Wild ROArs

Carlos Martinez, IEPG @IETF100

What ?

- Taking a look into how country code information for both prefix and declared origin AS actually looks
- Country Code in this case is *country code of registration* according to the RIRs published registry information
  - Bear in mind that this is not strictly “geolocation”

Why ?

- Original intention was to look into possible “interesting” cases where country codes for both prefix and declared origin_AS differ in ROA data
- For the purpose of this talk, a ROA is a structure like this:
  - Array[N] of “Prefix” – “MaxLen”
  - Int Origin_AS
- We will only be looking at:
  - ROAs from LACNIC’s repository
  - IPv4 prefixes

Datasets description

- Our source datasets:
  - RIR registry snapshots: the well-known “delegated-<<RIR>>-extended”
    - Found at http://<<RIR>>/pub/stats
    - We call this dataset **“numres.csv”**
  - ROA data
    - Source is the “export” feature of RIPE’s RPKI relying-party tool
    - We call this dataset **“roadata.csv”**
  - RIS Data, specifically a file produced daily that includes prefixes and origin Ass
    - Found in the awesome RIS project
    - We call this dataset “**riswhois.csv**”

Derivative (working) Dataset

- We add two fields to our “roadata.csv”
  - Registration Country Code of each prefix **(pfx_cc)**
  - Registration Country Code of each Origin_AS **(origin_as_cc)**

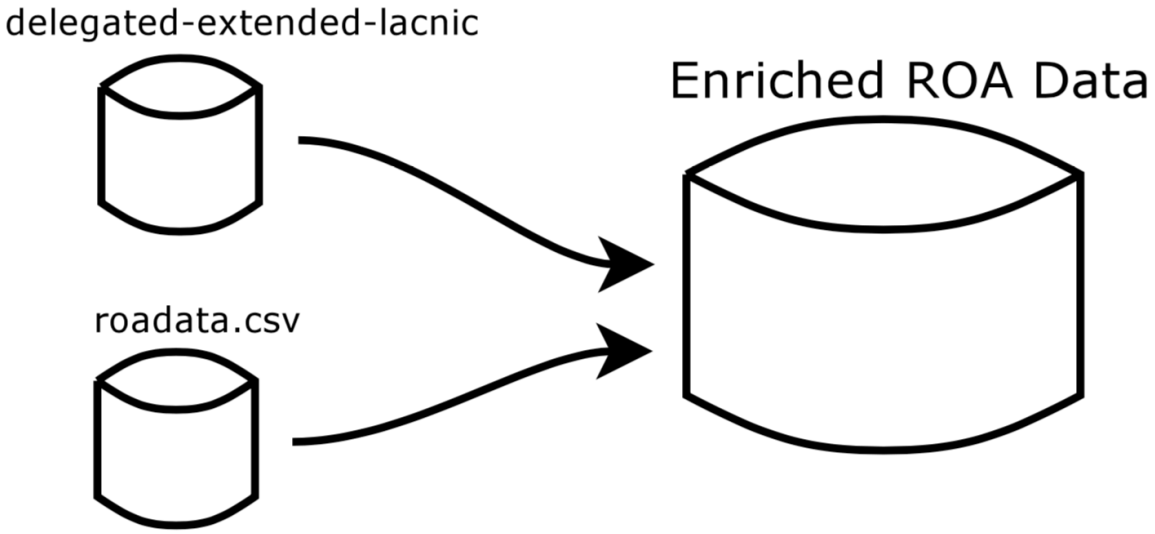
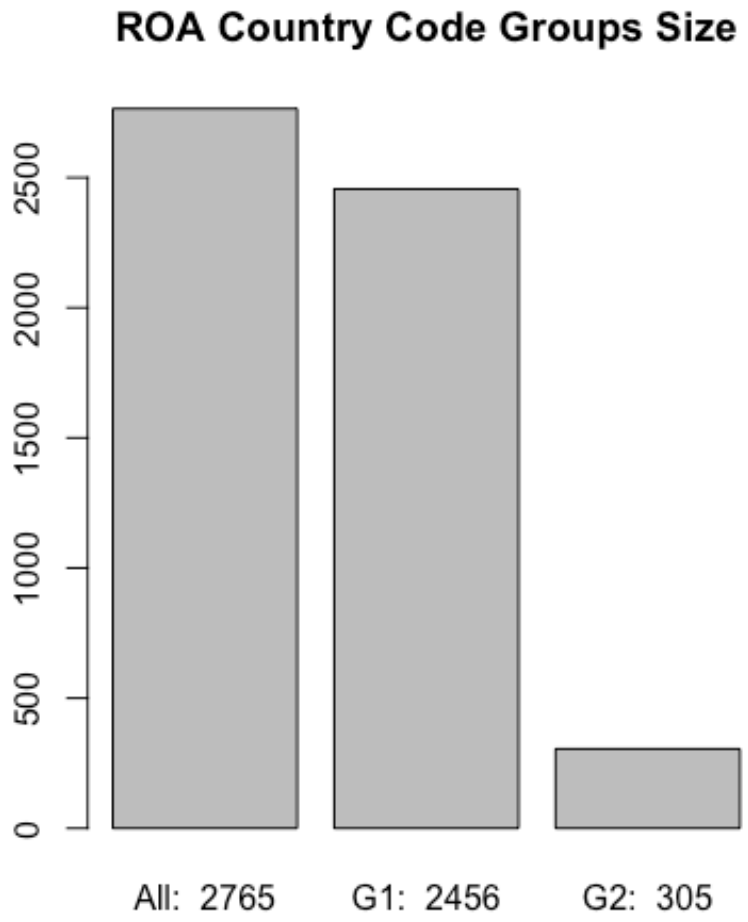


Fig. 1

ROA Country Code Groupings

- Group #0
  - All LACNIC's ROAs
- Group #1
  - Defined by the condition "pfx_cc == origin_as_cc"
- Group #2
  - Defined by the condition "pfx_cc != origin_as_cc"



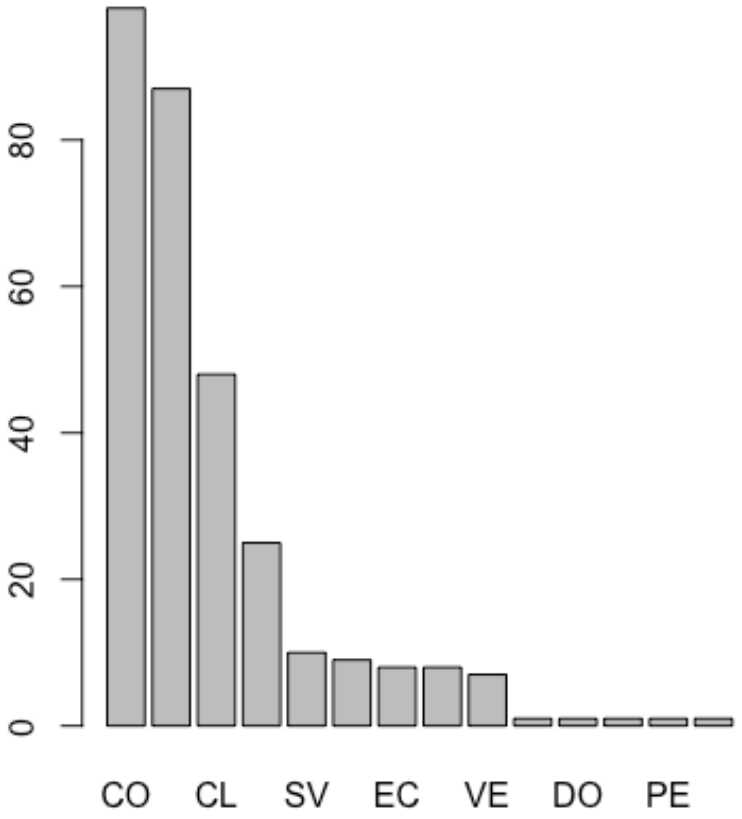
Drilling Down into Group #2

- 24 different country codes appear as “origin_as_cc”
  - *Remember: this is just for those ROAs where the prefix is registered to a different country code*
- Most of the *“green”* cases have clear explanations
  - Big carriers with single AS presence in multiple regions
- The “*red*” cases are really weird

1	137	US
2	44	EC
3	33	GT
4	17	BR
5	8	CL
6	8	PA
7	7	BG
8	7	CO
9	7	GB
10	6	ES
11	6	PE
12	5	AR
13	4	ZA
14	3	VE
15	2	MX
16	2	NL
17	2	UA
18	1	DE
19	1	HK
20	1	IL
21	1	IN
22	1	IT
23	1	SG
24	1	UY

Drilling Down into Group #2 (ii)

- Which prefix holding countries create ”foreign ROAs” the most ?



1	98	CO
2	87	AR
3	48	CL
4	25	CR
5	10	SV
6	9	PA
7	8	EC

Drilling Down into CL

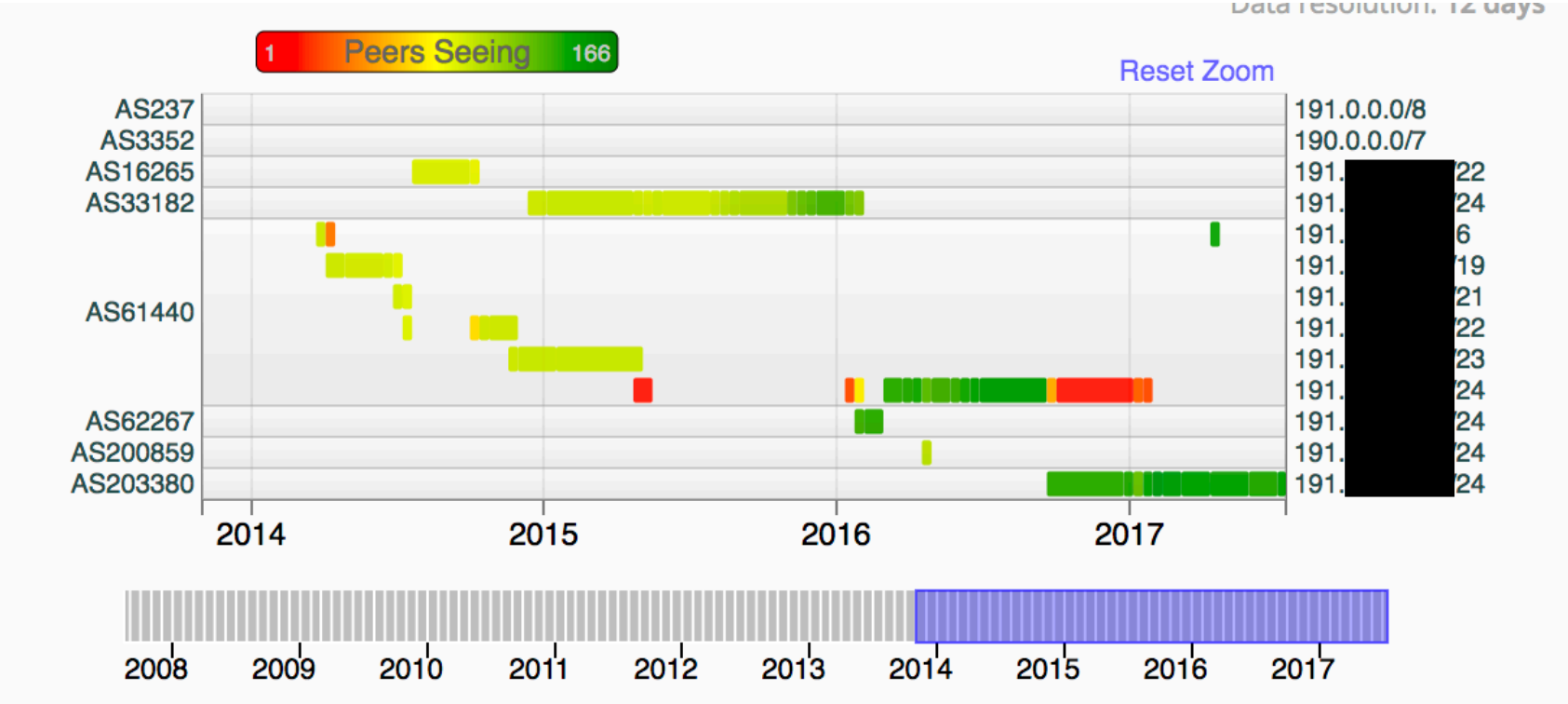
- Why CL?
  - Most of the “red” cases come from CL
  - The cases for CO and AR are mostly explained by large telcos operating in neighboring countries

1	22	AS396076	US
2	6	AS60458	ES
3	4	AS37692	ZA
4	3	AS33182	US
5	2	AS61317	GB
6	1	AS12586	DE
7	1	AS203380	GB
8	1	AS206776	BG
9	1	AS27	US
10	1	AS29073	NL
11	1	AS31708	GB
12	1	AS38001	SG
13	1	AS50673	NL
14	1	AS55526	IN
15	1	AS61102	IL
16	1	AS62240	GB

The curious case of 191.XXX.YY.0/24

- This is one of the ”red” cases
- Originally part of a large allocation made to an organization in CL
- Progressively de-aggregated into smaller and smaller chunks
- Some of these chunks are announce all over the world, including some for which ROAs have been created

The curious case of 191.XXX.YY.0/24



Progressive deaggregation

Final Comment

- I have redacted the actual prefixes and org names because over the past two weeks blocks from these “strange” cases have been involved in security incidents
- We are investigating them and collaborating with other organizations

Thanks!