Why Are There so Many Bad Routes on the Internet?

Eugene Bogomazov
Qrator Labs

What is Internet?

- Internet is a network of ASNes
- Main protocol in BGP
- So...

No, there were already enough BGP tutorials

What is really important?

- Internet is network of trust
  - But we will validate you
  - And filter you out
  - Based on what we decide as bad routes
  - Because actually we don“t trust you

- But what are these bad routes?

Bad boys

- Defined by the community
- You can look at BCP
- You can look at POV

What to do?

- Find who announce bad routes?
  - And why?
- Find who accepte these routes?
  - Big ones?
  - Or to catch a liar?
- And make them suffer?
  - MANRS?
  -  - RIPE policy in the future?
    - Attacking the wrong ones

Today coverage

- Too specific
  - Because can be easily filtered
  - And should not be globally propagated
- ROA Invalid
  - Because of hype

Love of counting

- Different rankings
- Other people“s money
- IP-addresses

(He also like to count)

- Are we worse then the GOAT?

Any report approach

- Take a BGP raw data
- Find bad routes
- Origin ASN in AS_PATH —> bad announcer
- All ASN in AS_PATH —> bad filters

- We can do that!

Basic assumptions

- Filtration of too specific is already great
  - Especially on TIER-1 level
  - What cannot be say about Invalid ROA
- Number of prefixes has a little meaning
  - So, look at the number of operators
- Problem with /32 (/128)

Blackhole

- Usually not made by operator
- Have low propagation
- But can influence overall statistic
- So, separate case

Exact numbers!

	For /32	Not for /32
ROA Valid	242	120568
ROA Invalid length	1402	18656
ROA Invalid asn	204	5288
Normal length	0	896615
Too specific	26044	43966

- Can start to do realtime update
  - And make charts, build graphics...

Fun Facts

- No «drop Invalid» policy in a wild
- Bad routes have a valid less specific
  - Most of too specific routes
  - Almost all with Invalid ROA length (97+%)
- Pretty big number of creators
  - 350+ operators with invalid length
  - 600+ operators with too specific

Invalid ROA length

- You create a ROA object
- Make a policy with maxLength
- Where restricts everyone
- And start to send bad routes
- While sending a valid alternative

- Several hundreds of such operators...

Route analysis

- Based on routes
- In which prefix and AS_PATH can be modified
  - For hijacks with manipulation
  - Or just for casual TE
  - Where is a border between them?

- Let“s remember something

Monitoring manipulation

- BGP collector
  - Many different routes
- Neighbor check
  - ASN in AS_PATH
- Become a critical point
  - All roads are lead through the attacker

AS49666

- Telecommunication Infrastructure Company in Iran
- The critical point for the region
- Remains the critical also for valid routes too
- Not our case
- However, interesting from stability point of view

- One legs have the same property

PoC

- Take a critical points for ISP invalid routes
- And for valid ones
- Find a difference between them
- If any — marked as suspicious
- Such suspicious for many different ISP?
  - Bingo

Minute of blame

- By Invalid length
  - AS263444, AS266721 and… maybe some Tier-1s
  - -120 conflict operators
- By too specific
  - AS4766, AS131477, AS9002
  - Only they made -150 conflicts gone
  - But there are many-many others

State of problems

- Normal cases vs illegal ones
  - Announces in one direction
  - Leak of static
- Avoiding critical point status
  - Drop neighbor check
  - Two or more places of attack

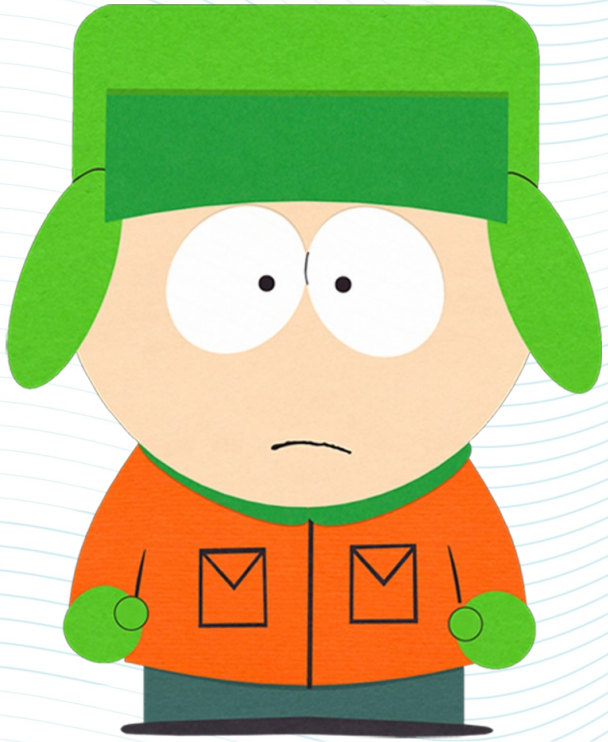
- Other road?

Silver bullet?

- Main questions:
  - Which prefix, ASN pairs are real?
  - Who is actually filtering?
  - Where is a guilty party?

- Full-view table from ISP will cover the first two for him
  - Enough region coverage — cover the last one

Moral (or I learned something)



- Garbage in — garbage out
- Breaking things is easy
  - Much harder to create
- Sometimes numbers are meaningless
- Need of transparency in monitoring

- Most of cases made by transit
  - Not by stubs

Questions?

Contacts: eb@qrator.net