Internet ASN squatting

What it's? How bad?,
How good?, What can we do?

What is ASN squatting

Autonomous System Numbers that have not been assigned either by a RIR or IANA but appear in the global routing table

History

We started looking for prefixes marked as “available” in the NRO file and we realized that ASN squatting is perfectly feasible. We were curious in knowing if it was happening.

How we did this study

- Linux Ubuntu 13.04
- Most scripts in python3
- Daily routing table is copied from: :
http://data.ris.ripe.net/rrc16/latest-bview.gz
- Daily NRO file is copied from:
http://www.nro.net/pub/stats/nro/delegated-extended
- Backend DB is Mysql
- Basicly two scripts:
    * One which takes the DB & the NRO to MySQL
    * A second script which looks for every prefix and ASN in the Routing tables and tries to find a match in the NRO info.

Difficulties

- The speed of processing
- ASNs allocations by RIRs to LIRs sometimes are done by blocks and not one by one (quantity > 1)

Example:
January 28. What we found:

AS222444 advertising 192.54.88.0 / 24
AS12845938 advertising 193.104.235.0 / 24
AS12845948 advertising 109.233.96.0 / 21
AS12845948 advertising 195.250.24.0 / 22

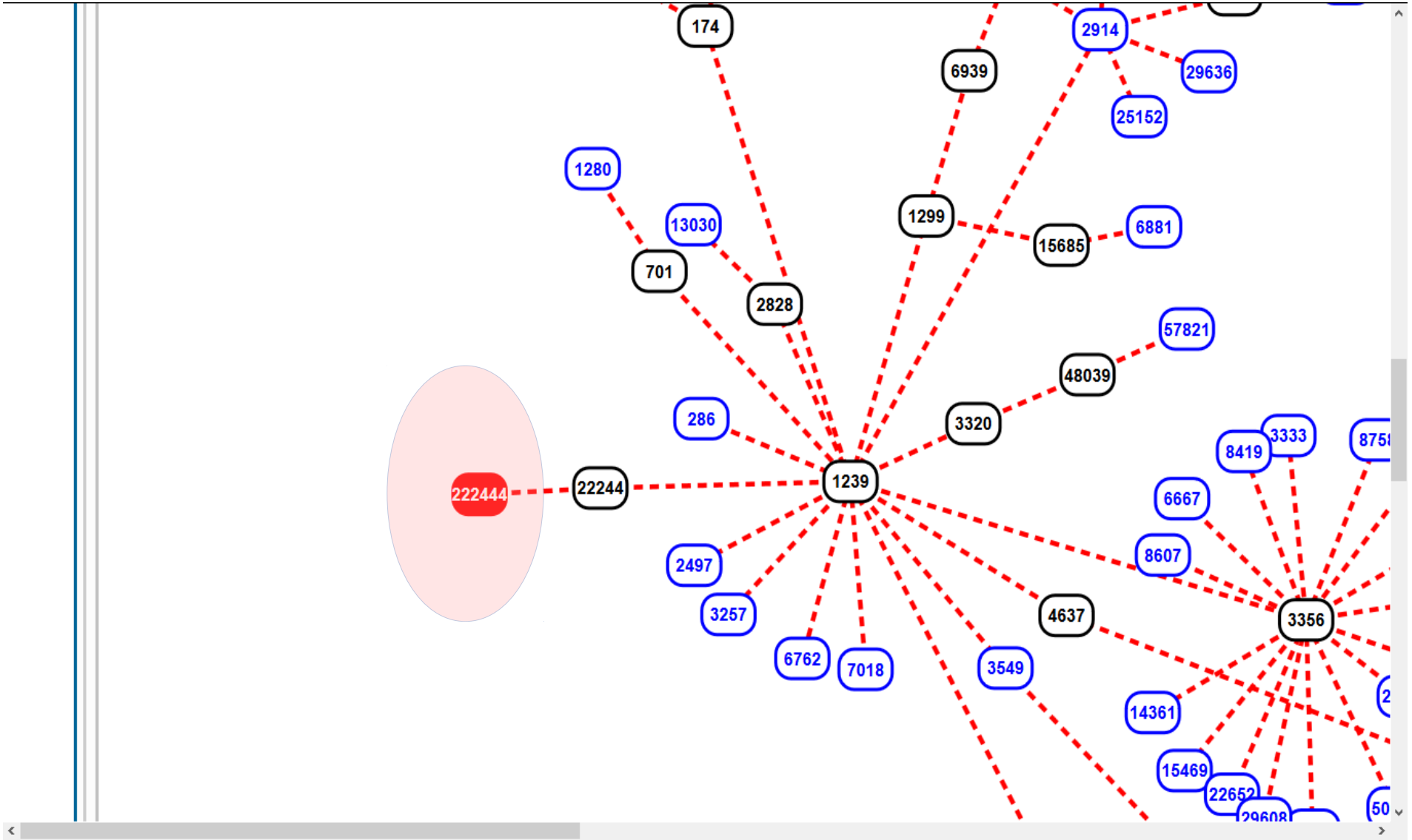
Was it true?:

- We double checked the information using several looking glasses in Internet such as Hurricane Electric and TATA
- We also checked it using RIPE's BGP Play

IANA AS list as of: 28/Jan/2014

	RIPE NCC			
199680-200191	Assigned by RIPE NCC	whois.ripe.net		2013-09-(
200192-262143	Unallocated			
262144-263167	Assigned by LACNIC	whois.lacnic.net		2006-11-2
263168-263679	Assigned by LACNIC	whois.lacnic.net		2013-06-1
263680-327679	Unallocated			
327680-328703	Assigned by AFRINIC	whois.afrinic.net		2006-11-2
328704-393215	Unallocated			
393216-394239	Assigned by ARIN	whois.arin.net		2006-11-3
394240-4199999999	Unallocated			
4200000000-4294967294	Reserved for Private Use		[RFC6996]	
4294967295	Reserved			

RIPE's BGPPLAY (28/Jan/2014)



TATA's LG (28/Jan/2014)

TATA COMMUNICATIONS
TAKING YOU FARTHER

AS6453 IPv4 and IPv6 Looking Glass

show ip bgp 193.104.235.0

Router: gin-n71-core1
Site: AE, Fujairah, N71
Command: show ip bgp 193.104.235.0

```
BGP routing table entry for 193.104.235.0/24
Bestpath Modifiers: deterministic-med
Paths: (2 available, best #1)
  Not advertised to any peer
  174 12741 12845938
    ldn-tcore1. (metric 7925) from jsd-core1. ( jsd-core1. )
      Origin IGP, valid, internal, best
      Community:
      Originator: 66.110.10.38
  174 12741 12845938
    ldn-tcore1. (metric 7925) from klt-tcore1. (66.110.11.12)
      Origin IGP, valid, internal
      Community:
      Originator: 66.110.10.38
```

HE's LG (28/Jan/2014)

Show options

```
core1.fmt1.he.net> show ip bgp routes detail 109.233.96.0
  Number of BGP Routes matching display condition : 1
       S:SUPPRESSED F:FILTERED s:STALE
1       Prefix: 109.233.96.0/21,  Status: BI,  Age: 1d14h10m4
         NEXT_HOP: 217.29.66.11, Metric: 1689, Learned from P
          LOCAL_PREF: 100,  MED: 20,  ORIGIN: igp,  Weight: 0
         AS_PATH: 3302 12845948 12845948
       Last update to IP routing table: 1d14h10m42s, 1 path(s
# Entry cached for another 60 seconds.
```

Is it good?

We don't think so:
Please read the next slide

Is it bad?

Yes, it's:
- In case of threat difficult to track
- No info in the whois DB
- You got to go the upstream provider, you will loss time, maybe won't get an answer

Can it be worse?

As usual, yes it can:
- Imagine a squatted prefix & a squatted ASN!!.., difficult to handle
- We can get a cascade effect, squatte ASN doing transit for another squatted AS
- Is this a potential problem?, more of this in the future?

Why is it happening?

As a comment:
- For AS222444 the upstream AS is: 22244 (regarding whois: Morotola-PHX). The prefix they are announcing belongs to Motorola

Typo error?

RPKI?

- Could be half of the solution since RPKI only validates prefixes.
- RPKI does not validate the if the AS is valid

March 1st results

222444 advertising 192.54.88.0 / 24
553330 advertising 27.116.57.0 / 24
553330 advertising 103.23.247.0 / 24
553330 advertising 175.106.42.0 / 24
553330 advertising 180.94.71.0 / 24
553330 advertising 180.94.72.0 / 24
553330 advertising 180.94.77.0 / 24
553330 advertising 180.94.83.0 / 24
553330 advertising 180.94.87.0 / 24
553330 advertising 180.94.91.0 / 24
553330 advertising 180.94.93.0 / 24
553330 advertising 180.94.95.0 / 24
553330 advertising 203.215.33.0 / 24
12845938 advertising 193.104.235.0 / 24
12845948 advertising 109.233.96.0 / 21

12845948 advertising 195.250.24.0 / 22

What can we do?

- In the same way ISPs filter bogon prefixes they should filter bogon ASs
- ISP traditionally checks for prefixes assignments but they don't check for AS assignment

Thanks & Question to the audience

- Do we need some mechanism to validate ASN?

(I think we know the answer)

If any question please don't hesitate