinate their Routing Registry efforts by providing mirroring and contact information.
AFRINIC
ALTDB
AOLTW
APNIC
ARIN
BELL
BBOI
CANARIE
EASYNET
EPOCH
HOST
JPIRR
LEVEL3
NESTEGG
NTTCOM
OPENFACE
OTTIX
PANIX
RADB
REACH
RGNET
RIPE
RISQ
ROGERS
TC
Registry Name (Source): AFRINIC
IP address or DNS name: whois.afrinic.net
Ftp site: ftp.afrinic.net/pub/dbase/
Databases Mirrored: none
Mirror Port and Info: whois.afrinic.net, port 43003
Whois Location: whois.afrinic.net
Type of Primary Data: AFRINIC members
Contact Info: irr@afrinic.net
NOC Info: noc@afrinic.net
Registry Name (Source): ALTDB
IP address or DNS name: whois.altdb.net
Ftp site: ftp://ftp.altdb.net/pub/altdb/
Mirror Port and Info: whois.altdb.net, port 43
Whois Location: whois.altdb.net
Type of Primary Data: free registry
Contact Info: db-admin@altdb.net

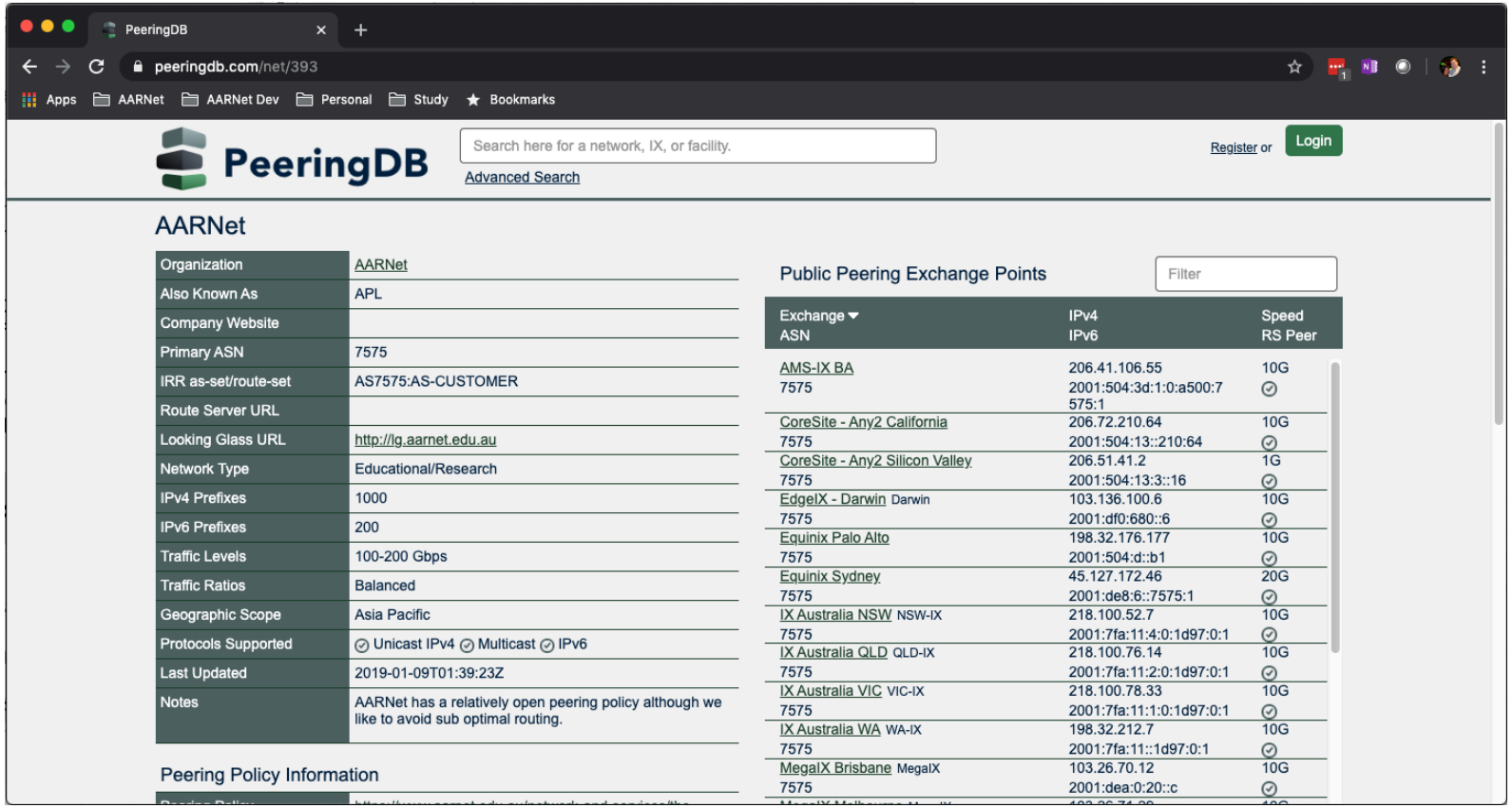
IRR

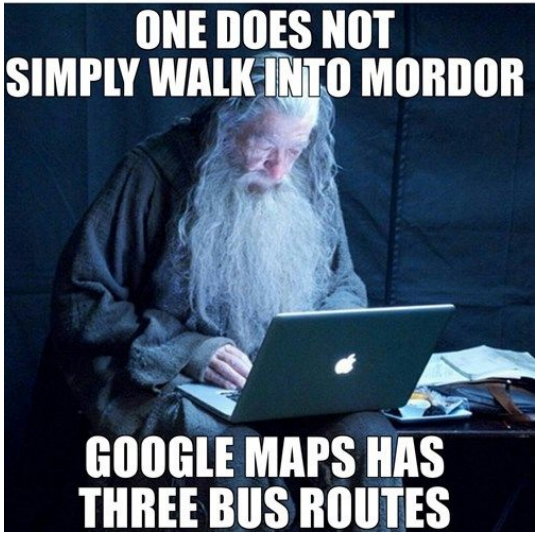

RADb Query - RADb
radb.net/query?advanced_query=&keywords=AS7575%3AAS-RNO&-T+option=&ip_option=&-i+option=
Apps
AARNet
AARNet Dev
Personal
Study
Bookmarks
RADb
THE INTERNET ROUTING REGISTRY
SUPPORT
QUERY
FAQ
CONTACT
SIGN IN
REGISTER
RADB QUERY
Query Help
AS7575:AS-RNO
Advanced Options
QUERY
as-set: AS7575:AS-RNO
descr: AARNet RNOs connecting to AARNet
members: AS4738, AS7569, AS7571, AS7570, AS7572, AS7573, AS7574
remarks: List of state based networks connected to AARNet
remarks: http://www.aarnet.edu.au
admin-c: SM6-AP
tech-c: ANOC-AP
mnt-by: MAINT-ASAARNET
changed: nobody@aarnet.edu.au 20140610
source: RADB

RPKI


RPKI Validator - Quick Overvie
rpki-validator.ripe.net/announcement-preview?asn=7575&prefix=202.6.112.0%2F24
Apps
AARNet
AARNet Dev
Personal
Study
Bookmarks
RPKI Validator
Trust Anchors
ROAs
Ignore Filters
Whitelist
BGP Preview
Announcement Preview
Announcement Preview
ASN: AS7575
Prefix: 202.6.112.0/24
Status: VALID
Relevant Validated ROAs
ASN
Prefix
Max Length
Source
URI
Status
7575
202.6.112.0/24
24
APNIC RPKI Root
VALID
RIPE NCC
Copyright ©2009-2019 the Réseaux IP Européens Network Coordination Centre RIPE NCC. All rights restricted. Version: 3.1.
https://rpki-validator.ripe.net/announcement-preview

PEERINGDB


PeeringDB
peeringdb.com/net/393
Apps
AARNet
AARNet Dev
Personal
Study
Bookmarks
PeeringDB
Search here for a network, IX, or facility.
Advanced Search
Register or
Login
AARNet
Organization
AARNet
Also Known As
APL
Company Website
Primary ASN
7575
IRR as-set/route-set
AS7575:AS-CUSTOMER
Route Server URL
Looking Glass URL
http://lg.aarnet.edu.au
Network Type
Educational/Research
IPv4 Prefixes
1000
IPv6 Prefixes
200
Traffic Levels
100-200 Gbps
Traffic Ratios
Balanced
Geographic Scope
Asia Pacific
Protocols Supported
Unicast IPv4 Multicast IPv6
Last Updated
2019-01-09T01:39:23Z
Notes
AARNet has a relatively open peering policy although we like to avoid sub optimal routing.
Peering Policy Information
Public Peering Exchange Points
Filter
Exchange
ASN
IPv4
IPv6
Speed
RS Peer
AMS-IX BA
206.41.106.55
10G
7575
2001:504:3d:1:0:a500:7575:1
CoreSite - Any2 California
206.72.210.64
10G
7575
2001:504:13::210:64
CoreSite - Any2 Silicon Valley
206.51.41.2
1G
7575
2001:504:13:3::16
EdgeIX - Darwin Darwin
103.136.100.6
10G
7575
2001:df0:680::6
Equinix Palo Alto
198.32.176.177
10G
7575
2001:504:d::b1
Equinix Sydney
45.127.172.46
20G
7575
2001:de8:6::7575:1
IX Australia NSW NSW-IX
218.100.52.7
10G
7575
2001:7fa:11:4:0:1d97:0:1
IX Australia QLD QLD-IX
218.100.76.14
10G
7575
2001:7fa:11:2:0:1d97:0:1
IX Australia VIC VIC-IX
218.100.78.33
10G
7575
2001:7fa:11:1:0:1d97:0:1
IX Australia WA WA-IX
198.32.212.7
10G
7575
2001:7fa:11::1d97:0:1
MegaIX Brisbane MegaIX
103.26.70.12
10G
7575
2001:dea:0:20::c



PREVENT PROPAGATION OF INCORRECT ROUTING INFORMATION

Source: https://www.pinterest.com.au/pin/42502790217129995

aarnet

ROUTE HIJACKING

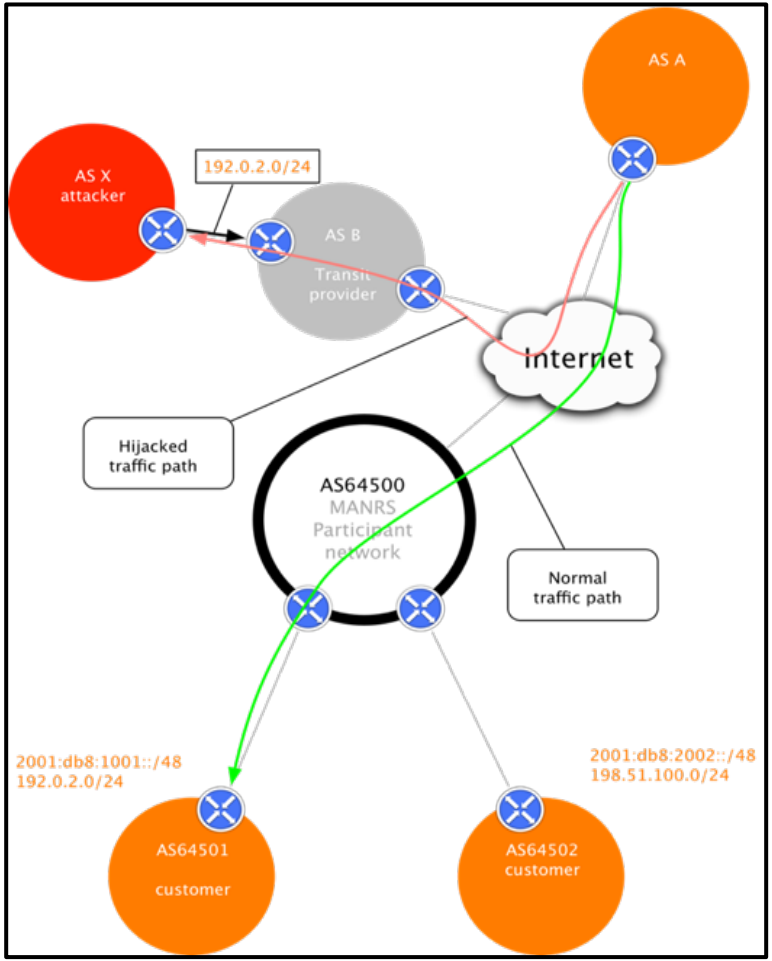
Example:

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).

AS-Path, Prefix Lists, Prefix-limits, Using RPSL, Route Validation (RPKI/ROAs)



Source: https://www.manrs.org/wp-content/uploads/2018/09/MANRS-Ambassador-Presentation.pptx

aarnet

WHY DOES AARNET CARE?

An example of why we care, is that in December 2018, one of our clients /16 was announced by an ISP in the US for approximately 24hrs, which resulted in their traffic to Google failing completely (No Gmail, Youtube, Search, Drive etc). But all other traffic was working.

- The customer reached out to AARNet about the fault
- AARNet reached out to Google to find out why the traffic wasn't being returned
- Google advised they were receiving our clients /16 via from an ISP in the US who had a direct connection to Google, which they were not filtering, which resulted in Google preferring to send traffic back to the ISP in the US rather than to AARNet and the real client due to a shorter AS-Path length.
- Luckily, we were able to contact the ISP in the US and ask them to cease announcing the route, which they did, restoring connectivity to our client.

PREVENT TRAFFIC WITH SPOOFED SOURCE IP ADDRESSES

Source: https://scifi.stackexchange.com/questions/35262/where-did-you-shall-not-pass-come-from

IP ADDRESS SPOOFING

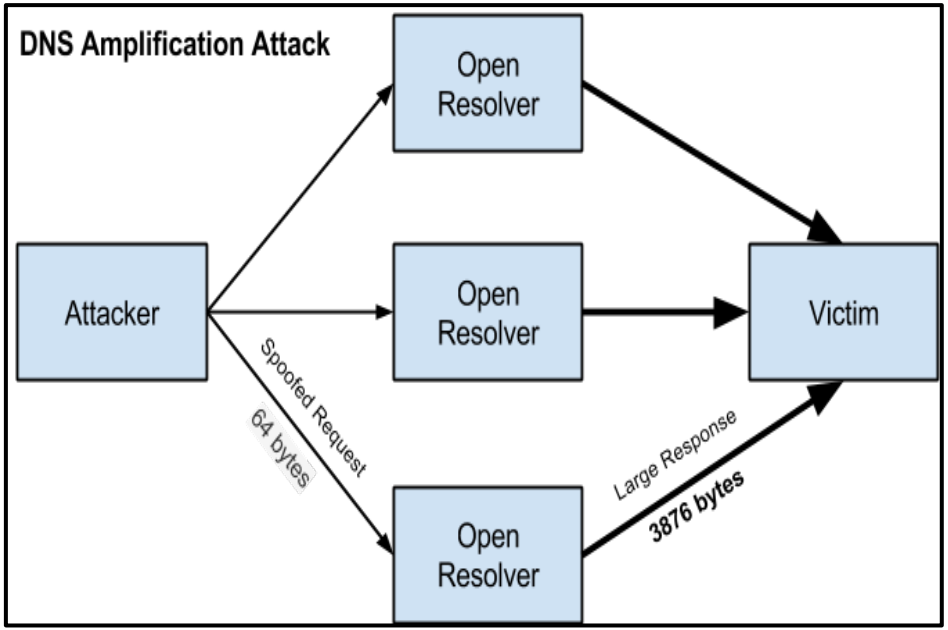
Example:

DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack.

Fix:

Source address validation: systems for source address validation can help tell if the end users and customer networks have correct source IP addresses (combined with filtering).

URPF, ACLs can be utilized to achieve this.



Source: https://www.manrs.org/wp-content/uploads/2018/09/MANRS-Ambassador-Presentation.pptx

TEST YOURSELF!

https://spoofer.caida.org/summary.php

Don’t just test your office links, test your client’s links as well!

Use automation to make sure your filters are in place across all interfaces to stop spoofing!

SPOOFING BY COUNTRY!

Country	Client IP blocks	Spoofing IP blocks	Blocking IP blocks		Inconsistent IP blocks	Client ASNs	Spoofing ASNs
			Non-NAT	NAT			
bra (Brazil)	2358	457 (19.4%)	274 (11.6%)	1612 (68.4%)	15 (0.6%)	398	201 (50.5%)
ind (India)	1624	452 (27.8%)	192 (11.8%)	979 (60.3%)	1 (0.1%)	58	15 (25.9%)
usa (United States)	4659	210 (4.5%)	1115 (23.9%)	3330 (71.5%)	4 (0.1%)	492	115 (23.4%)
tha (Thailand)	493	44 (8.9%)	22 (4.5%)	427 (86.6%)	0 (0.0%)	22	5 (22.7%)
egy (Egypt)	135	44 (32.6%)	3 (2.2%)	88 (65.2%)	0 (0.0%)	3	2 (66.7%)
kor (South Korea)	809	35 (4.3%)	466 (57.6%)	308 (38.1%)	0 (0.0%)	38	7 (18.4%)
ita (Italy)	294	34 (11.6%)	20 (6.8%)	240 (81.6%)	0 (0.0%)	46	16 (34.8%)
arg (Argentina)	166	33 (19.9%)	15 (9.0%)	118 (71.1%)	0 (0.0%)	31	7 (22.6%)
chl (Chile)	160	33 (20.6%)	9 (5.6%)	118 (73.8%)	0 (0.0%)	28	12 (42.9%)
gbr (United Kingdom)	984	32 (3.3%)	133 (13.5%)	819 (83.2%)	0 (0.0%)	105	22 (21.0%)
nld (Netherlands)	535	31 (5.8%)	148 (27.7%)	356 (66.5%)	0 (0.0%)	99	18 (18.2%)
mys (Malaysia)	174	28 (16.1%)	11 (6.3%)	135 (77.6%)	0 (0.0%)	11	3 (27.3%)
irn (Iran)	125	28 (22.4%)	10 (8.0%)	86 (68.8%)	1 (0.8%)	23	6 (26.1%)
deu (Germany)	1226	24 (2.0%)	316 (25.8%)	885 (72.2%)	1 (0.1%)	77	15 (19.5%)
are (United Arab Emirates)	69	23 (33.3%)	15 (21.7%)	31 (44.9%)	0 (0.0%)	6	3 (50.0%)
can (Canada)	560	22 (3.9%)	93 (16.6%)	444 (79.3%)	1 (0.2%)	71	18 (25.4%)
zaf (South Africa)	274	21 (7.7%)	31 (11.3%)	221 (80.7%)	1 (0.4%)	48	15 (31.3%)
isr (Israel)	206	20 (9.7%)	8 (3.9%)	178 (86.4%)	0 (0.0%)	17	4 (23.5%)
rus (Russian Federation)	209	19 (9.1%)	40 (19.1%)	150 (71.8%)	0 (0.0%)	76	12 (15.8%)
fra (France)	418	18 (4.3%)	63 (15.1%)	336 (80.4%)	1 (0.2%)	54	12 (22.2%)
aus (Australia)	634	16 (2.5%)	53 (8.4%)	564 (89.0%)	1 (0.2%)	54	13 (24.1%)

Source: https://spoofer.caida.org/country_stats.php

FACILITATE GLOBAL OPERATIONAL COMMUNICATION AND COORDINATION

Source: https://www.teepublic.com/t-shirt/1920078-stranger-things-who-you-gonna-call

COMMUNICATION CHANNELS

Your security is in someone else's hands.

Why should they help you? You can start by helping them.

- Is your WHOIS/IRR/ABUSE contacts up to date?
- PeeringDB?
- IRR (RADB/MERIT)?
- APNIC/ARIN/AFRINIC/LACNIC/RIPE NCC?

Where is the line between good and bad routing security?

We need globally recognized security expectations for all network operators to raise the bar on routing security.

FACILITATE VALIDATION OF ROUTING INFORMATION AT A GLOBAL SCALE

Source: https://blog.apnic.net/2017/06/27/improving-route-roa-management-myapnic/

aarnet

ROUTE VALIDATION

AT&T/as7018 now drops invalid prefixes from peers

From: Jay Borkenhagen <jayb () braeburn org>
Date: Mon, 11 Feb 2019 09:53:45 -0500

FYI:

The AT&T/as7018 network is now dropping all RPKI-invalid route announcements that we receive from our peers.

We continue to accept invalid route announcements from our customers, at least for now. We are communicating with our customers whose invalid announcements we are propagating, informing them that these routes will be accepted by fewer and fewer networks over time.

Thanks to those of you who are publishing ROAs in the RPKI. We would also like to encourage other networks to join us in taking this step to improve the quality of routing information in the Internet.

Thanks!

Jay B.

ROUTE VALIDATION

```
[wdm@gingernut ~]$ whois 202.6.112.0/24 -h whois.bgpmon.net
[snip]
% For more information visit:
% https://portal.bgpmon.net/bgpmonapi.php


Prefix:             202.6.112.0/24
Prefix description: AARNet Office LAN, Perth, WA
Country code:       AU
Origin AS:          7575
Origin AS Name:     AARNET-AS-AP Australian Academic and Research Network (AARNet), AU
RPKI status:        ROA validation successful
First seen:         2011-10-19
Last seen:          2019-12-17
Seen by #peers:     56
```

ROUTE VALIDATION

```
[wdm@gingernut ~]$ whois 138.44.16.0/24 -h whois.bgpmon.net
[snip]
% For more information visit:
% https://portal.bgpmon.net/bgpmonapi.php


Prefix:              138.44.16.0/23
Prefix description:  RSP, NSWRNO, AARNET
Country code:        AU
Origin AS:           7570
Origin AS Name:      AARNET-NSW-RNO Australian Academic and Research Network (AARNet), AU
RPKI status:         ROA validation failed: Invalid Origin ASN, expected 7575
First seen:          2019-02-23
Last seen:           2019-12-17
Seen by #peers:      47
```

ROUTE VALIDATION

https://sg-pub.ripe.net/jasper/rpki-web-test/

WE HAVE TO WORK TOGETHER

The more we all work together to build a hardy, secure global routing infrastructure the better it will be for all.

There would be less incidents due to fat fingers and malicious actors and the damage these issues could cause would have a smaller blast radius.

So there are no excuses, join MANRS now!

REFERENCES

- Recommended Internet Service Provider Security Services and Procedures, Section Network Infrastructure, http://www.rfc-editor.org/bcp/bcp46.txt
- BGP operations and security, https://datatracker.ietf.org/doc/rfc7454/
- Border Gateway Protocol Security, NIST: Special Publication SP 800-54, http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf
- Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure, http://tools.ietf.org/html/rfc3871
- Using RPSL in Practice, http://tools.ietf.org/html/rfc2650
- Using the RIPE Database as an Internet Routing Registry, https://labs.ripe.net/Members/denis/using-the-ripe-database-as-an-internet-routing-registry
- BGP Security Best Practices, FCC CSRIC III WG4 Final Report, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf
- Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, http://tools.ietf.org/html/bcp38
- Ingress Filtering for Multihomed Networks, http://tools.ietf.org/html/bcp84
- Securing the Edge, http://www.icann.org/committees/security/sac004.txt
- RIPE Anti-Spoofing Task Force HOW-TO, http://www.ripe.net/ripe/docs/ripe-431
- Peering DB, https://www.peeringdb.com
- RADB, http://www.radb.net/
- Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)", http://www.rfc-editor.org/bcp/bcp185.txt

Source: https://www.manrs.org/manrs/

THANK YOU

Warrick Mitchell

warrick.mitchell@aarnet.edu.au