RPKI implementation at BIT

By: Teun Vink (teun@bit.nl)

About BIT and myself

- AS12859
- Business-to-business ISP and Datacenters
- Focus on technology, tailor-made solutions
- Teun: 13 years at BIT, team leader of Network Operations

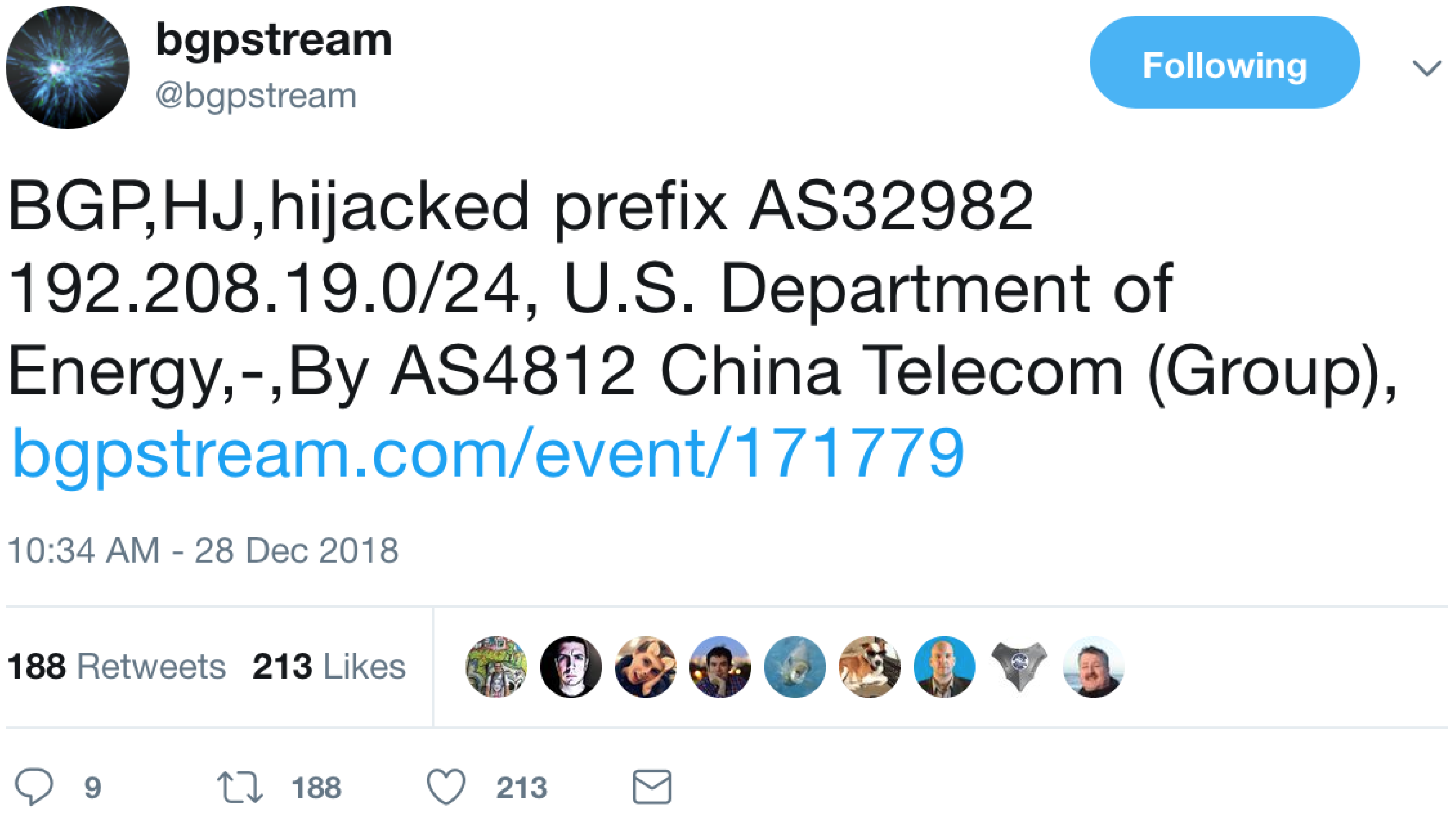
RPKI Implementation - Why?

Our customers expect from us that we:

- keep their IPs and services reachable
- offer them correct routes to the internet

And thus that we implement available tools to achieve that.

RPKI Implementation - Why?



bgpstream
@bgpstream

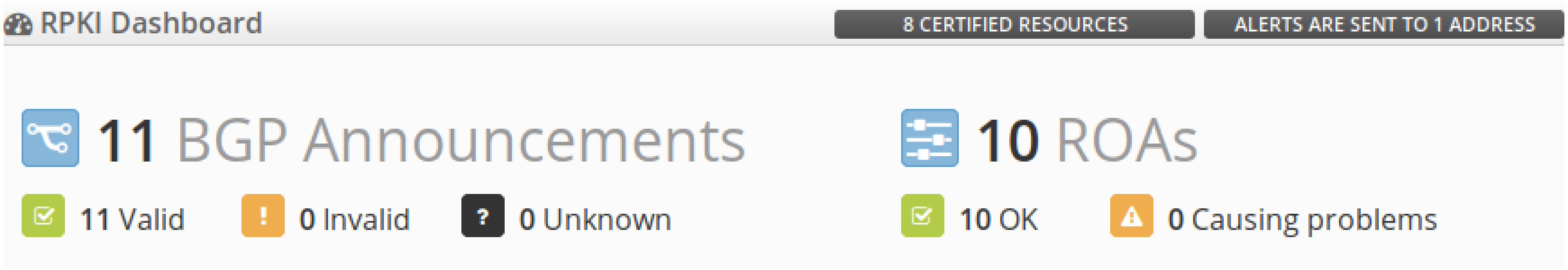
BGP,HJ,hijacked prefix AS32982 192.208.19.0/24, U.S. Department of Energy,-,By AS4812 China Telecom (Group), bgpstream.com/event/171779

10:34 AM - 28 Dec 2018

188 Retweets 213 Likes

RPKI signing at BIT

- All our own prefixes were signed in September 2018
- Making ROAs is easy in RIPE's LIR Portal



RPKI Dashboard

8 CERTIFIED RESOURCES

ALERTS ARE SENT TO 1 ADDRESS

11 BGP Announcements

✓ 11 Valid

! 0 Invalid

? 0 Unknown

10 ROAs

✓ 10 OK

⚠ 0 Causing problems

RPKI signing - considerations

- DDoS mitigation:
  - Divert traffic via BGP through NBIP Nawas by advertising more specific routes
  - **ROAs need to match!**
- Customers with own IP's need to fix ROAs themselves

RPKI validation

- Implemented in September 2018
- Validation on Juniper core routers (JunOS 15.1R7.8)
- RIPE RPKI Validator (wish: Routinator as 2nd validator)
- Chosen policy: `invalid == reject`

RPKI validation - implementation

1. Install RIPE's RPKI Validator (don't forget ARIN's TAL)
2. Configure validation sessions on Juniper routers
3. Check validation databases
4. Add an *import policy* on routes learned from transits and peers. First **label only**: `valid` / `unknown` / `invalid`

RPKI validation - implementation (2)

1. Many manual checks on `invalid` routes
2. `invalid == reject` import policy on peerings and transits
3. `invalid == reject` import policy on customer BGP sessions
4. Now we shouldn't see any `invalid` routes!
5. Add `invalid == reject` to **all** export policies

RPKI validation - considerations

- `invalid == reject` **only** works if present on **all** eBGP sessions
- If you accept a default route validation is pointless*
- Implement and test monitoring of validators and validation sessions
- Be careful when transferring IP space!

bit internet technology

RPKI validation in practice

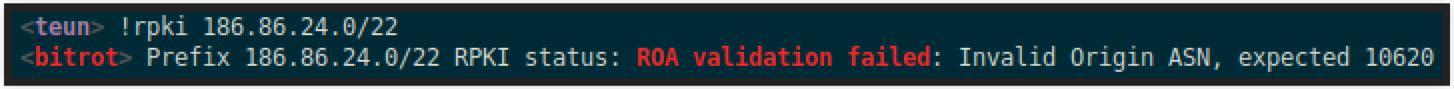
Tools and knowledge

- Training support desks is essential, so they can recognize reachability issues possibly caused by RPKI
- Offer tooling to check RPKI validation status

Checking validation status

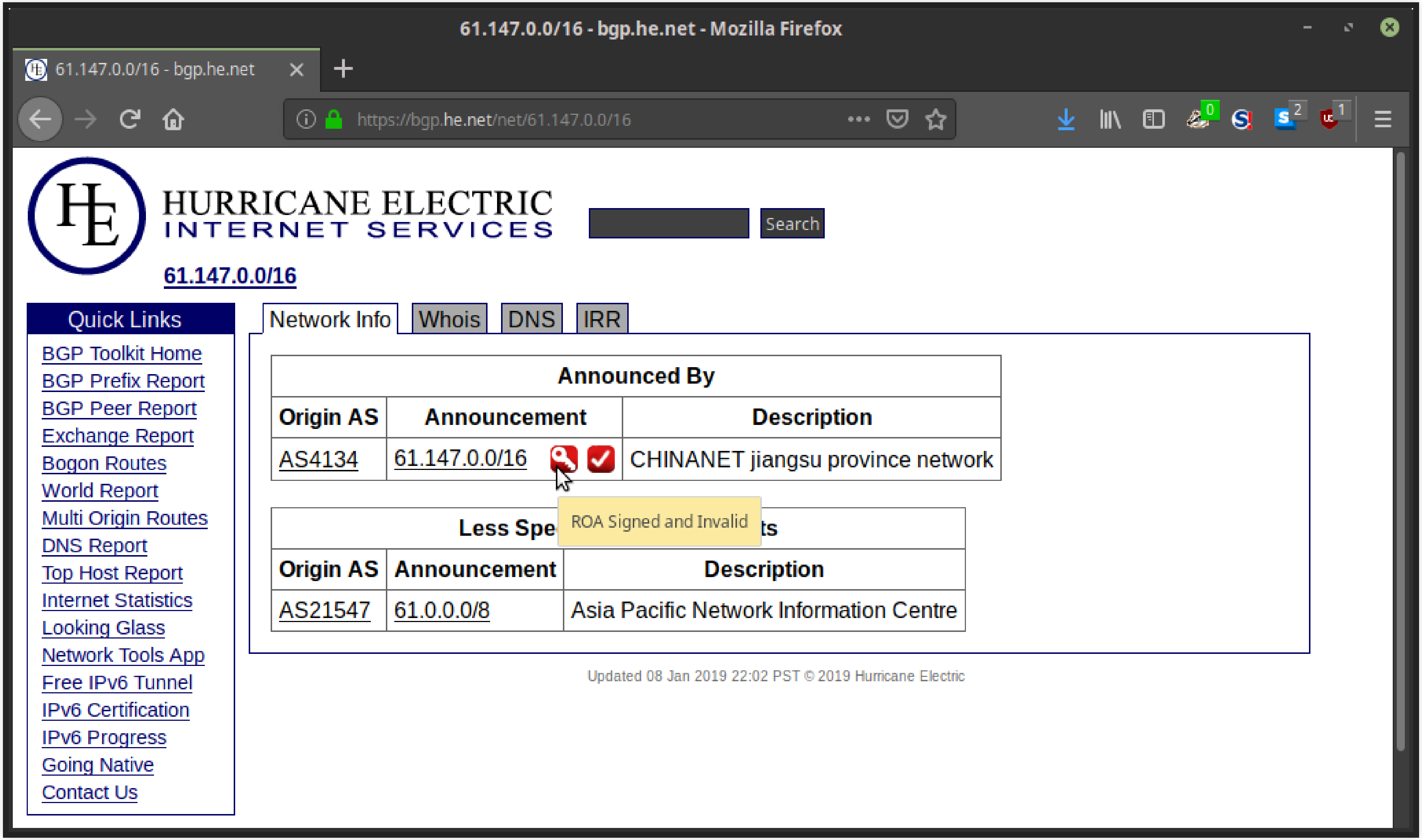
```
$ whois -h whois.bgpmon.net 61.147.0.0/16

Prefix:                61.147.0.0/16
Prefix description:
Country code:          CN
Origin AS:             4134
Origin AS Name:        CHINANET-BACKBONE No.31,Jin-rong Street, CN
RPKI status:           ROA validation failed: Invalid Origin ASN, expected 23650
First seen:            2011-10-19
Last seen:             2019-01-08
Seen by #peers:        65
```



```
<teun> !rpki 186.86.24.0/22
<bitrot> Prefix 186.86.24.0/22 RPKI status: ROA validation failed: Invalid Origin ASN, expected 10620
```

External tools



61.147.0.0/16

Announced By

Origin AS	Announcement	Description
AS4134	61.147.0.0/16	CHINANET jiangsu province network

ROA Signed and Invalid

Less Spe[…]**ts**

Origin AS	Announcement	Description
AS21547	61.0.0.0/8	Asia Pacific Network Information Centre

Updated 08 Jan 2019 22:02 PST © 2019 Hurricane Electric

Experiences

Problems caused by RPKI validation reported by customers:

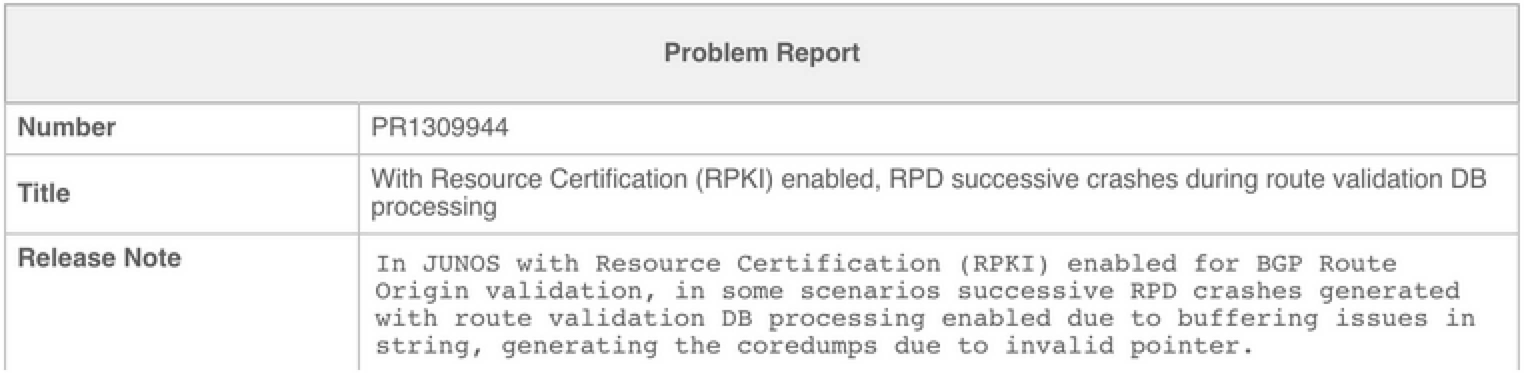
5

- 1st was reported within 1h after enabling
- 3 were resolved quickly after contacting owners
- 2 were resolved* after several months
- all seem to be unintentional, administrative errors

Experiences

- Customers understand and appreciate that we reject RPKI invalid routes, even if that breaks things
- Having an external source to point at helps to show there's a problem at the other side
- So far we only had to configure **one** exception

Experiences



Problem Report	
Number	PR1309944
Title	With Resource Certification (RPKI) enabled, RPD successive crashes during route validation DB processing
Release Note	In JUNOS with Resource Certification (RPKI) enabled for BGP Route Origin validation, in some scenarios successive RPD crashes generated with route validation DB processing enabled due to buffering issues in string, generating the coredumps due to invalid pointer.

- 22-12-2018: major outage due to validation
- Continuous crashes of RPD process, eventually disabling RPKI validation sessions stopped the crashes
- RPKI validation is **temporarily disabled** since
- We **will** reactivate RPKI validation

Final remarks

- Don't be afraid to implement RPKI signing and validation
- Herd immunity: my network becomes safer if **you** implement both signing and validation

bit internet technology

Questions?

Teun Vink (teun@bit.nl)