APNIC 42

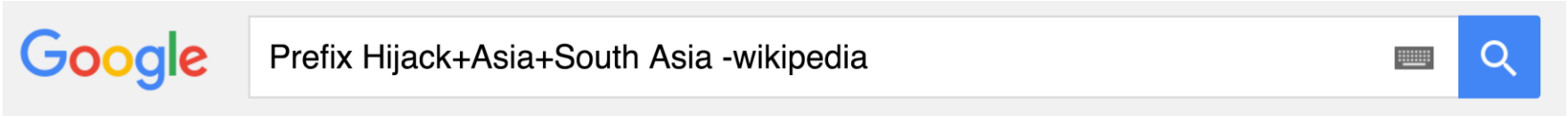
Securing the Global Routing System and the Approach of Operators

Adli Wahid
Security Specialist
adli@apnic.net

COLOMBO, SRI LANKA
28 September – 5 October 2016

#apnic42

Incidents



Motivations!

The New Threat: Targeted Internet Traffic Misdirection

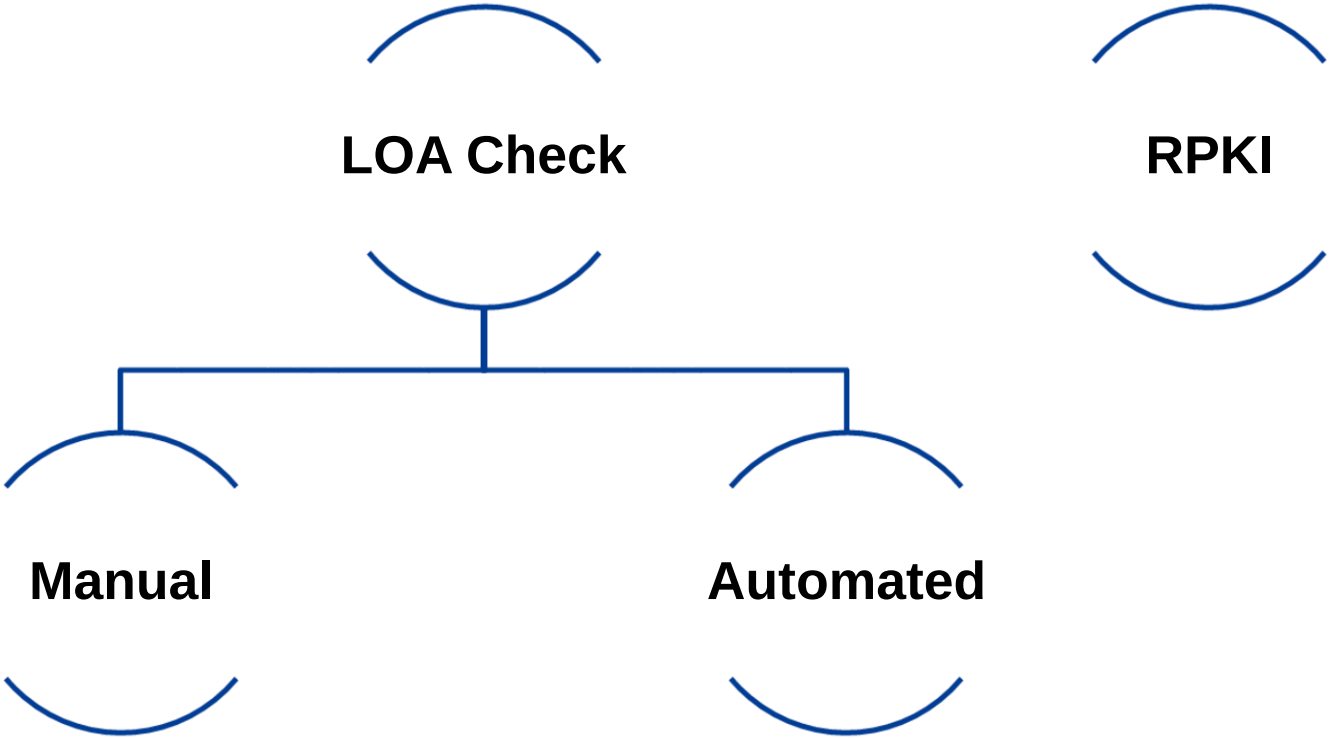
Traffic interception has certainly been a hot topic in 2013. The world has been focused on interception carried out the old fashioned way, by getting into the right buildings and listening to the right cables. But there's actually been a significant uptick this year in a completely different kind of attack, one that can be carried out by anybody, at a distance, using Internet route hijacking.

After consultations with many of the affected parties, we're coming forth with some details in the hope that we can make this particular vulnerability obsolete.

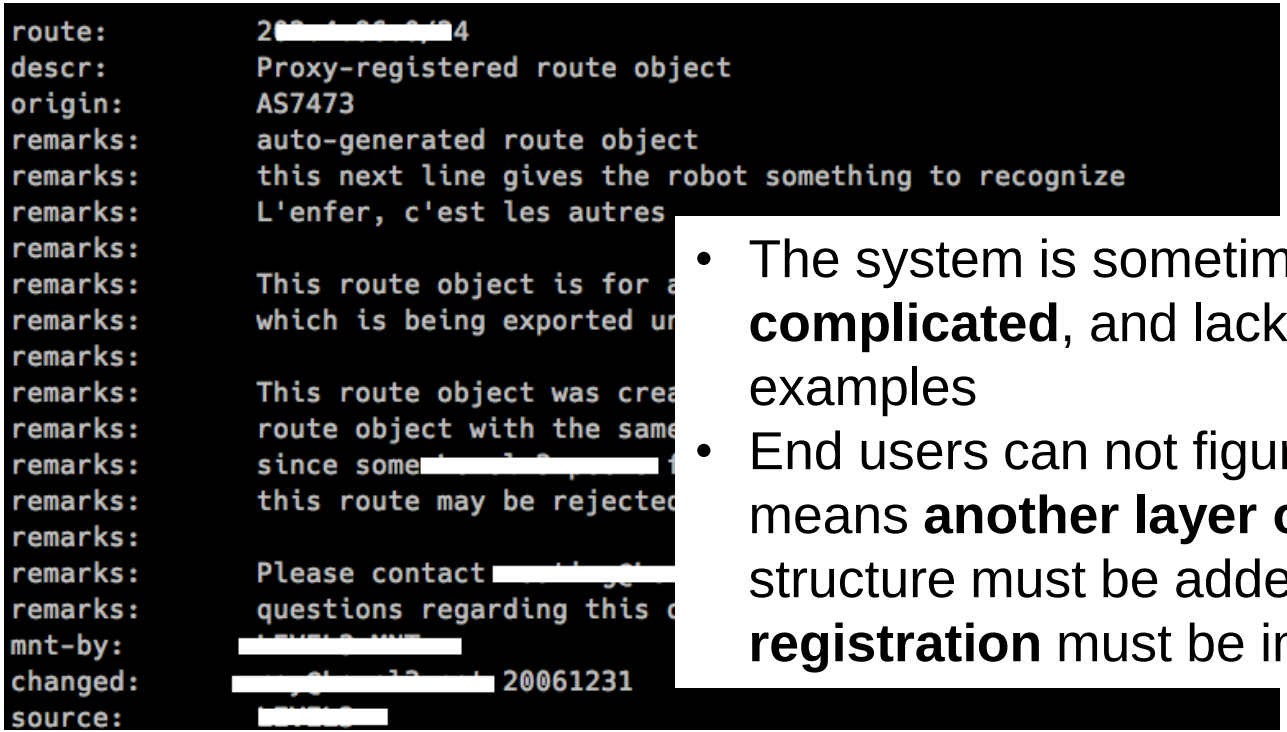
some **spammers** are currently using **short-lived bogus BGP announcements** to send spam from hijacked parts of the IPv4 address space. Such a spammer would use BGP to **announce some address space**, then **send spam** from those addresses, and then **withdraw the announcement**.

Current Practice

Tools & Techniques



LoA Check



- The system is sometimes overly **complicated**, and lacks sufficient examples
- End users can not figure it out, which means **another layer of support** structure must be added, or **proxy registration** must be implemented

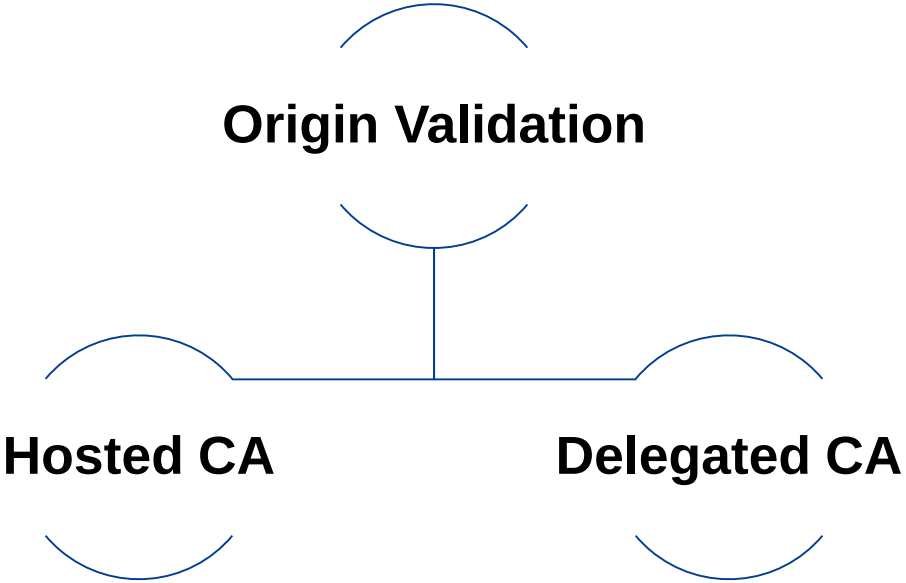
LoA Check & RPSL

```
~ whois -h whois.radb.net AS1299 | more
aut-num:        AS1299
org:            ORG-TA45-RIPE
as-name:        TELIANET
import:         from AS57 action pref=50; accept AS-NLG-TO-TRANSIT
import:         from AS62 action pref=50; accept AS-c1
import:         from AS109 action pref=50; accept AS109
import:         from AS174 action pref=100; accept AS-PSINET
import:         from AS209 action pref=100; accept AS209
import:         from AS286 action pref=100; accept AS-KPN
import:         from AS293 action pref=100; accept AS-ESNET
import:         from AS577 action pref=50; accept AS577:AS-CUSTOMERS
import:         from AS612 action pref=50; accept AS612
import:         from AS701 action pref=100; accept AS701 AS701:AS-CUS
import:         from AS702 action pref=100; accept AS702:RS-EURO AS70
import:         from AS714 action pref=50; accept AS714
import:         from AS786 action pref=50; accept AS-JANETUS
import:         from AS812 action pref=50; accept AS-ROGERS:AS-CUSTOM
import:         from AS852 action pref=50; accept AS-TELUS
import:         from AS855 action pref=50; accept AS855:AS-CUSTOMERS
import:         from AS1239 action pref=100; accept AS1239 AS1239:AS-
import:         from AS1248 action pref=50; accept AS-NOK
import:         from AS1257 action pref=100; accept AS-TELE2
import:         from AS1267 action pref=50; accept AS1267 AS-INFOSTRA
import:         from AS1273 action pref=50; accept AS-CW
import:         from AS1280 action pref=50; accept AS1280:AS-SET
```

A publicly accessible description of every import and export policy to **every transit, peer, and customer**, is difficult to maintain, and is not in the **best business interests** of many ISPs

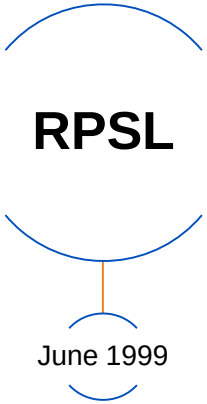
```
~ whois -h whois.radb.net AS1299 | wc -l
4924
~ _
```

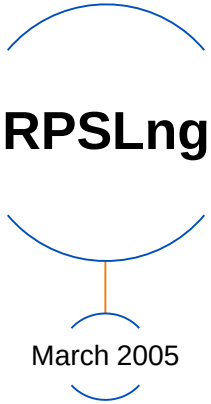
RPKI Implementation

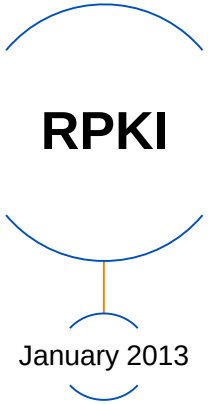


*upgrade at least ASBRs to RPKI capable code

Technology & Learning Curve

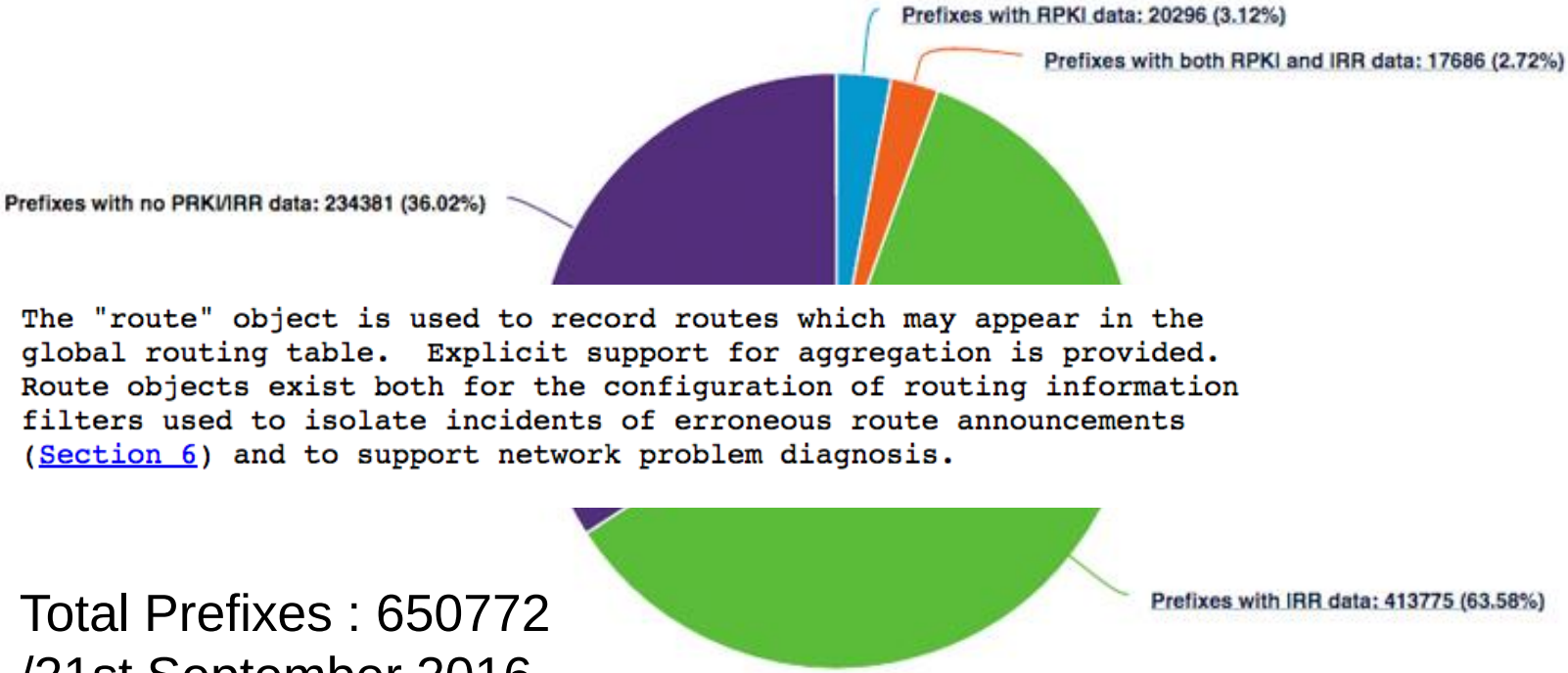






But how are operators adopting and implementing?

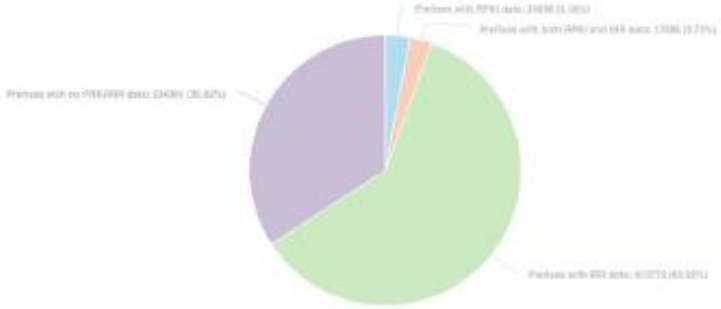
Prefixes Distribution

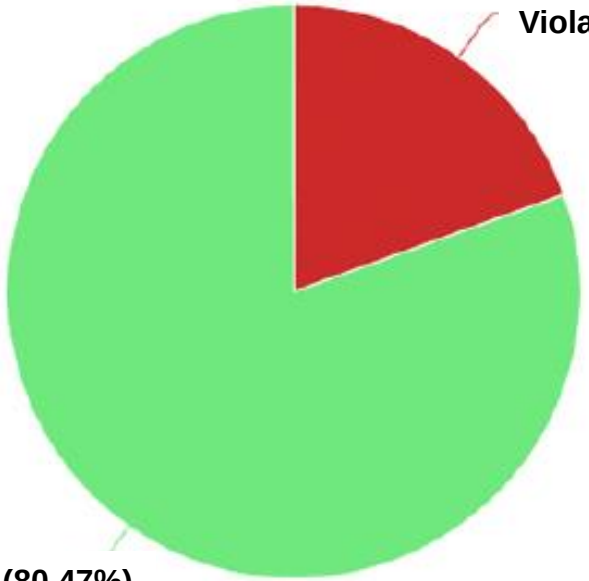


The "route" object is used to record routes which may appear in the global routing table. Explicit support for aggregation is provided. Route objects exist both for the configuration of routing information filters used to isolate incidents of erroneous route announcements (Section 6) and to support network problem diagnosis.

Total Prefixes : 650772
/21st September 2016

Prefixes With IRR Data





Violations: 80794 (19.53%)

Consistent: 332981 (80.47%)

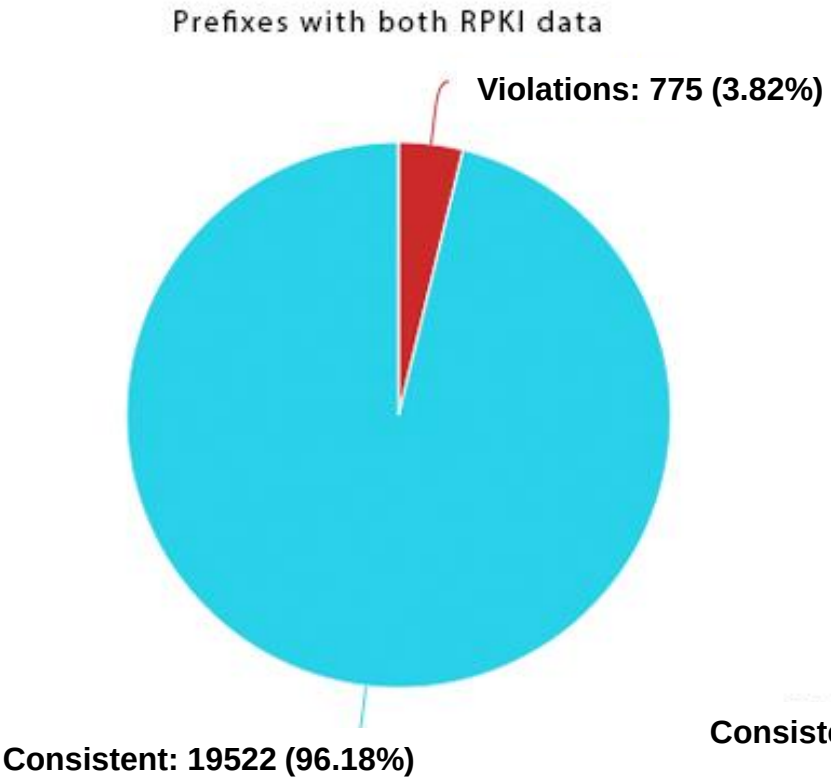
IRR Data Violations Example

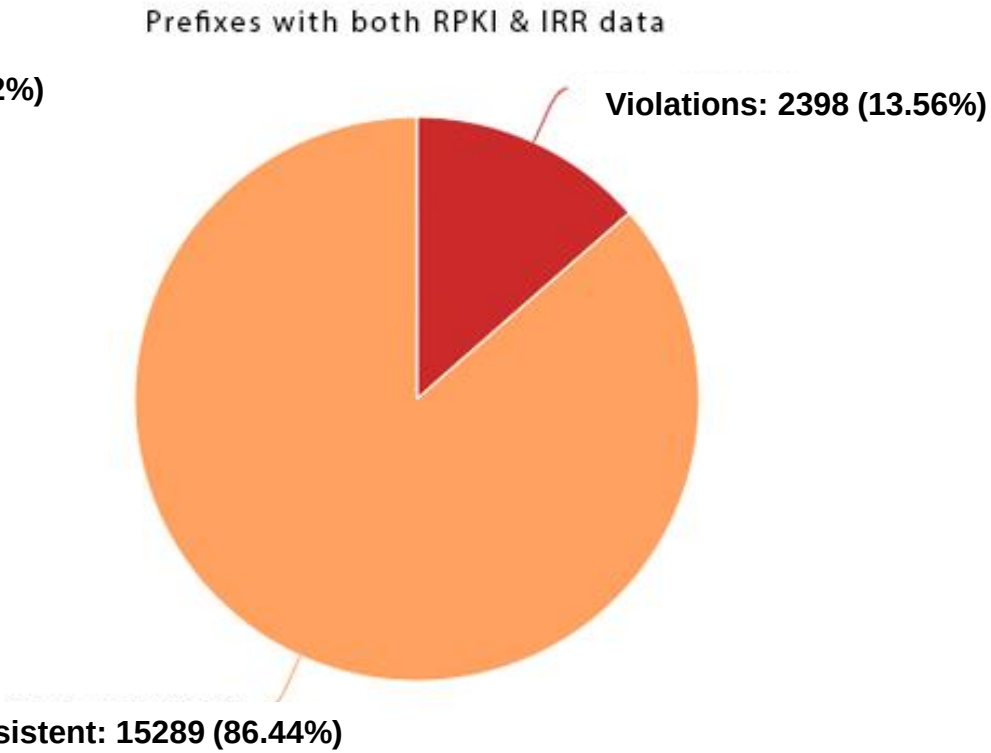
Prefix/Len	Recv Origin AS	IRR Origin AS
203.27.30.0/24	4294836336	2147483647
103.62.28.0/24	4294836383	2147483647
103.62.29.0/24	4294836383	2147483647

```
~ Desktop whois -h whois.radb.net 203.27.30.0/24
route:      203.27.30.0/24
descr:      Proxy route object registered by AS2764
origin:     AS4294836336
remarks:    This route object was created by AAPT on behalf of a customer.
remarks:    As some of AAPTs upstream networks filter based on IRR objects,
remarks:    this route object has bee
remarks:    of this prefix is not rej
notify:     routing.shared@aapt.com.a
mnt-by:     MAINT-AS2764
changed:    nobody@aapt.com.au 201606
source:     RADB
```

```
g.net>show ip bgp 103.62.29.0/24
BGP routing table entry for 103.62.29.0/24, version 198378
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     2
  Refresh Epoch 2
  4826 4294836383
    49.255.232.169 from 49.255.232.169 (114.31.194.12)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 316282439 316282836 316333767
      rx pathid: 0, tx pathid: 0x0
```

Prefixes With RPKI





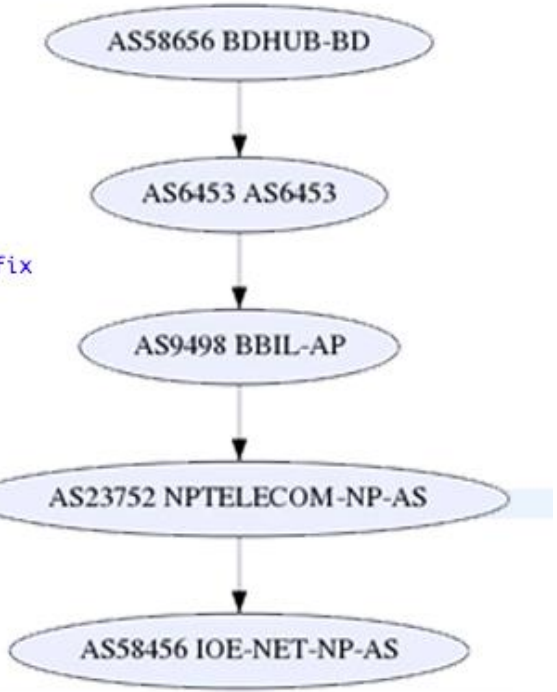
RPKI Data Violation Example

- Most of the cases involve an invalid prefix (fixed length mismatch)
  - Create ROA for /22 but announce 24
- Invalid origin AS is also visible

```
~ whois -h whois.bgpmon.net " --roa 14080 213.192.242.0/23"
2 - Not Valid: Invalid Origin ASN, expected 8903
```

RPKI Data Violation Example


```
{
  "validated_route": {
    "route": {
      "origin_asn": "AS58456",
      "prefix": "202.70.91.0/24"
    },
    "validity": {
      "state": "Invalid",
      "reason": "as",
      "description": "At least one VRP Covers the Route Prefix
      "VRPs": {
        "matched": [],
        "unmatched_as": [
          {
            "asn": "AS23752",
            "prefix": "202.70.64.0/19",
            "max_length": 19
          }
        ],
        "unmatched_length": []
      }
    }
  }
}
```

How About South Asia?

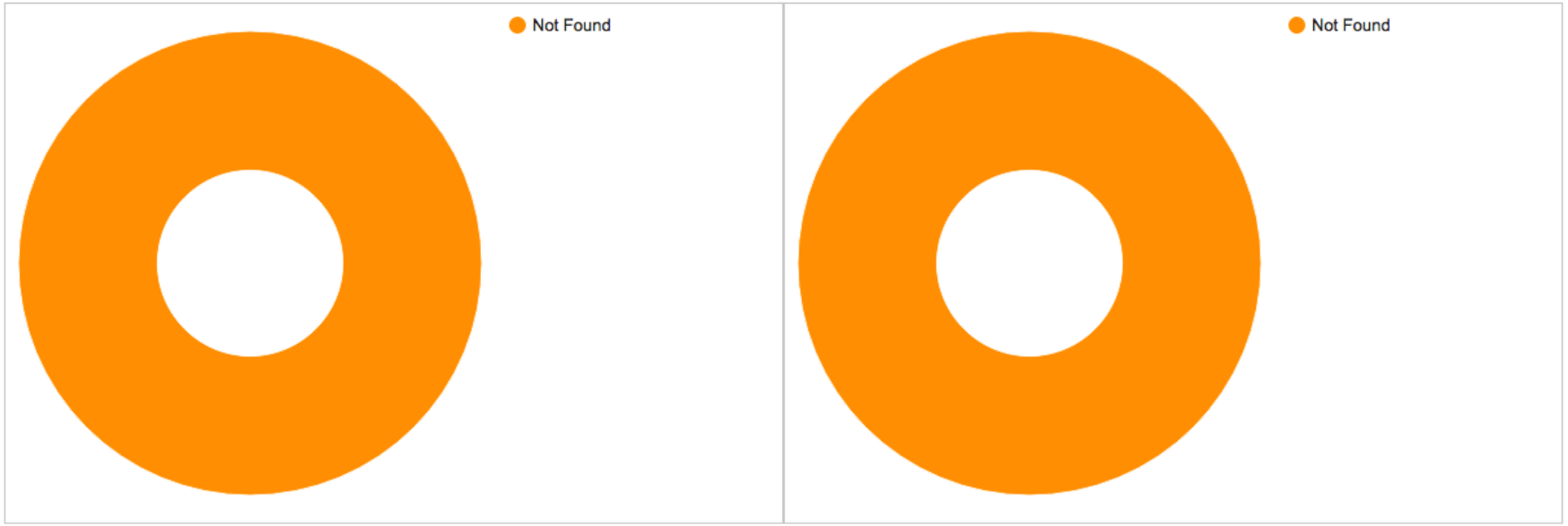
ROAs in South Asia

Country	IPv4 prefixes covered	IPv4 prefixes valid
Afghanistan	0%	0%
Bangladesh	24.24%	23.26%
Bhutan	86.67%	86.67%
India	0.39%	0.39%
Maldives	0%	0%
Nepal	55.93%	21.19%
Pakistan	11.55%	11.5%
Sri Lanka	50.18%	40.99%

source : https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html
date : 21st September 2016

Afghanistan

Total ASNs delegated by RIR: 46, Visible IPv4 routes: 270, Visible IPv6 routes: 3

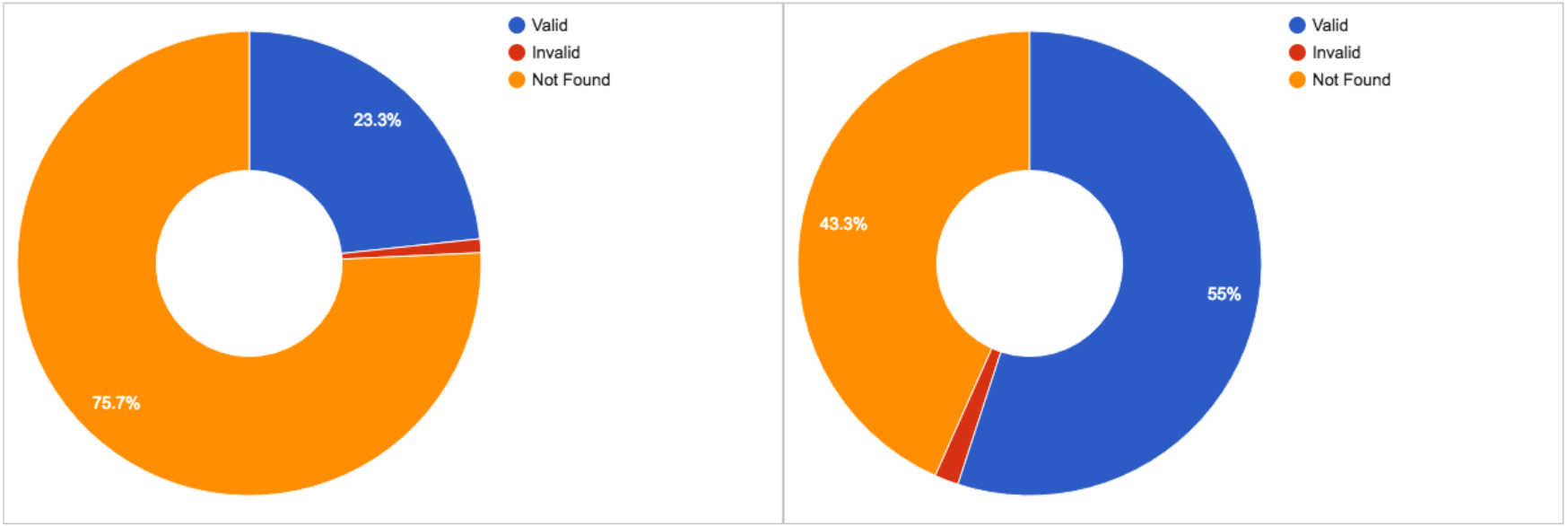


This graph generated on Wed 21 Sep 2016 12:36:52 AEST

http://rpki.apnictraining.net/output/af.html

Bangladesh

Total ASNs delegated by RIR: 402, Visible IPv4 routes: 3449, Visible IPv6 routes: 60

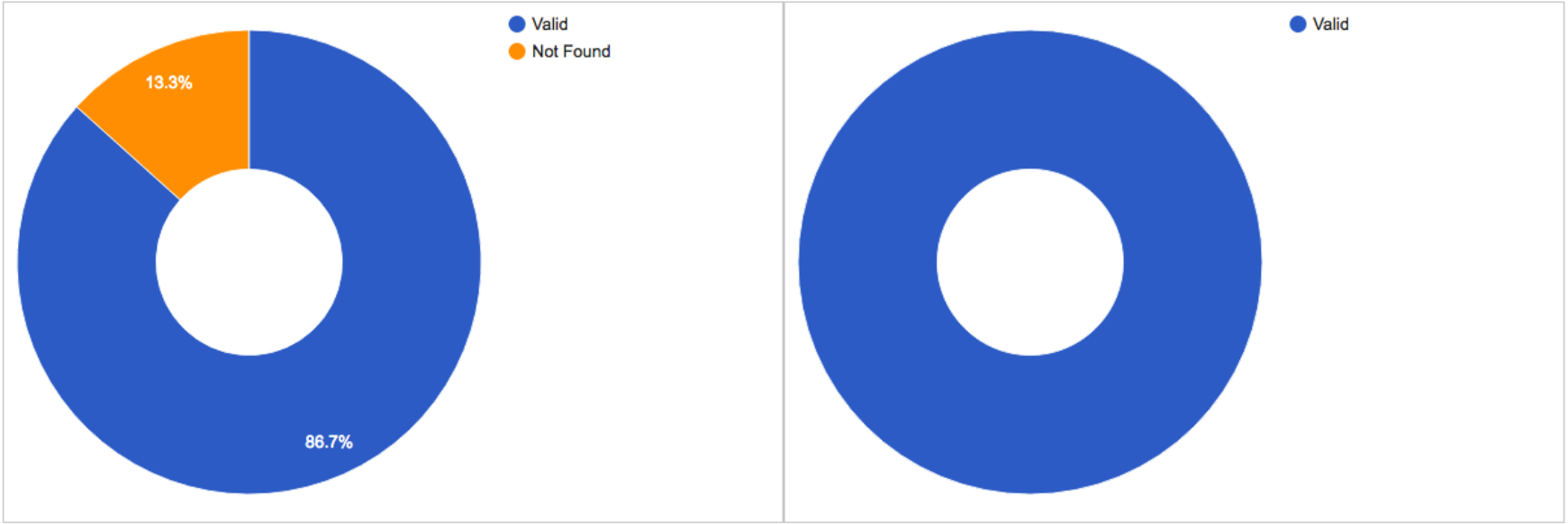


This graph generated on Wed 21 Sep 2016 12:10:48 AEST

http://rpki.apnictraining.net/output/bd.html

Bhutan

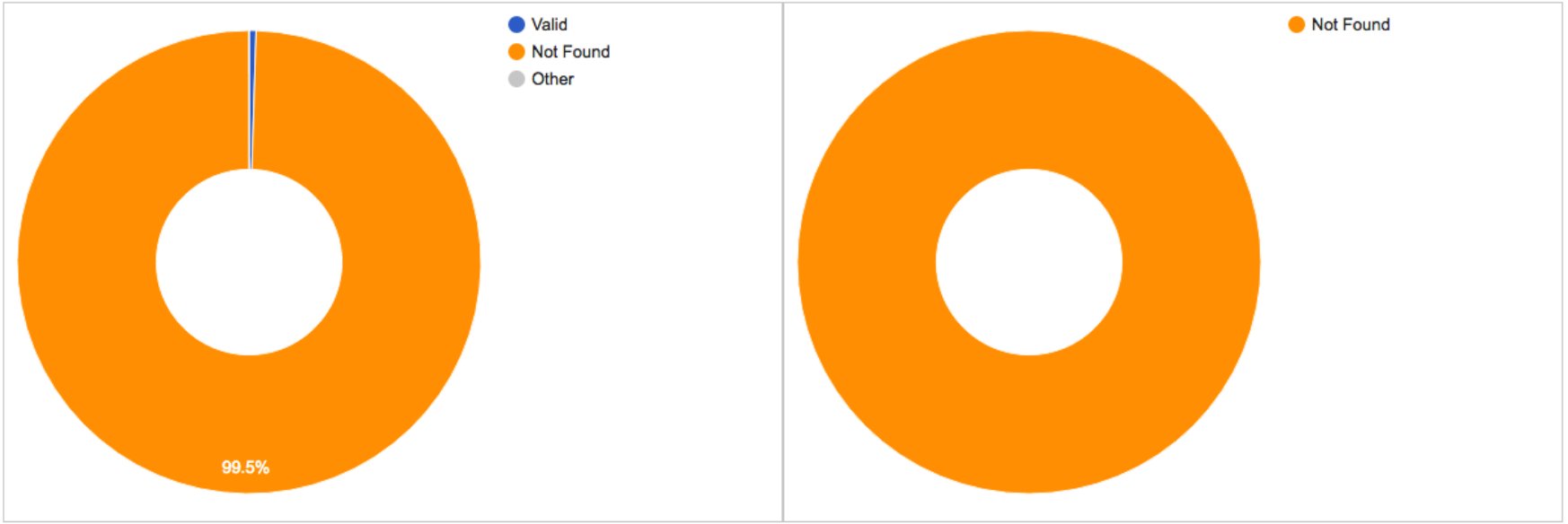
Total ASNs delegated by RIR: 6, Visible IPv4 routes: 15, Visible IPv6 routes: 3



http://rpki.apnictraining.net/output/bt.html

India

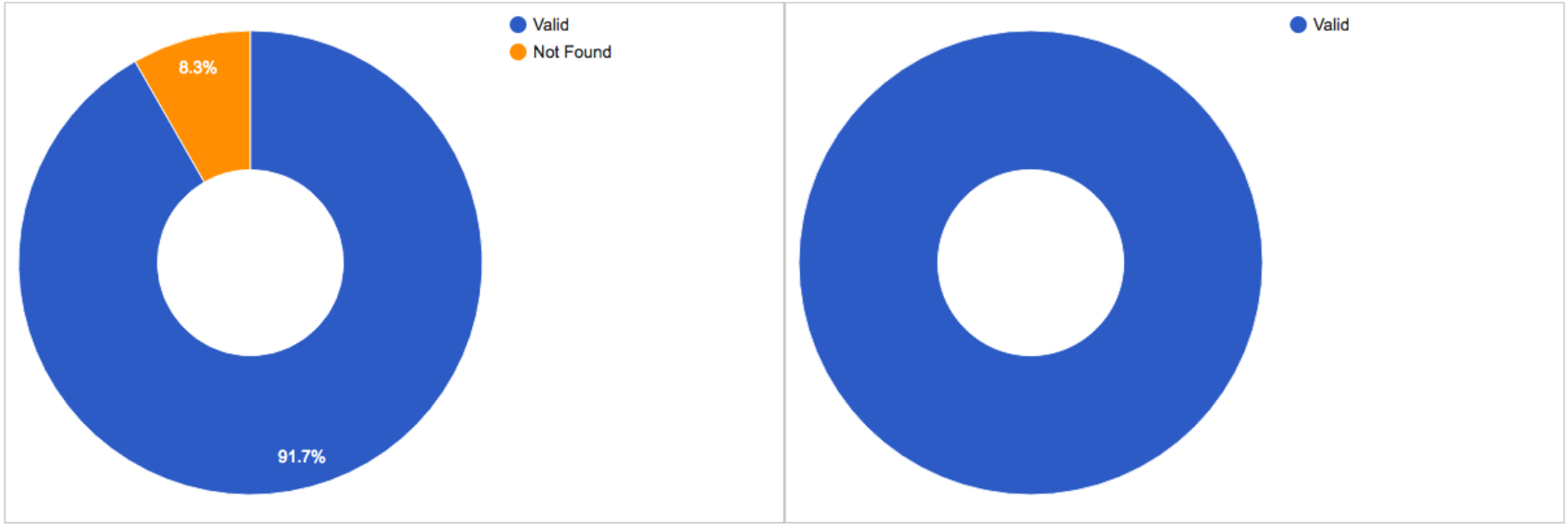
Total ASNs delegated by RIR: 722, Visible IPv4 routes: 29944, Visible IPv6 routes: 1045



http://rpki.apnictraining.net/output/in.html

Maldives

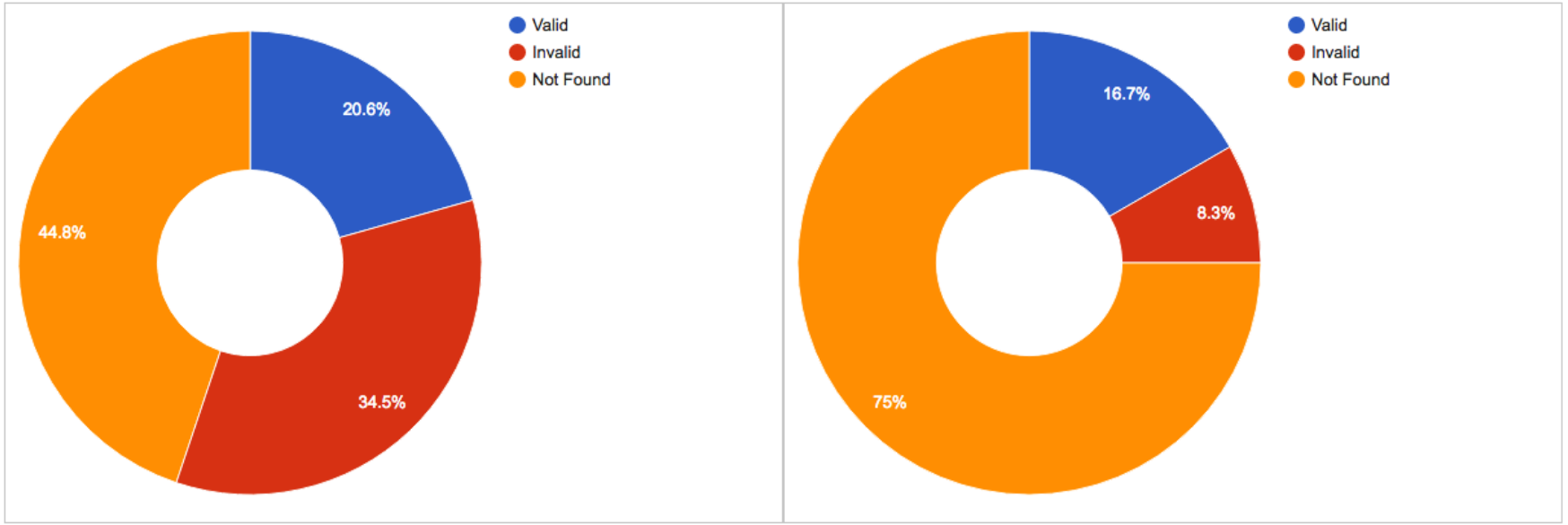
Total ASNs delegated by RIR: 7, Visible IPv4 routes: 217, Visible IPv6 routes: 11



http://rpki.apnictraining.net/output/mv.html

Nepal

Total ASNs delegated by RIR: 60, Visible IPv4 routes: 475, Visible IPv6 routes: 12

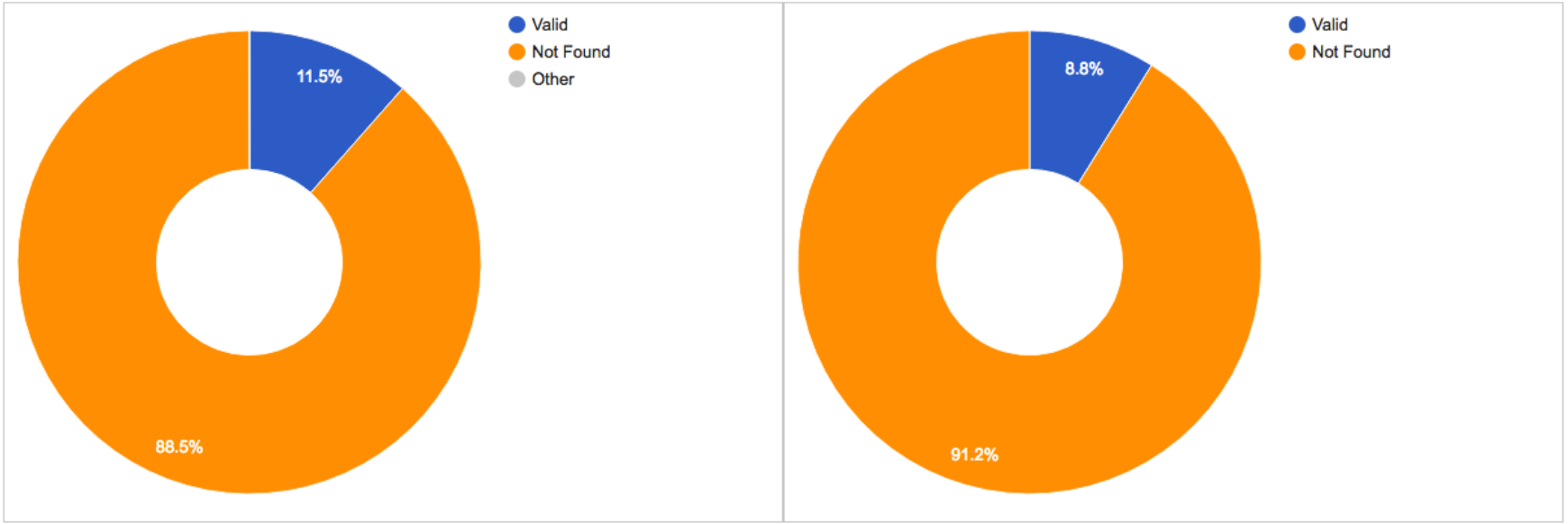


This graph generated on Wed 21 Sep 2016 13:02:36 AEST

http://rpki.apnictraining.net/output/np.html

Pakistan

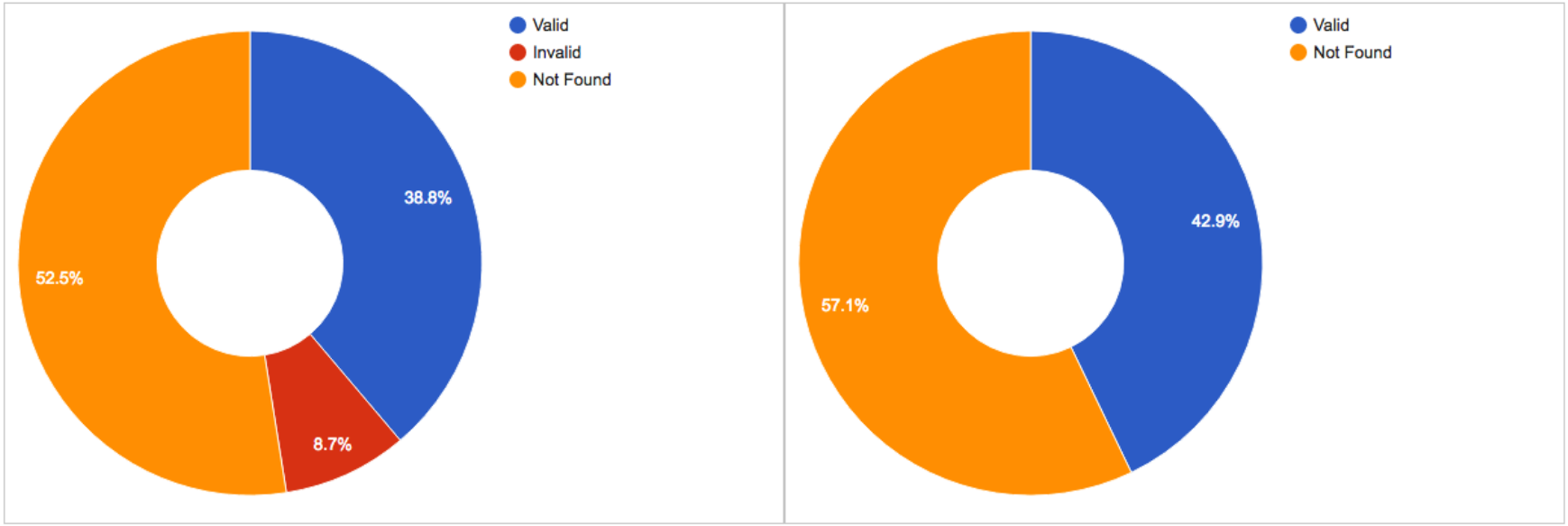
Total ASNs delegated by RIR: 123, Visible IPv4 routes: 3924, Visible IPv6 routes: 34



http://rpki.apnictraining.net/output/pk.html

Sri Lanka

Total ASNs delegated by RIR: 22, Visible IPv4 routes: 299, Visible IPv6 routes: 14



This graph generated on Wed 21 Sep 2016 14:06:58 AEST

http://rpki.apnictraining.net/output/lk.html

Summary

- RPKI adoption is growing
  - In most cases, operators create ROAs for min length and advertise longest prefix
  - Some ROAs are invalid due to further allocation to customers
- BGP operations and security
  - draft-ietf-opsec-bgp-security-07

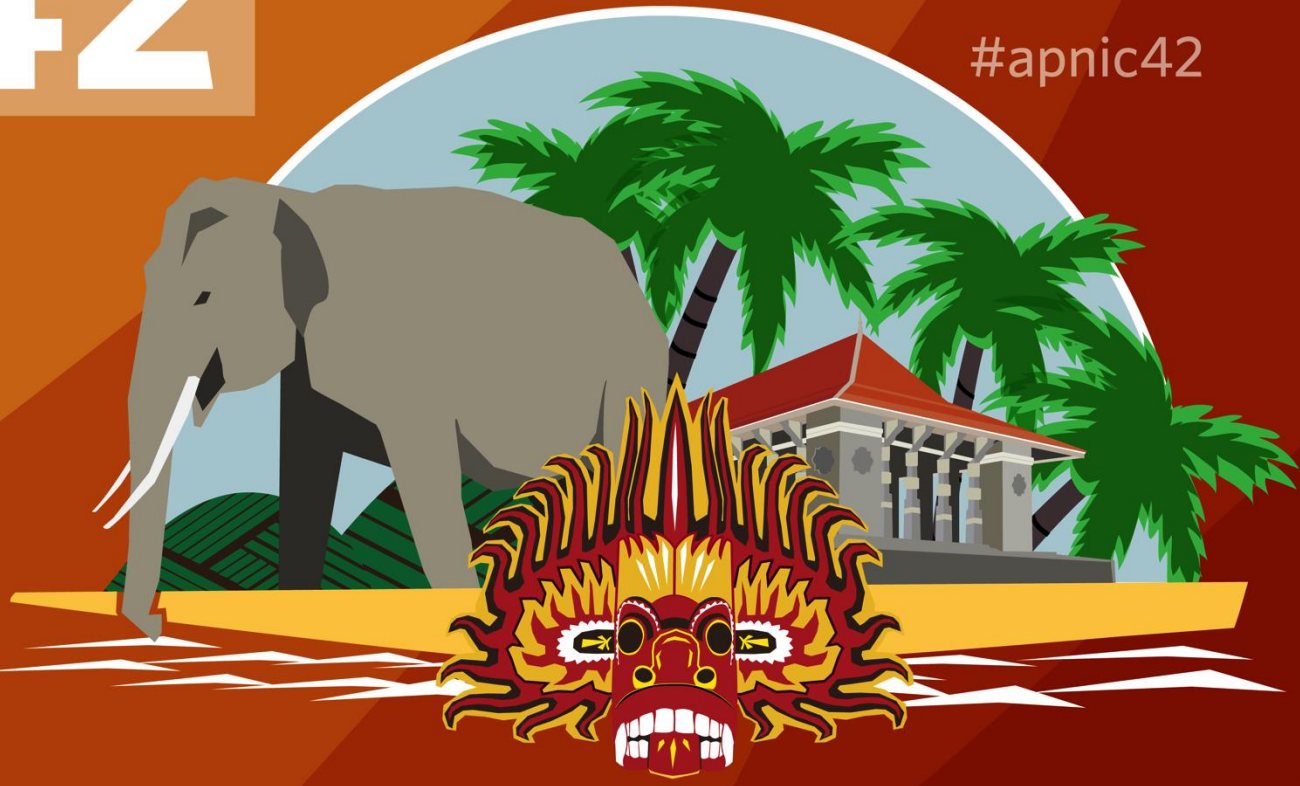
Data Collection

- OpenBMP
  - https://github.com/OpenBMP/openbmp
- RPKI Dashboard
  - https://github.com/remydb/RPKI-Dashboard
- RIPE RPKI Statistics
  - https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html
- RIPE Cache Validator API
  - http://rpki-validator.apnictraining.net:8080/export

https://www.apnic.net/rpki

APNIC 42

#apnic42



COLOMBO, SRI LANKA

28 September – 5 October 2016