BGP and RPKI Monitoring with BGPalerter

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

Why monitoring

- Monitoring the correctness of BGP is a fundamental activity for any actor operating on the Internet
- Monitoring BGP is not only identifying hijacks committed by other ASes, but especially for timely identifying what your AS is doing.
  - Identify a prefix you were not supposed to announce
  - Identify a loss of visibility due to a wrong just-deployed configuration

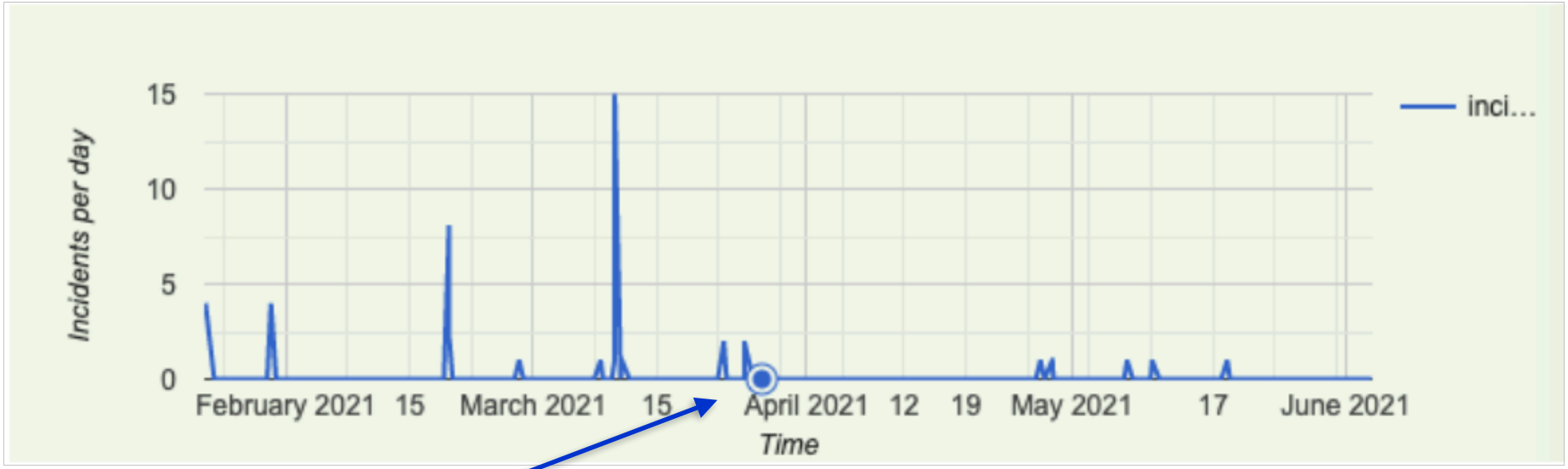
Additionally, RPKI…

- **BGP + RPKI are two different planes,** making them work in parallel requires some effort

In an Internet composed of thousands of network players, with different levels of automation and expertise, providing free and easy to use tools for monitoring the correctness of **BGP** and **RPKI** is a key operation in improving the stability of the global Internet

Massimo Candela | massimo@ntt.net | @webrobotics

Some of our results



where we stepped-up our game

- **86.84% reduction of RPKI-invalid announcements**
- With the new system we staged/tested and monitored 565 new ROAs

Massimo Candela | massimo@ntt.net | @webrobotics

BGPalerter

BGPalerter is a tool for monitoring BGP and RPKI

- We developed it for monitoring NTT's prefixes
- We released it open-source (BSD-3-Clause)
  - https://github.com/nttgin/BGPalerter
- It works in real time
- It's easy to use
  - Includes auto configuration
  - No data collection needed

Open datasets

- By default BGPalerter connects to Open datasets

- The BGP data is coming from RIPE RIS Live
  - Which is real-time, free, and has 600+ peers worldwide
  - It's an amazing project from RIPE NCC

Want to peer?

https://ris.ripe.net

Download and run. That's all.

```
wget https://github.com/nttgin/BGPalerter/releases/latest/download/bgpalerter-linux-x64

chmod +x bgpalerter-linux-x64

./bgpalerter-linux-x64
```

- Or, run it as a Linux service

What you can monitor

- Any of your prefixes loses visibility;
- Any of your prefixes is hijacked;
- Your AS is announcing RPKI invalid prefixes;
- Your AS is announcing prefixes not covered by a ROA;
- Your AS is announcing a new prefix that was never announced before;
- Any of your ROAs is expiring;
- ROAs covering your prefixes are no longer available;
- RPKI Trust Anchors malfunctions;
- A ROA involving any of your prefixes or ASes was deleted/added/edited;
- An unexpected upstream (left-side) AS appears in an AS path;
- An unexpected downstream (right-side) AS appears in an AS path;
- One of the AS path used to reach your prefix matches a specific condition defined by you.

Example of BGPalerter notifications

visibility
The prefix 165.254.225.0/24 (description 1) has been withdrawn. It is no longer visible from 4 peers.

misconfiguration
AS2914 is announcing 46.3.92.0/22 but this prefix is not in the configured list of announced prefixes

hijack
A new prefix 165.254.255.0/25 is announced by AS4, and AS15562. It should be instead 165.254.255.0/24 (description 2) announced by AS15562

hijack
A new prefix 2a00:5884:ffff:/48 is announced by AS208585. It should be instead 2a00:5884::/32 (alarig fix test) announced by AS204092, and AS45

hijack
The prefix 2a00:5884::/32 (alarig fix test) is announced by AS15563 instead of AS204092, and AS45

newprefix
Possible change of configuration. A new prefix 2a00:5884:ffff:/48 is announced by AS204092. It is a more specific of 2a00:5884::/32 (alarig fix test).

Massimo Candela | massimo@ntt.net | @webrobotics

Examples of RPKI alerts

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

OpenBSD rpki-client

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

Reports

- At the moment alerts can be delivered to:
  - **Files, Email, Slack, Alerta dashboard, Kafka, Syslog, Webex, Mattermost, Telegram, Pushover, any HTTP end-point**

Report by email

```
The prefix 165.254.255.0/24 (Job) is announced by AS2914 instead of AS15562


DETAILS:
----------------------------------------------------
Monitored prefix:      165.254.255.0/24
Prefix Description:    Job
Usually announced by:  AS15562
Event type:            basic-hijack-detection
Now announced by:      AS2914
Now announced with:    165.254.255.0/24
When event started:    2019-08-15 09:10:05 UTC
Last event:            2019-08-15 09:10:05 UTC
Detected by peers:     1
See in BGPlay:         https://stat.ripe.net/widget
/bgplay#w.resource=165.254.255.0/24&w.ignoreReannouncements=true&
w.starttime=1565859905&w.endtime=1565860205&
w.rrcs=0,1,2,5,6,7,10,11,13,14,15,16,18,20&w.type=bgp
```

Contribute!

- Source code on GitHub
  - https://github.com/nttgin/BGPalerter
- More BGPalerter news on twitter: @webrobotics

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