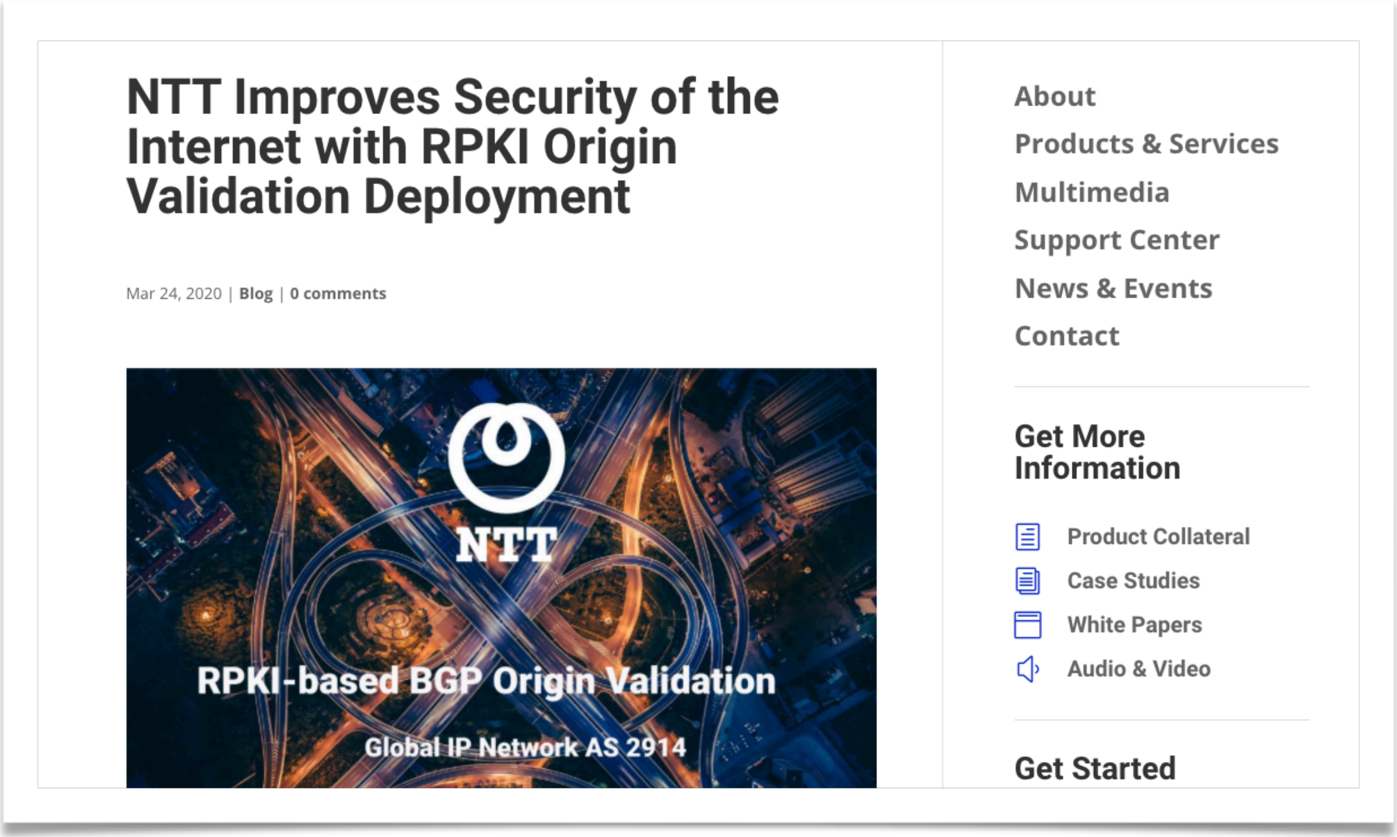
A one-year review of RPKI operations

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:

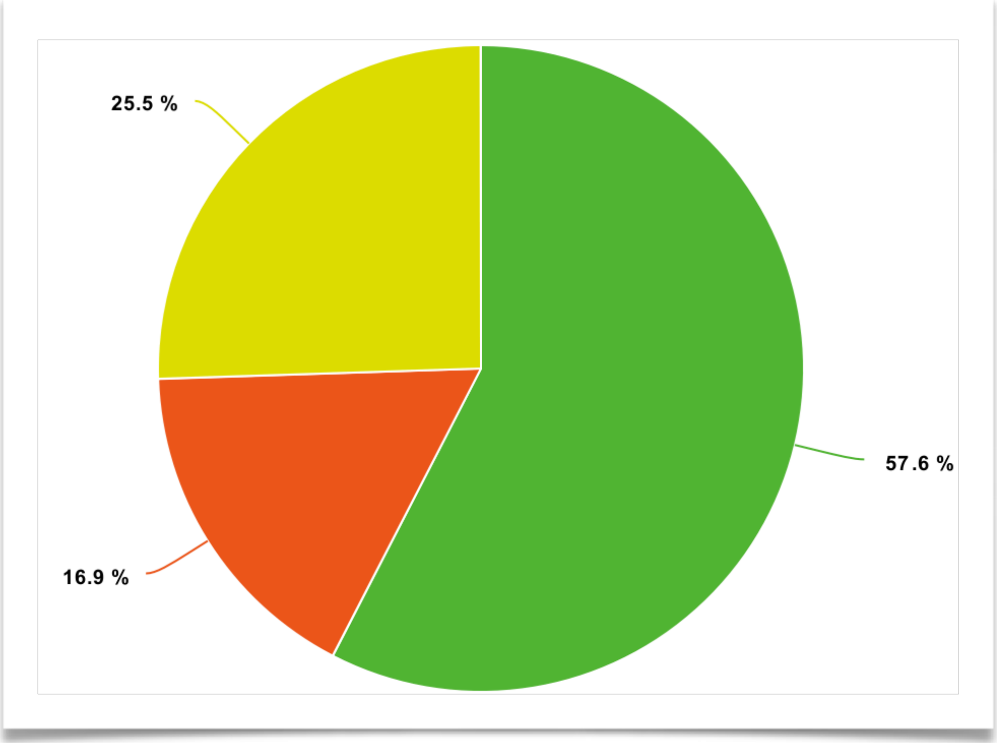
1. Wrong maxLength
2. We announced a customer’s prefix, but they had no ROA for AS2914 (AS mismatch due to customer’s ROA)
3. We migrated prefixes from one AS to another, but no ROA update (AS mismatch)

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)

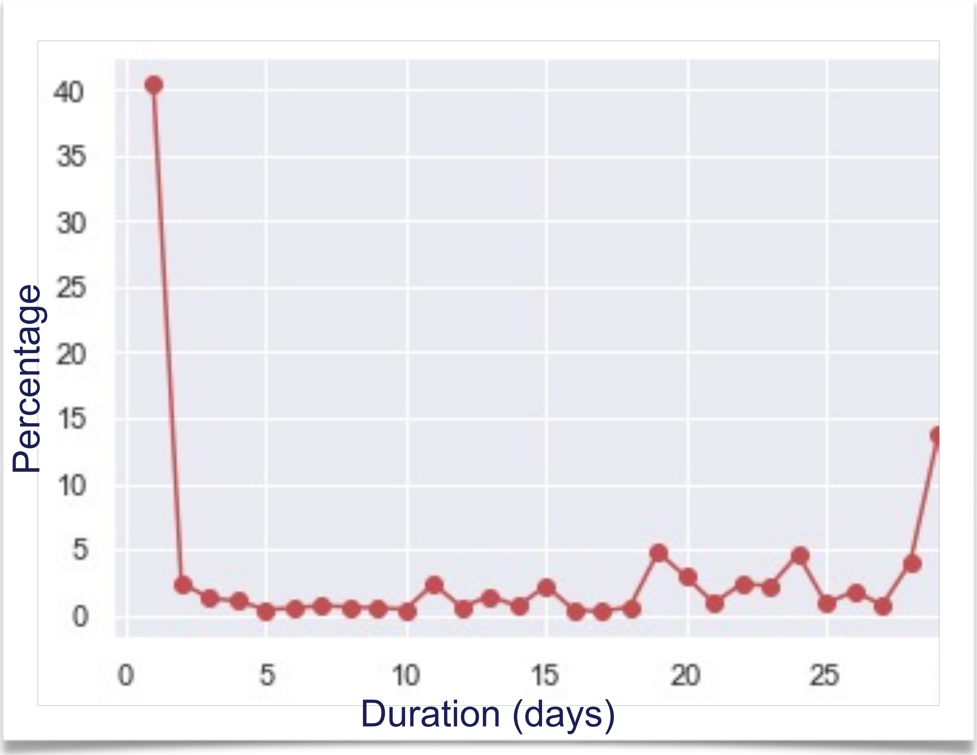


RPKI timing

- 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



How did we address our mistakes?

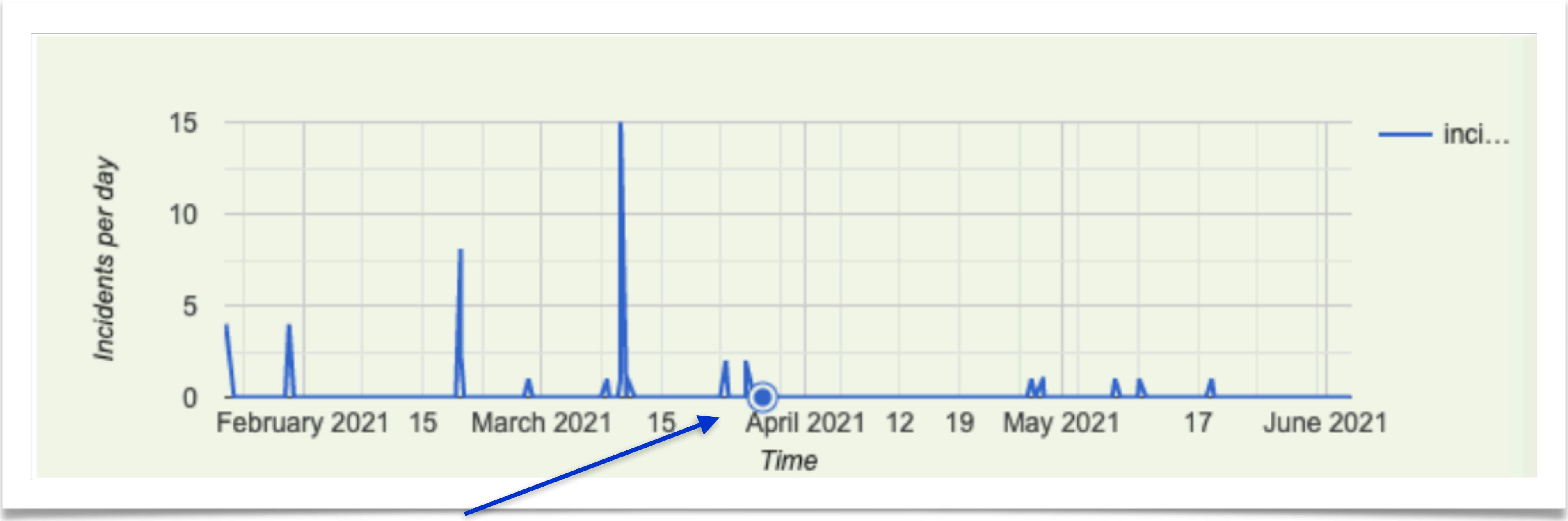
1. Introduced a new automation platform

2. Improved our monitoring

3. Introduced a strict procedure to follow

4. Improved communication with customers

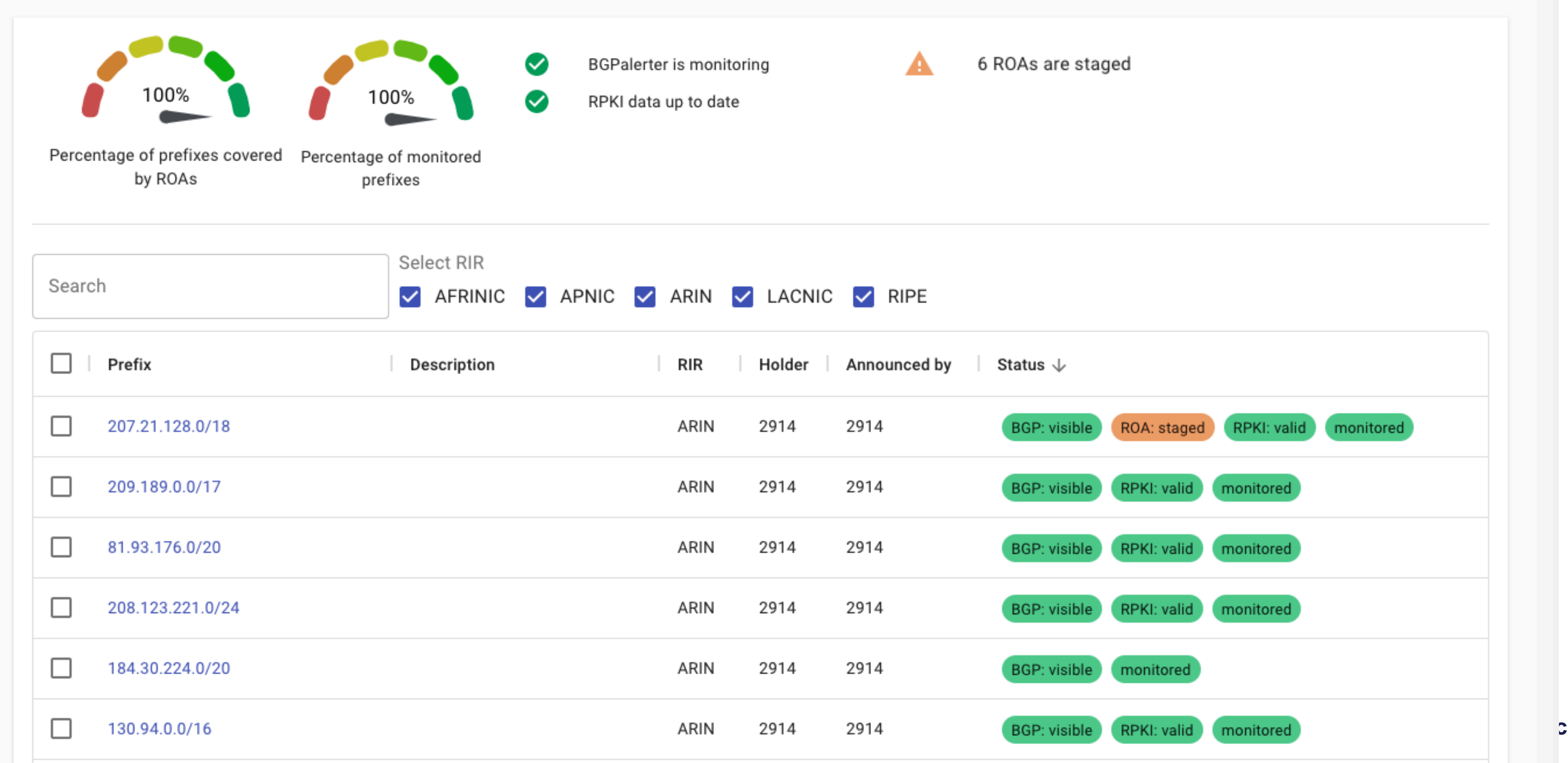
Before seeing how, let’s see the results



where we stepped-up our game

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

NTT's IP Management Platform (automation + monitoring)



Percentage of prefixes covered by ROAs

Percentage of monitored prefixes

✓ BGPalerter is monitoring

✓ RPKI data up to date

⚠ 6 ROAs are staged

Search

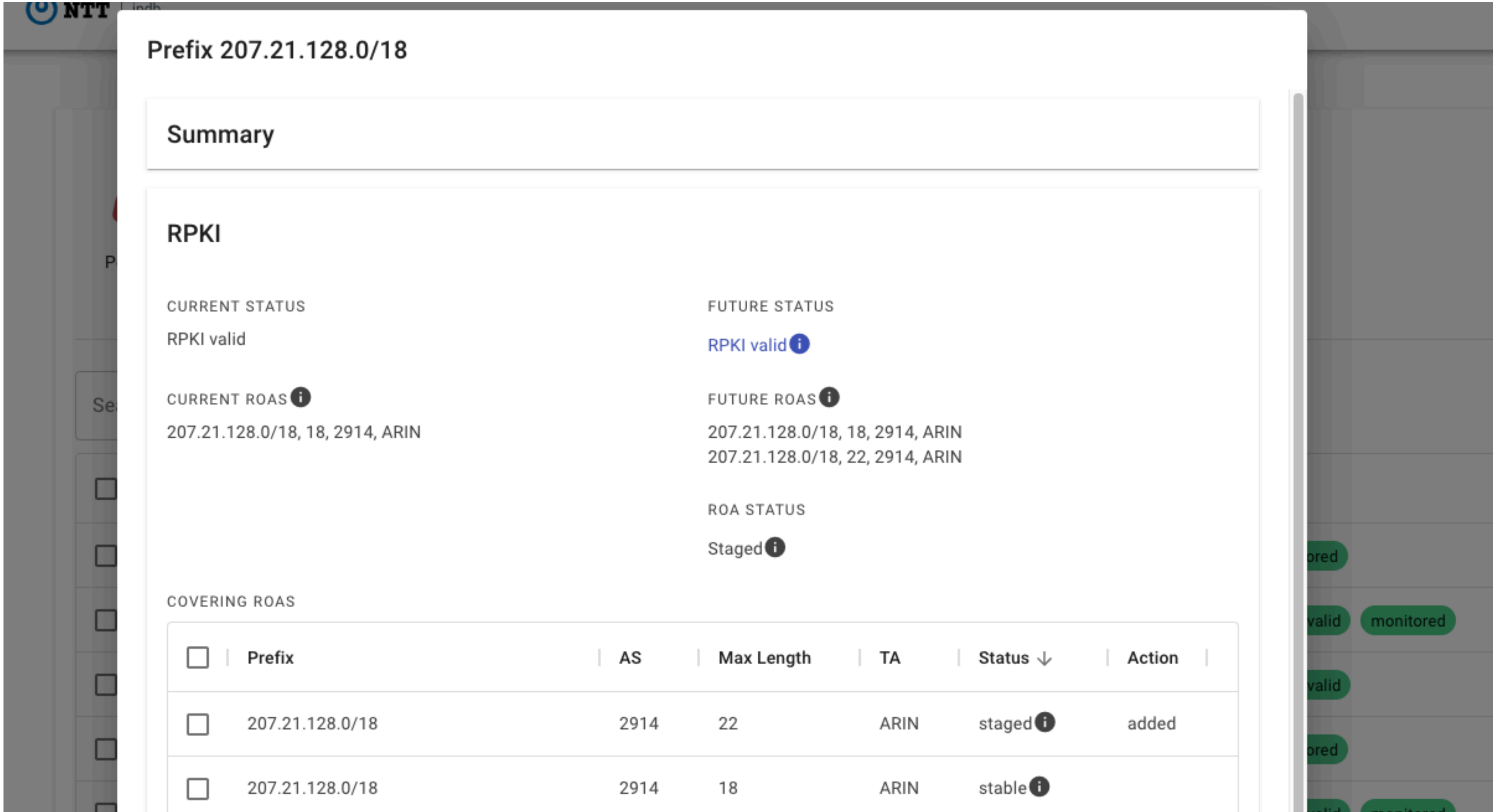
Select RIR

☑ AFRINIC ☑ APNIC ☑ ARIN ☑ LACNIC ☑ RIPE

□	Prefix	Description	RIR	Holder	Announced by	Status ↓
□	207.21.128.0/18		ARIN	2914	2914	BGP: visible ROA: staged RPKI: valid monitored
□	209.189.0.0/17		ARIN	2914	2914	BGP: visible RPKI: valid monitored
□	81.93.176.0/20		ARIN	2914	2914	BGP: visible RPKI: valid monitored
□	208.123.221.0/24		ARIN	2914	2914	BGP: visible RPKI: valid monitored
□	184.30.224.0/20		ARIN	2914	2914	BGP: visible monitored
□	130.94.0.0/16		ARIN	2914	2914	BGP: visible RPKI: valid monitored

cs

RPKI management



Prefix 207.21.128.0/18

Summary

RPKI

CURRENT STATUS

RPKI valid

FUTURE STATUS

RPKI valid

CURRENT ROAS

207.21.128.0/18, 18, 2914, ARIN

FUTURE ROAS

207.21.128.0/18, 18, 2914, ARIN
207.21.128.0/18, 22, 2914, ARIN

ROA STATUS

Staged

COVERING ROAS

□	Prefix	AS	Max Length	TA	Status ↓	Action
□	207.21.128.0/18	2914	22	ARIN	staged	added
□	207.21.128.0/18	2914	18	ARIN	stable	

botics

Our four stages for ROAs

- ***Staged*** - the ROA exists only in the local database
  - RPKI validation is performed on a merge of public ROAs and staged ROAs
  - If what currently announced (or what is supposed to be announced) is RPKI valid, **all** the ROAs covering the prefix can be committed
- ***Committed*** - the ROA is ready to be published
  - The ROA is sent to the proper repo (e.g., RIR)
- ***Public*** - the ROA is visible on public repos
  - RPKI is up to date now
- ***Stable*** - the ROA has been monitored for 24 hours without issues
  - The monitoring will continue forever

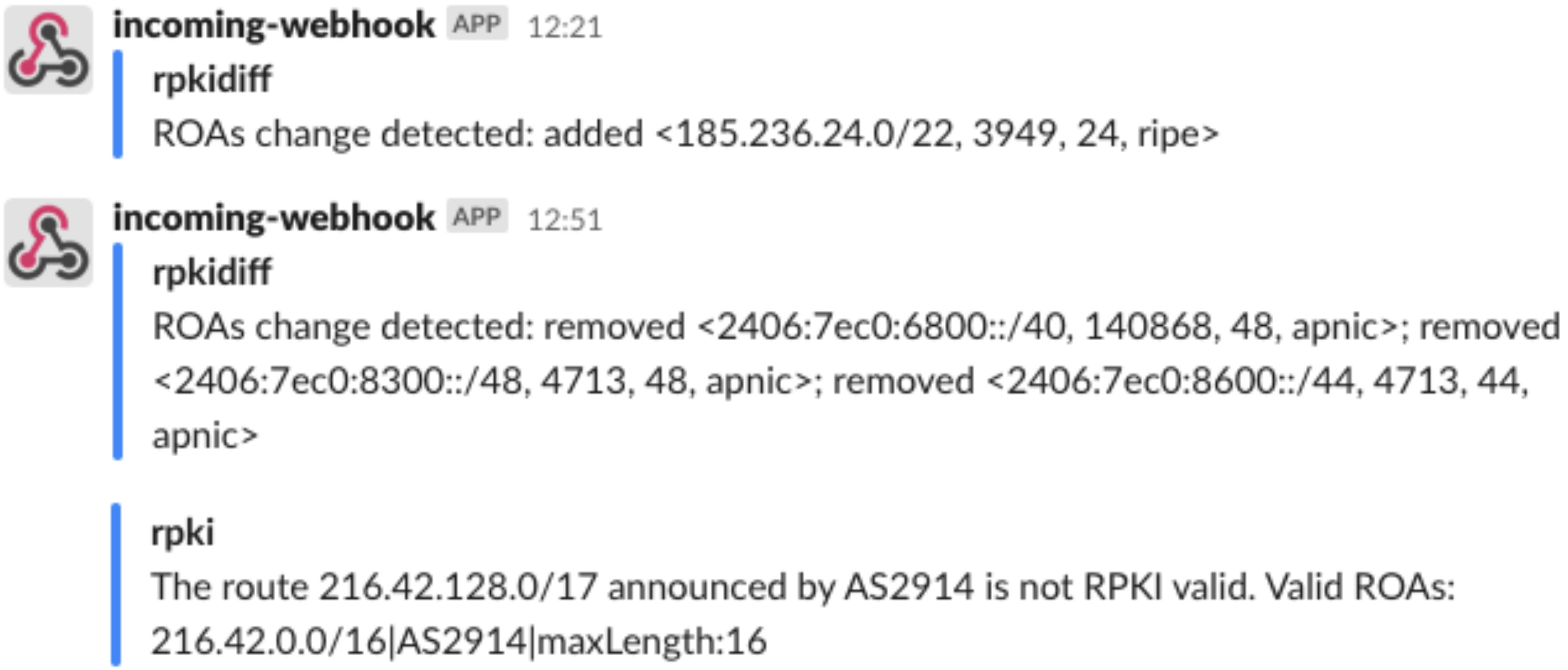
BGPalerter

- 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, 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

Shout outs to some amazing projects

- RIPE RIS Live
  - real-time, free, and has 600+ peers worldwide
  - It’s an amazing project from RIPE NCC
  - Want to peer? https://ris.ripe.net

- OpenBSD rpki-client
  - https://www.rpki-client.org/
  - Exports data about expiring ROAs (thanks Job Snijders)
  - Runs on any Linux and BSD distribution

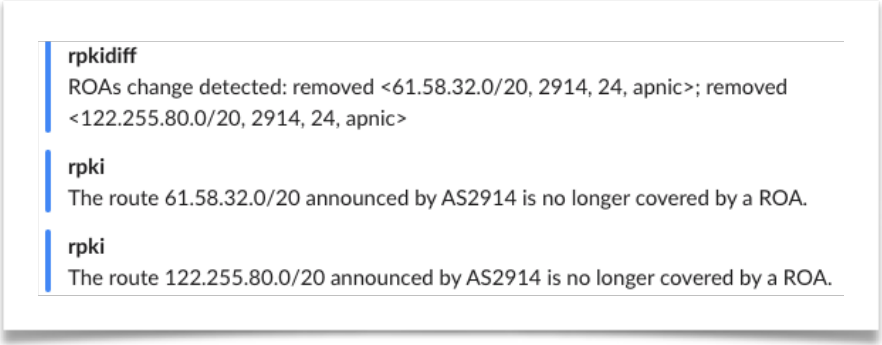
MANRS

- Mutually Agreed Norms for Routing Security
- A list of concrete actions for ISPs, IXPs, CDNs, and HW vendors

RPKI infrastructure malfunctions

- 12 August 2020
  - BGPalerter reports many prefixes "no longer covered by ROA” in ARIN
    - Users think it’s a BGPalerter false positive (e.g., https://github.com/nttgin/BGPalerter/issues/324)
  - ARIN announcement https://www.arin.net/announcements/20200813/
  - **Time for a new TA monitoring feature!**

- 06 February 2021
  - TWNIC ROAs disappear
  - BGPalerter sends alerts
  - Hardware failure reported by TWNIC



rpkidiff
ROAs change detected: removed <61.58.32.0/20, 2914, 24, apnic>; removed <122.255.80.0/20, 2914, 24, apnic>

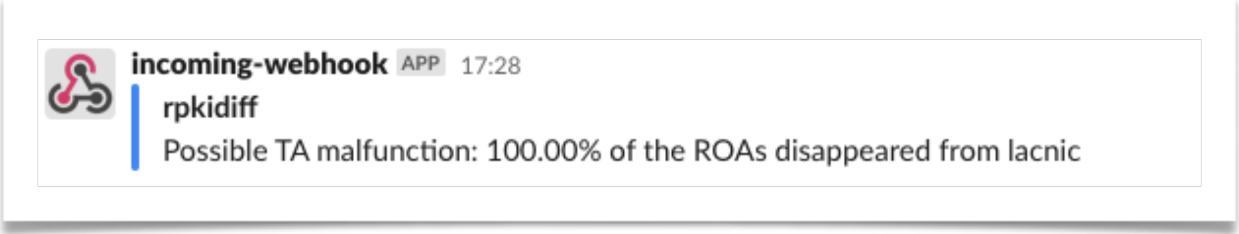
rpki
The route 61.58.32.0/20 announced by AS2914 is no longer covered by a ROA.

rpki
The route 122.255.80.0/20 announced by AS2914 is no longer covered by a ROA.

RPKI infrastructure malfunctions

- 18 March 2021
  - We discover that we missed RIPE ROAs in a validation cycle
    - This happened already in the past.
  - We found a manifest containing references to not available certs
  - We report this to the RIPE NCC staff, and they fix it
    - https://www.ripe.net/ripe/mail/archives/routing-wg/2021-May/004345.html

- 17 June 2021
  - We discovered LACNIC disappearing over rsync
  - We whatsapp our friends at LACNIC and they fix it



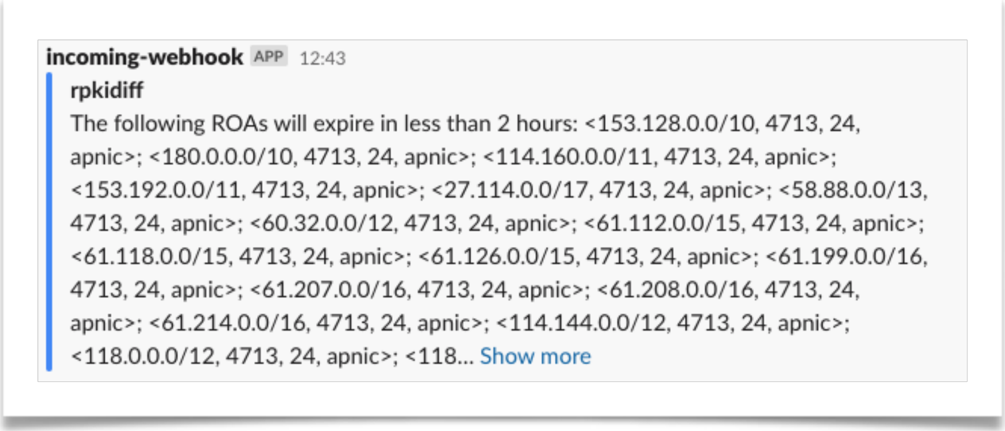
incoming-webhook APP 17:28

rpkidiff

Possible TA malfunction: 100.00% of the ROAs disappeared from lacnic

RPKI infrastructure malfunctions

- 1 February 2022
  - JPNIC partial TA malfunction
  - Several ROAs were expiring soon
  - We report it to JPNIC, and they fix it, it was a disk full
    - https://www.nic.ad.jp/en/topics/2022/20220202-01.html



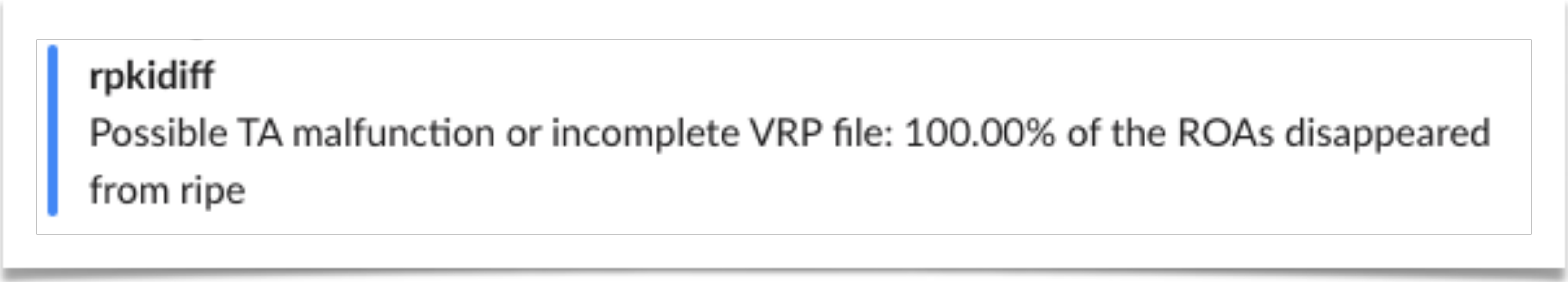
incoming-webhook APP 12:43

rpkidiff

The following ROAs will expire in less than 2 hours: <153.128.0.0/10, 4713, 24, apnic>; <180.0.0.0/10, 4713, 24, apnic>; <114.160.0.0/11, 4713, 24, apnic>; <153.192.0.0/11, 4713, 24, apnic>; <27.114.0.0/17, 4713, 24, apnic>; <58.88.0.0/13, 4713, 24, apnic>; <60.32.0.0/12, 4713, 24, apnic>; <61.112.0.0/15, 4713, 24, apnic>; <61.118.0.0/15, 4713, 24, apnic>; <61.126.0.0/15, 4713, 24, apnic>; <61.199.0.0/16, 4713, 24, apnic>; <61.207.0.0/16, 4713, 24, apnic>; <61.208.0.0/16, 4713, 24, apnic>; <61.214.0.0/16, 4713, 24, apnic>; <114.144.0.0/12, 4713, 24, apnic>; <118.0.0.0/12, 4713, 24, apnic>; <118... Show more

RPKI infrastructure malfunctions

- 16 February 2022
  - rrdp.ripe.net becomes unreachable AND too many connections to rsync
  - BGPalerter detects the issue
  - It was a DNS misconfiguration
    - https://www.ripe.net/ripe/mail/archives/routing-wg/2022-February/004522.html



rpkidiff

Possible TA malfunction or incomplete VRP file: 100.00% of the ROAs disappeared from ripe

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