BGPalerter

Real-time BGP monitoring

Massimo Candela

Senior Software Engineer - Network Information Systems Development

massimo@ntt.net

BGPalerter

BGPalerter is a tool for analyzing streams of eBGP data

- We developed it for monitoring NTT prefixes
  - hijacks, visibility loss, unexpected changes of configuration
- 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

Example

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The prefix 165.254.225.0/24 (description 1) has been withdrawn.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

visibility
The prefix 2a00:5884::/32 (alarig fix test) has been withdrawn. It is no longer visible from 4 peers.

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

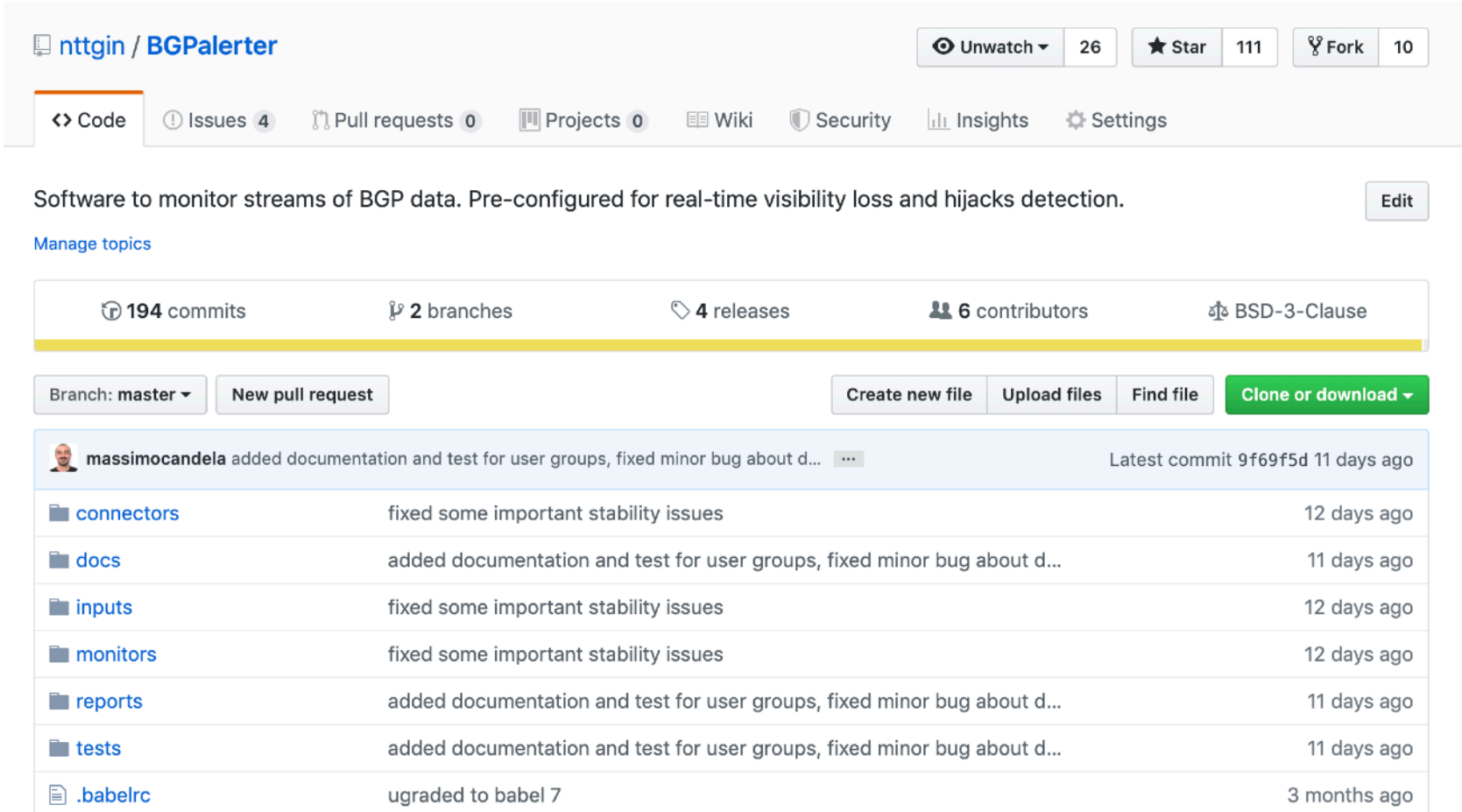
hijack
A new prefix 2a00:5884:ffff:/48 is announced by AS208585. It should be instead 2a00:5884::/32 (alarig fix test) announced by AS204092, and AS45

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).

Setup

Setup


nttgin / BGPalerter
Unwatch 26
Star 111
Fork 10
Code
Issues 4
Pull requests 0
Projects 0
Wiki
Security
Insights
Settings
Software to monitor streams of BGP data. Pre-configured for real-time visibility loss and hijacks detection.
Edit
Manage topics
194 commits
2 branches
4 releases
6 contributors
BSD-3-Clause
Branch: master
New pull request
Create new file
Upload files
Find file
Clone or download
massimocandela added documentation and test for user groups, fixed minor bug about d...
Latest commit 9f69f5d 11 days ago
connectors fixed some important stability issues 12 days ago
docs added documentation and test for user groups, fixed minor bug about d... 11 days ago
inputs fixed some important stability issues 12 days ago
monitors fixed some important stability issues 12 days ago
reports added documentation and test for user groups, fixed minor bug about d... 11 days ago
tests added documentation and test for user groups, fixed minor bug about d... 11 days ago
.babelrc ugraded to babel 7 3 months ago

Setup

Releases | Tags

Draft a new release

Latest release

v1.20.1

0be673a

v1.20.1

Edit

 **massimocandela** released this 12 days ago · 3 commits to master since this release

[minor]

- Fixed some stability issues when RIPEstat APIs are not reachable when generating prefix lists
- Fixed stability issue of monitorPath
- Fixed bug missing some prefixes on re-connect to RIS stream (e.g. on 1006 error)
- Fixed rare crash case when BGP updates arrive malformed

▼ Assets 4

bgpalerter-linux-x64	62.7 MB
bgpalerter-macos-x64	62.9 MB
Source code (zip)	

Setup

```
wget https://github.com/nttgin/BGPalerter/releases/download/v1.20.0/bgpalerter-linux-x64

chmod 700 bgpalerter-linux-x64
```

Generate prefixes list

```
./bgpalerter-linux-x64 generate -a YOUR_AS -o prefixes.yml
```

- You can provide multiple Autonomous Systems
- You will receive a warning if some of the announced prefixes don’t have ROAs
    - Check the output file by hand

Monitored prefixes

```
165.254.225.0/24:
  description: Job
  asn: 15562
  ignoreMorespecifics: false
  ignore: false

165.254.255.0/24:
  description: Job
  asn: 15562
  ignoreMorespecifics: false
  ignore: false

192.147.168.0/24:
  description: Job
  asn: 15562
  ignoreMorespecifics: false
  ignore: false
```

Run!

```
./bgpalerter-linux-x64
```

```
BGPalerter, version: 1.20.1 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
```

Components

Connectors

Monitors

Reports

- Connectors connect to the data sources
- Monitors filter and analyse the data. Alerts are generated
- Reports compact/throttle the alerts and deliver them

config.yml

```yaml
monitors:
  - file: monitorHijack
    channel: hijack
    name: basic-hijack-detection
    params:
      thresholdMinPeers: 2

  - file: monitorNewPrefix
    channel: newprefix
    name: prefix-detection
    params:
      thresholdMinPeers: 2

  - file: monitorVisibility
    channel: visibility
    name: withdrawal-detection
    params:
      thresholdMinPeers: 10

reports:
  - file: reportFile
    channels:
      - hijack
      - newprefix
      - visibility
      - path
```

Connectors

- Connectors connect to data sources
- The first implemented connects to RIPE RIS Live
  - **Which is real-time, free, and has 600+ peers worldwide**
  - We don’t parse MRT dumps, we get the streaming through WebSockets

Want to peer?

https://ris.ripe.net

Reports

- Alerts are automatically bundled/throttled
- Can be delivered by email, slack, file, whatever
  - Users groups allow to deliver alerts about specific resources, or about specific types of issue, to specific set of users/targets
- Can be delivered to another monitoring system or database
  - Including the BGP messages that triggered the alert

Report on file

```
massimo@bgpalerter:~$ tail -f logs/reports-2019-09-22.log
2019-09-22T00:47:21.681Z [production] verbose: A new prefix 1.22.84.0/24 is announced by AS45528. It should be instead
2019-09-22T00:47:21.681Z [production] verbose: A new prefix 1.22.72.0/23 is announced by AS45528. It should be instead
2019-09-22T00:47:21.681Z [production] verbose: A new prefix 1.22.84.0/22 is announced by AS45528. It should be instead
2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.72.0/24 is announced by AS45528. It should be instead
2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.94.0/23 is announced by AS45528. It should be instead
2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.83.0/24 is announced by AS45528. It should be instead
2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.85.0/24 is announced by AS45528. It should be instead
2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.86.0/24 is announced by AS45528. It should be instead
2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.88.0/24 is announced by AS45528. It should be instead
2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.87.0/24 is announced by AS45528. It should be instead
```

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
```

Report on Slack

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

visibility
The prefix 2a00:5884::/32 (alarig fix test) has been withdrawn. It is no longer visible from 4 peers.

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).

Monitored prefixes

```
165.254.255.0/24:
  description: Rome peering
  asn: 2914
  ignoreMorespecifics: false
  ignore: false,
  group: aGroupName,
  excludeMonitors:
    - withdrawal-detection
  path:
    match: ".*2194,1234$"
    notMatch: ".*5054.*"
    matchDescription: detected scrubbing center
    maxLength: 20
    minLength: 4
```

For researchers?

- BGPalerter can analyse big amounts of BGP data without abusing of your CPU
- You can code your monitor class for the features you want to study
  - Follow the code!
  - More info in the docs
- You can code your report class to store the results/data somewhere

BGPalerter + RPKI (experiment)

- A sort of RPKI observatory/registry
- BGPalerter parses **all** BGP updates from all collectors and peers
  - Listening for 0.0.0.0/0 and ::/0
- Each prefix, AS pair is sent to Cloudflare* for RPKI validation

- 5.000+ BGP messages are analysed and validated per second!
- On average 5 routes/second are invalid

*Thanks to Louis Poinsignon and Vasco Asturiano for the -**fast-** Cloudflare RPKI validator

BGPalerter + RPKI (experiment)

Logs about invalid routes are dumped on files

- https://massimocandela.com/bgpalerter/dumps/rpki/
- Constantly appended to the file with the current date

```
The route 194.36.86.0/24 announced by AS42724 is not RPKI valid. Accepted with AS path: [37239,37468,1299,3356,9121,9121,43260,42724]
The route 103.135.208.0/24 announced by AS138454 is not RPKI valid. Accepted with AS path: [37680,6939,1299,6453,58717,134382,134382,13845
The route 185.188.114.0/24 announced by AS42163 is not RPKI valid. Accepted with AS path: [16735,3356,29049,49666,12880,202251,49100,48309
The route 185.188.115.0/24 announced by AS42163 is not RPKI valid. Accepted with AS path: [16735,3356,29049,49666,12880,202251,49100,48309
The route 185.188.112.0/24 announced by AS42163 is not RPKI valid. Accepted with AS path: [16735,3356,29049,49666,12880,202251,49100,48309
The route 185.188.113.0/24 announced by AS29577 is not RPKI valid. Accepted with AS path: [16735,3356,29049,49666,12880,202251,49100,48309
The route 188.253.0.0/24 announced by AS61362 is not RPKI valid. Accepted with AS path: [16735,3356,29049,49666,12880,202251,49100,41881,5
The route 45.142.247.0/24 announced by AS58313 is not RPKI valid. Accepted with AS path: [16735,3356,62240,62240,57695,58313]
The route 45.142.246.0/24 announced by AS58313 is not RPKI valid. Accepted with AS path: [16735,3356,62240,62240,57695,58313]
The route 202.128.108.0/24 announced by AS9583 is not RPKI valid. Accepted with AS path: [16735,3257,9583]
The route 103.52.88.0/24 announced by AS4638 is not RPKI valid. Accepted with AS path: [16735,3356,7473,7474,45349,4638]
The route 103.52.90.0/24 announced by AS4638 is not RPKI valid. Accepted with AS path: [16735,3356,7473,7474,45349,4638]
The route 103.52.89.0/24 announced by AS4638 is not RPKI valid. Accepted with AS path: [16735,3356,7473,7474,45349,4638]
The route 60.198.140.0/24 announced by AS136782 is not RPKI valid. Accepted with AS path: [16735,3257,17676,38638,136782]
The route 31.210.148.0/24 announced by AS394923 is not RPKI valid. Accepted with AS path: [37680,6939,34309,394923]
The route 31.210.149.0/24 announced by AS394923 is not RPKI valid. Accepted with AS path: [37680,6939,34309,394923]
The route 181.13.56.0/23 announced by AS52436 is not RPKI valid. Accepted with AS path: [327960,327782,37100,174,3356,3549,52361,52436]
```

Contribute!

- Source code on GitHub
  - https://github.com/nttgin/BGPalerter
- Thanks to:
  - Job Snijders
  - RIPE RIS (in particular Christopher Amin)

Massimo Candela
Senior Software Engineer
Network Information Systems Development
massimo@ntt.net

www.gin.ntt.net
@GinNTTnet #globalipnetwork #AS2914