



Easy BGP and RPKI monitoring

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

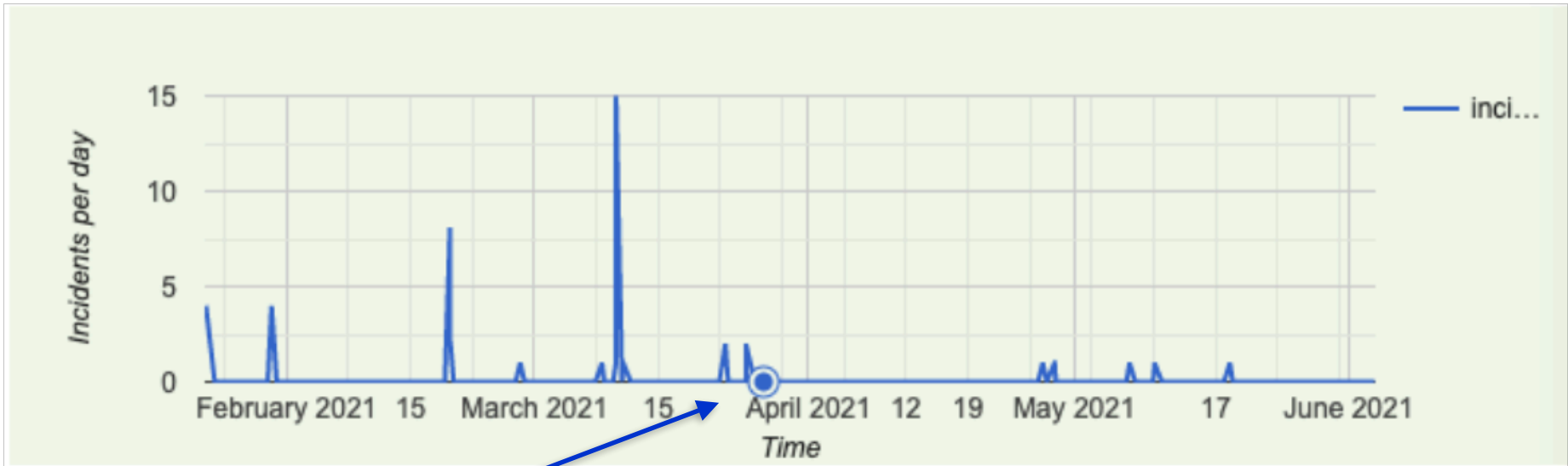
Additionally, RPKI...



- **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

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

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

- 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>

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).

Examples of RPKI alerts



rpkidiff

Possible TA malfunction or incomplete VRRP 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>

rпки
















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



Setup

[main](#) 4 branches 25 tags

[Go to file](#) [Add file](#) [Code](#)

 massimocandela Merge pull request #801 from nttgin/dependabot/npm_... 3aaa07b 13 hours ago 1,998 commits		
 .github	fixed wrong kafka source	2 months ago
 docs	improved expiring roa doc	2 months ago
 src	minor logging improvements	2 months ago
 tests	split channels for rpki and roa monitoring	2 months ago
 .babelrc	prep for npm packaging	17 months ago
 .eslintrc.json	added mocha support for esling	3 years ago
 .gitignore	added tmp files to gitignore	11 months ago
 .hound.yml	Update .hound.yml	3 years ago
 .npmignore	added support for external config manager and for user groups defin...	13 months ago
 AUTHORS	add github actions (#446)	15 months ago
 Dockerfile	default to node 14 for builds	6 months ago
 LICENSE	added license bsd3	3 years ago
 README.md	fixed link to pull api in readme	9 months ago
 build.sh	default to node 14 for builds	6 months ago

About



Software to monitor streams of BGP data. Pre-configured for real-time detection of visibility loss, RPKI invalid announcements, hijacks, and more.

[monitoring](#) [internet](#) [bgp](#) [network](#)
[rpki](#)

- [Readme](#)
- [BSD-3-Clause License](#)
- [490 stars](#)
- [35 watching](#)
- [96 forks](#)

Releases 21

[v1.29.0](#) Latest
on Oct 25, 2021

[+ 20 releases](#)

Contributors 41



Releases / v1.29.0

v1.29.0

Latest

Compare



 massimocandela released this Oct 25, 2021  v1.29.0  3d2e08a

[minor]

- Introduced authentication header for websocket connections [006eb64](#)
- Introduced timeout verification in case of missing open message from RIS [0125b17](#)
- Introduced OpsGenie HTTP configuration example [d1761bb](#) (thanks @trickv)
- Introduced RocketChat HTTP configuration example [0f52fb2](#) (thanks @cadirol)
- Binaries are now compiled against node 14 [006eb64](#)

[patch]

- Updated dependencies
- Fixed trailing slash bug on ws parameters [e4f19d3](#)
- Improved documentation about volume parameter [2bb199a](#)
- Update Kafka version in automated tests environment [53203ba](#)
- Adopted semver nomenclature in documentation [4491f4e](#)
- Filter out RIS beacons when these are used only as a health check of the socket (preventing [#732](#) for some RIS feeders) [4301b2b](#)
- Improved TA malfunction alert [fdce01d](#)

- 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](#)

Auto configuration



```
BGPalerter, version: 1.29.0 environment: production
```

```
Loaded config: /config.yml
```

```
? The file prefixes.yml cannot be loaded. Do you want to auto-configure BGPalerter? Yes
```

```
? Which Autonomous System(s) you want to monitor? (comma-separated, e.g. 2914,3333)  
2914
```

```
? Do you want to be notified when your AS is announcing a new prefix? Yes
```

```
? Do you want to be notified when a new upstream AS appears in a BGP path? Yes
```

```
? Do you want to be notified when a new downstream AS appears in a BGP path? Yes
```



```
BGPalerter, version: 1.29.0 environment: production
Loaded config: /home/bgpalerter/production/config.yml
Monitoring 165.254.225.0/24
Monitoring 165.254.255.0/24
Monitoring 192.147.168.0/24
Monitoring AS2914
```

- The auto-configuration runs only the first time
- If your prefixes are not covered by ROAs, a warning will ask you to review prefixes.yml by hand

- Alerts are automatically bundled/throttled
- At the moment alerts can be delivered to:
 - **Files, Email, Slack, Alerta dashboard, Kafka, Syslog, Webex, Mattermost, Telegram, Pushover, any HTTP end-point**
- Users groups allow to deliver alerts about specific resources, or about specific types of issue, to specific set of users/targets
- Also the BGP messages can be sent to files, another monitoring system, or database

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>

```
1 connectors:
2   - file: connectorRIS
3     name: ris
4     params:
5       carefulSubscription: true
6       url: ws://ris-live.ripe.net/v1/ws/
7       perMessageDeflate: true
8       subscription:
9         moreSpecific: true
10        type: UPDATE
11        host:
12        socketOptions:
13          includeRaw: false
14
15 monitors:
16   - file: monitorHijack
17     channel: hijack
18     name: basic-hijack-detection
19     params:
20       thresholdMinPeers: 2
21
22   - file: monitorNewPrefix
23     channel: newprefix
24     name: prefix-detection
25     params:
26       thresholdMinPeers: 2
27
28   - file: monitorPath
29     channel: path
30     name: path-matching
31     params:
32       thresholdMinPeers: 0
33
34   - file: monitorVisibility
35     channel: visibility
36     name: withdrawal-detection
37     params:
38       thresholdMinPeers: 20
39
40
```

```
15 monitors:
16   - file: monitorHijack
17     channel: hijack
18     name: basic-hijack-detection
19     params:
20       thresholdMinPeers: 2
21
22   - file: monitorNewPrefix
23     channel: newprefix
24     name: prefix-detection
25     params:
26       thresholdMinPeers: 2
27
28   - file: monitorPath
29     channel: path
30     name: path-matching
31     params:
32       thresholdMinPeers: 0
33
34   - file: monitorVisibility
35     channel: visibility
36     name: withdrawal-detection
37     params:
38       thresholdMinPeers: 20
39
40   - file: monitorAS
41     channel: misconfiguration
42     name: asn-monitor
43     params:
44       thresholdMinPeers: 2
45
46   - file: monitorRPKI
47     channel: rpki
48     name: rpki-monitor
49     params:
50       vrpProvider: ntt
51       thresholdMinPeers: 1
52       checkUncovered: false
53       preCacheROAs: true
54       refreshVrpListMinutes: 15
55
```

```
55 reports:
56 - file: reportFile
57   channels:
58     - hijack
59     - newprefix
60     - visibility
61     - path
62     - misconfiguration
63     - rpki
64   params:
65     persistAlertData: false
66     alertDataDirectory: alertdata/
67
68 # - file: reportEmail
69 #   channels:
70 #     - hijack
71 #     - newprefix
72 #     - visibility
73 #     - path
74 #     - misconfiguration
75 #     - rpki
76 #   params:
77 #     showPaths: 5 # Amount of AS_PATHs to report in the alert
78 #     senderEmail: bgpalerter@xxxx
79 #     # BGPalerter uses nodemailer.
80 #     # The smtp section can be configured with all the parameters available at https://nodemailer.com/smtp/
81 #     # the following are just the most useful one
82 #     smtp:
83 #       host: localhost
84 #       port: 25
85 #       secure: false # If true the connection will use TLS when connecting to server. If false it will be still possible doing connection upgrade via STARTTLS
86 #       ignoreTLS: false # If true TLS will be completely disabled, including STARTTLS. Set this to true if you see certificate errors in the logs.
87 #       auth:
88 #         user: username
89 #         pass: password
90 #         type: login
91 #       tls:
92 #         rejectUnauthorized: true # Reject unauthorized certificates
93 #     notifiedEmails:
94 #       default:
95 #         - joe@example.org
96 #         - noc@example.org
97
98 # - file: reportSlack
99 #   channels:
100 #     - hijack
101 #     - newprefix
```



```
216 #####
217 # Notification settings:
218 # - notificationIntervalSeconds
219 #     Defines the amount of seconds after which an alert can be repeated. An alert is repeated only if the event that
220 #     triggered it is not yet solved.
221 # - persistStatus
222 #     Persist the status of BGPalerter. If the process is restarted, the list of alerts already sent is recovered
223 #     and they are not repeated. The process must be able to write on disc, this option will create a file inside .cache/
224
225 notificationIntervalSeconds: 14400
226 persistStatus: true
227
228 logging:
229   directory: logs
230   logRotatePattern: YYYY-MM-DD
231   backlogSize: 1000 #Advanced option, read the doc
232   maxRetainedFiles: 10
233   maxFileSizeMB: 15
234   compressOnRotation: false
235
236 checkForUpdatesAtBoot: true
237
238 #####
239 # Process monitoring settings:
240 # Uncomment or add classes under processMonitors if you want to monitor or send logs about the status of the BGPalerter process
241
242 #processMonitors:
243 # - file: uptimeApi
244 #   params:
245 #     useStatusCodes: true
246 #     host: null
247 #     port: 8011
248 #
249 # - file: uptimeHealthcheck
250 #   params:
251 #     url: url_to_poll
252 #     intervalSeconds: 300
253 #     method: get
254 #
255 # - file: sentryModule
256 #   params:
257 #     dsn: https://<key>@sentry.io/<project>
```

```
217 #####
218 # Notification settings:
219 # - notificationIntervalSeconds
220 #   Defines the amount of seconds after which an alert can be repeated. An alert is repeated only if the event that
221 #   triggered it is not yet solved.
222 # - persistStatus
223 #   Persist the status of BGPalerter. If the process is restarted, the list of alerts already sent is recovered
224 #   and they are not repeated. The process must be able to write on disc, this option will create a file inside .cache/
225
226 notificationIntervalSeconds: 14400
227 persistStatus: true
228
229 logging:
230   directory: logs
231   logRotatePattern: YYYY-MM-DD
232   backlogSize: 1000 #Advanced option, read the doc
233   maxRetainedFiles: 10
234   maxFileSizeMB: 15
235   compressOnRotation: false
236
237 checkForUpdatesAtBoot: true
238
239 #####
240 # Process monitoring settings:
241 # Uncomment or add classes under processMonitors if you want to monitor or send logs about the status of the BGPalerter process
242
243 processMonitors:
244   - file: uptimeApi
245     params:
246       useStatusCodes: true
247       host: null
248       port: 8011
249
250   # - file: uptimeHealthcheck
251   #   params:
252   #     url: url_to_poll
253   #     intervalSeconds: 300
254   #     method: get
255
256   # - file: sentryModule
257   #   params:
258   #     dsn: https://<key>@sentry.io/<project>
259
```

```
{
  "warning": false,
  "connectors": [
    {
      "name": "ConnectorRIS",
      "connected": true
    }
  ]
}
```



Supporting RPKI deployment

```
15 monitors:
16   - file: monitorHijack
17     channel: hijack
18     name: basic-hijack-detection
19     params:
20       thresholdMinPeers: 2
21
22   - file: monitorNewPrefix
23     channel: newprefix
24     name: prefix-detection
25     params:
26       thresholdMinPeers: 2
27
28   - file: monitorPath
29     channel: path
30     name: path-matching
31     params:
32       thresholdMinPeers: 0
33
34   - file: monitorVisibility
35     channel: visibility
36     name: withdrawal-detection
37     params:
38       thresholdMinPeers: 20
39
40   - file: monitorAS
41     channel: misconfiguration
42     name: asn-monitor
43     params:
44       thresholdMinPeers: 2
45
46   - file: monitorRPKI
47     channel: rpki
48     name: rpki-monitor
49     params:
50       vrpProvider: ntt
51       thresholdMinPeers: 1
52       checkUncovered: false
53       preCacheROAs: true
54       refreshVrpListMinutes: 15
55
```

Generate your VRPs JSON file



- Using external VRPs list is quick and easy, but you are essentially trusting somebody else writing such VRPs correctly
- You can generate your JSON file periodically and BGPalerter will load it

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

rpki-client




```
15 monitors:
16   - file: monitorHijack
17     channel: hijack
18     name: basic-hijack-detection
19     params:
20       thresholdMinPeers: 2
21
22   - file: monitorNewPrefix
23     channel: newprefix
24     name: prefix-detection
25     params:
26       thresholdMinPeers: 2
27
28   - file: monitorPath
29     channel: path
30     name: path-matching
31     params:
32       thresholdMinPeers: 0
33
34   - file: monitorVisibility
35     channel: visibility
36     name: withdrawal-detection
37     params:
38       thresholdMinPeers: 20
39
40   - file: monitorAS
41     channel: misconfiguration
42     name: asn-monitor
43     params:
44       thresholdMinPeers: 2
45
46   - file: monitorRPKI
47     channel: rpki
48     name: rpki-monitor
49     params:
50     vrpFile: test/vrps.json
51     thresholdMinPeers: 1
52     checkUncovered: false
53     preCacheROAs: true
54     refreshVrpListMinutes: 15
55
```

Fake VRPs JSON file?



- You can use BGPalerter to do some tests before to deploying RPKI
- You can add in vrps.json some ROA that you plan to sign but you didn't yet
- You can leave it running and check if any of your announcements are going to be RPKI invalid and if you organization is able to stick to the “signed” ROAs

Contribute!



- Source code on GitHub
 - <https://github.com/nttgin/BGPalerter>

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