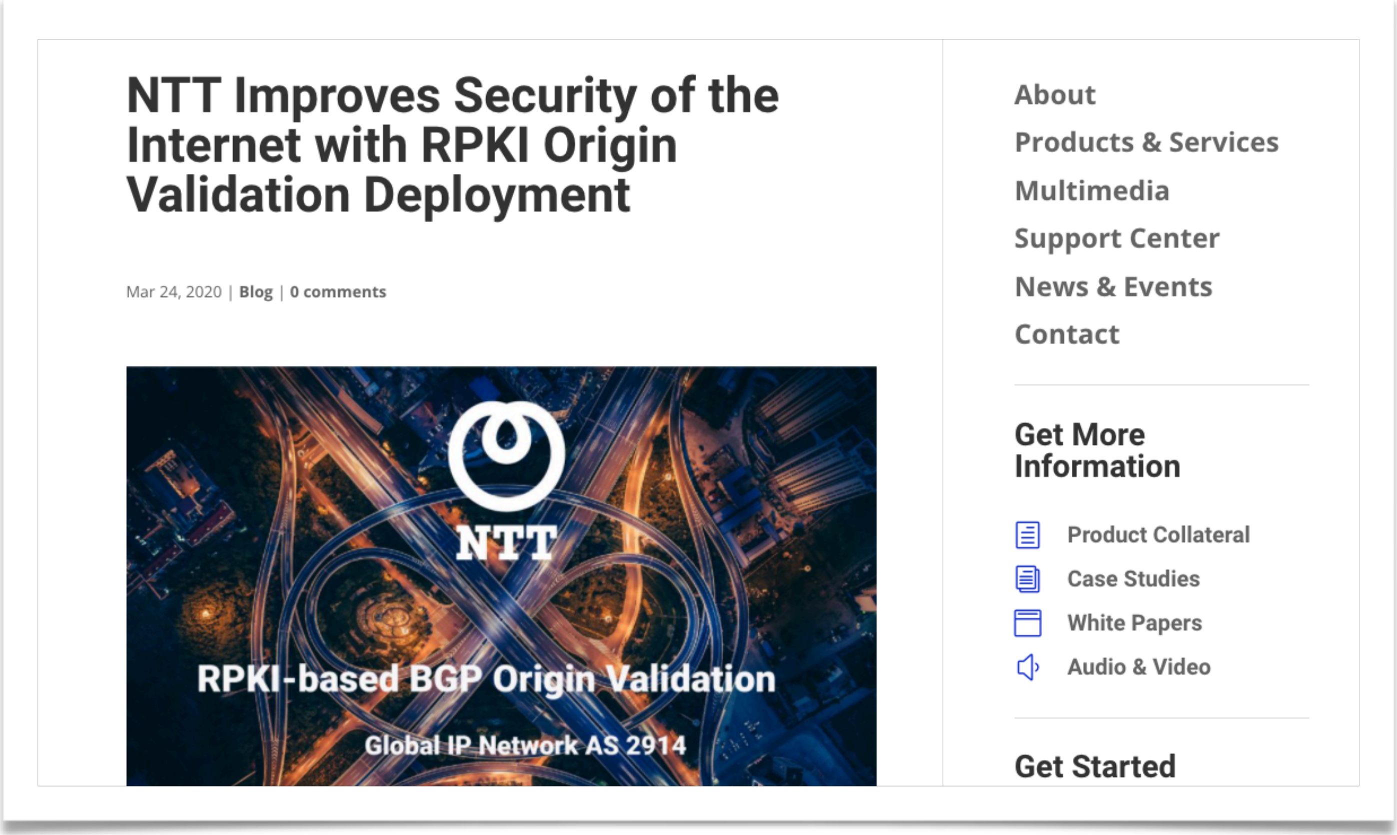
NTT

A one-year review of RPKI operations

Massimo Candela
Senior Software Engineer
Global IP Network
massimo@ntt.net
@webrobotics

NTT’s RPKI Origin Validation announcement



NTT Improves Security of the Internet with RPKI Origin Validation Deployment

Mar 24, 2020 | **Blog** | **0 comments**

However…

- *RPKI requires additional knowledge*

- *RPKI requires additional procedures*

Common mistakes

- You want to announce a prefix, but you forget about RPKI
  - Are you sure it will be “unknown”?

- You do not forget about RPKI, but you forget about timing
  - Publication time
  - Propagation time

A review of 2021

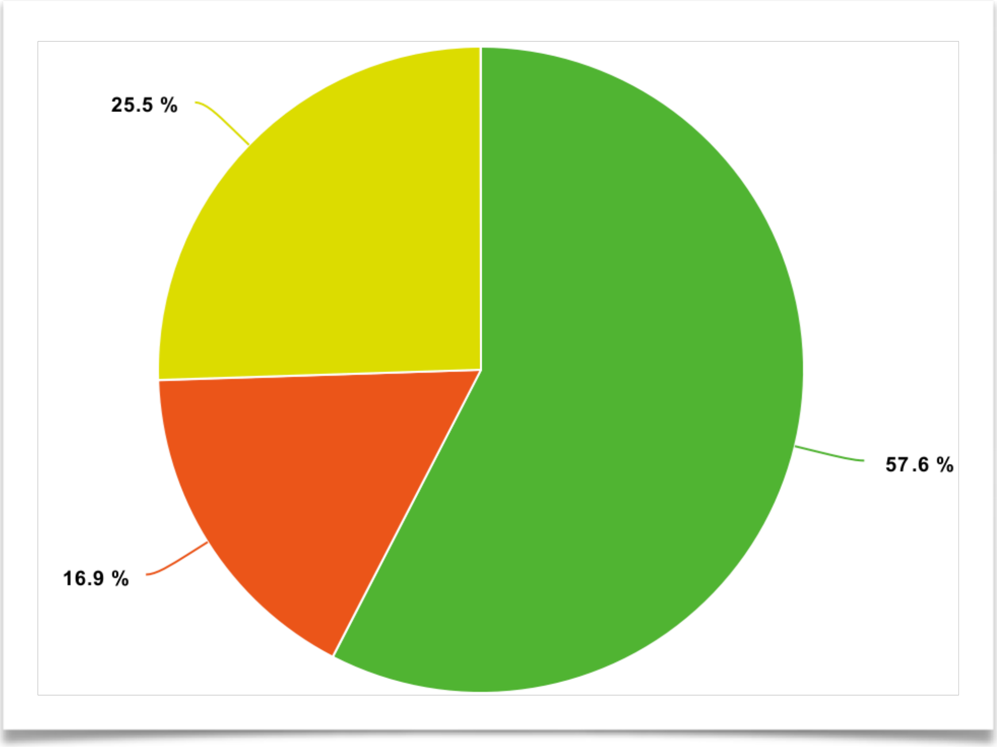
- I reviewed 1 year of RPKI-related alerts generated by our BGPalerter installation
- I divided the alerts in 3 categories:
  1. Wrong maxLength
  2. We announced a customer’s prefix, but they had no ROA for AS2914 (AS mismatch due to customer’s ROA)
  3. We migrated prefixes from one AS to another, but no ROA update (AS mismatch)

A review of 2021

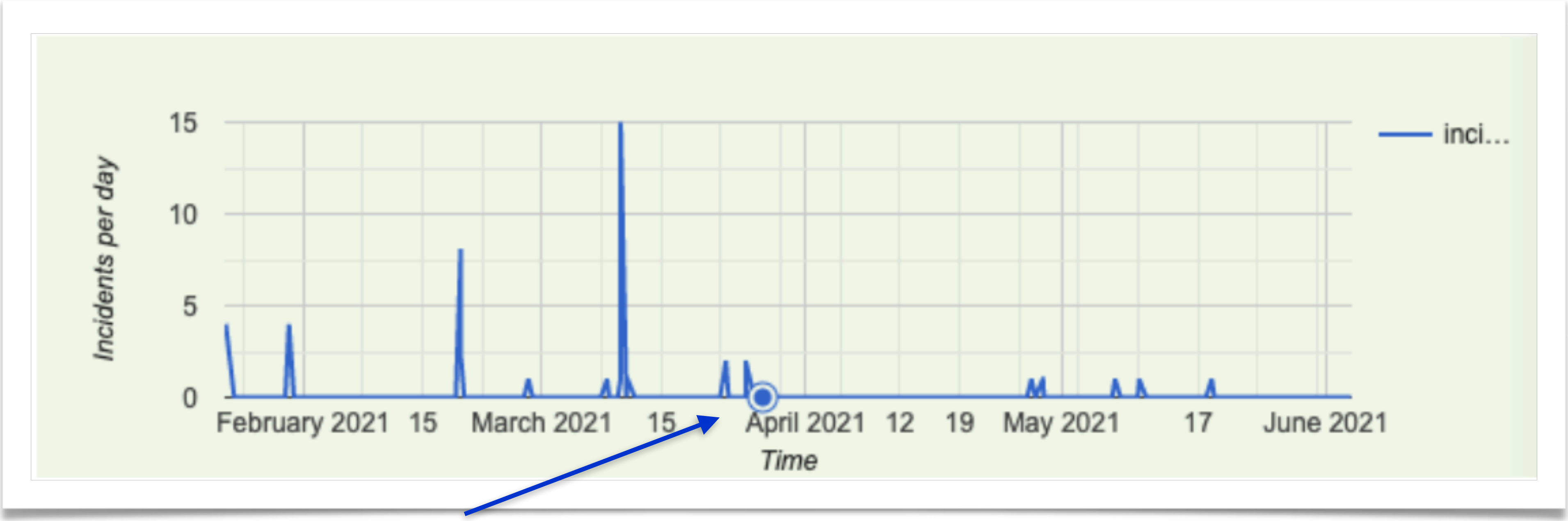
🟩 Wrong maxLength

🟧 We announced a customer’s prefix, but they had no ROA for AS2914 (AS mismatch due to customer’s ROA)

🟨 We migrated prefixes from one AS to another, but no ROA update (AS mismatch)



Results after NTT improvements



where we stepped-up our game

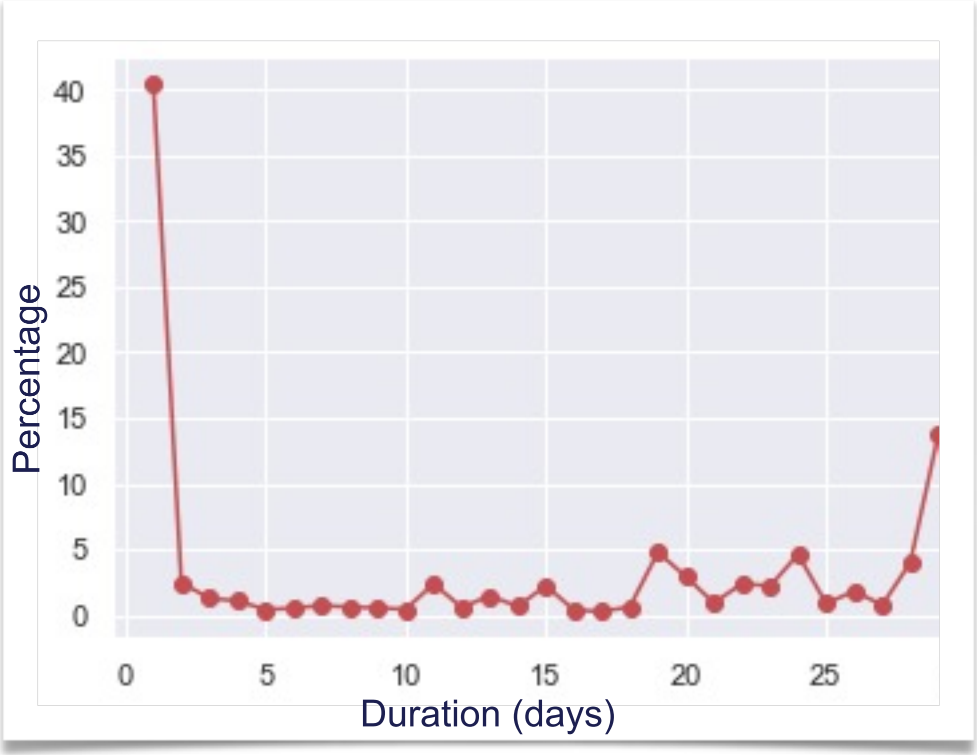
- **86.84% reduction of RPKI-invalid announcements**

RPKI timing

- Invalid announcements can be just transient
  - e.g., you announce before the ROA is public

But how do you define “transient” if you are not monitoring?

Invalid MaxLength 2021 - 1 month window



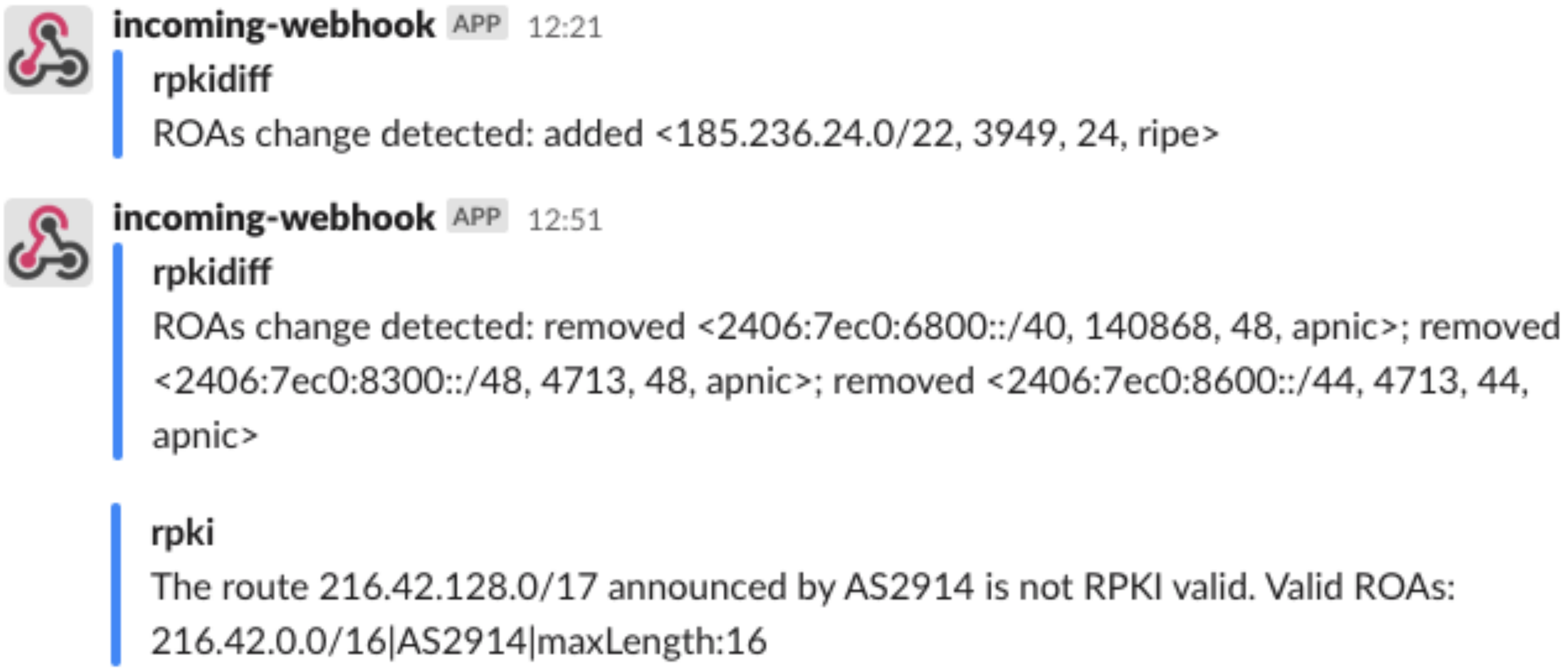
BGPalerter

- Most of the logic is implemented in BGPalerter
  - https://github.com/nttgin/BGPalerter
  - Real-time monitoring for BGP and RPKI
  - It is easy to use
    - Auto-configuration
    - No installation required - It’s just a binary that you run
    - No data collection required
  - *Hijack detection, visibility loss, path monitoring, upstream/downstream monitoring, and RPKI monitoring*

BGPalerter RPKI monitoring

- You will receive an alert if:
  - Your AS is announcing RPKI invalid prefixes
  - Your AS is announcing prefixes not covered by ROAs
  - ROAs covering your prefixes disappeared
  - A ROA involving any of your prefixes or ASes was deleted/added/edited
  - TA malfunction or corrupted VRP file
  - A ROA is expiring

Examples of alerts



incoming-webhook APP 12:21

rpkidiff

ROAs change detected: added <185.236.24.0/22, 3949, 24, ripe>

incoming-webhook APP 12:51

rpkidiff

ROAs change detected: removed <2406:7ec0:6800::/40, 140868, 48, apnic>; removed <2406:7ec0:8300::/48, 4713, 48, apnic>; removed <2406:7ec0:8600::/44, 4713, 44, apnic>

rpki

The route 216.42.128.0/17 announced by AS2914 is not RPKI valid. Valid ROAs: 216.42.0.0/16|AS2914|maxLength:16

Thank you.

Massimo Candela

Senior Software Engineer, Network Information Systems Development

Global IP Network

massimo@ntt.net

@webrobotics

www.gin.ntt.net

@GinNTTnet #globalipnetwork #AS2914