



# Monitorare BGP in modo semplice

**Massimo Candela**

Senior Software Engineer - Network Information Systems Development

[massimo@ntt.net](mailto:massimo@ntt.net)

# Eccomi!



Massimo Candela  
Senior Software Engineer  
NTT  
[massimo@ntt.net](mailto:massimo@ntt.net)



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
  - No data collection needed
  - Zero dependencies

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

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

# Requirements



- Nothing, just a laptop with any of: Linux, Mac, Windows
- We will use the binary so you don't need to install any dependency



# Example of BGPalerter notification

## 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The prefix 165.254.225.0/24 (description 1) has been withdrawn.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The prefix 2a00:5884::/32 (alarig fix test) has been withdrawn.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 ▾

27

★ Star

196

Fork

23

<> Code

Issues 5

Pull requests 1

Actions

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

554 commits

2 branches

0 packages

9 releases

11 contributors

BSD-3-Clause

Branch: master ▾

New pull request

Create new file

Upload files

Find file

Clone or download ▾



massimocandela Update README.md

Latest commit e37501a 16 days ago

📁 .github	Update stale.yml	21 days ago
📁 docs	Update configuration.md	18 days ago
📁 src	minor change to error text	21 days ago
📁 tests	fixed ignoreMorespecifics match error for monitorAS	21 days ago
📄 .babelrc	upgraded to babel 7	7 months ago
📄 .eslintrc.json	added mocha support for esling	4 months ago
📄 .gitignore	added alertdata to gitignore	23 days ago
📄 .hound.yml	Update .hound.yml	4 months ago
📄 .travis.yml	introduce travis ci	6 months ago

Latest release

v1.24.0

3b23a90

Compare

Edit

## v1.24.0



massimocandela released this 9 days ago - [1 commit](#) to dev since this release




### [features]

- Introduced research environment, which removes some constraints enforced in production in order to allow experimental analysis
- Introduced auto configuration wizard
- Introduced Webex support (thanks Alan Haynes)

### [minor]

- Updated dependencies
- Deprecation of resource\_templates in favour of resourceTemplates in config.yml
- Fixed generate prefixes option -s
- Download default configuration from Git repo (which includes commented options), generate it locally only if the download fails

### Assets 5

 <a href="#">bgpalerter-linux-x64</a>	60.4 MB
 <a href="#">bgpalerter-macos-x64</a>	58.7 MB
 <a href="#">bgpalerter-win-x64.exe</a>	57.4 MB

# Setup

- Download and run. That's all.

```
wget https://github.com/nttgin/BGPalerter/releases/download/v1.24.0/bgpalerter-linux-x64
```

```
chmod 700 bgpalerter-linux-x64
```

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

# Setup - auto-configuration



```
BGPalerter, version: 1.24.0 environment: production
```

```
Loaded config: /Users/massimocandela/Documents/work/BGPalerter/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
```

```
? Are there sub-prefixes delegated to other ASes? (e.g. sub-prefixes announced by customers) Yes
```

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

# Run!



```
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
```



# 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
```

# Explanation of prefixes.yml

```
165.254.255.0/24:  
  description: Rome peering  
  asn: 2914  
  ignoreMorespecifics: false  
  ignore: false  
  group: aUserGroup  
  excludeMonitors:  
    - withdrawal-detection  
  path:  
    match: ".*2194,1234$"  
    notMatch: ".*5054.*"  
    matchDescription: detected scrubbing center  
    maxLength: 128  
    minLength: 2
```

# 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

```
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>



- Alerts are automatically bundled/throttled
- At the moment alerts can be delivered to:
  - Files
  - Email
  - Slack
  - Alerta dashboard
  - Kafka
  - Syslog
  - Webex
- 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>

# 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).

# A Dashboard for BGPalerter



The screenshot shows the BGPalerter dashboard interface. At the top, there's a navigation bar with the 'alerta' logo, tabs for 'Recent', 'Top 10', and 'Watch', and links for 'Configuration', 'Jane Bloggs', and 'About'. Below this is a search bar with 'Service' and 'error' entered, and a dropdown menu set to 'Open'. A blue 'Auto Update' button is on the right. Below the search bar are filters for 'ALL 133', 'Infrastructure 44', 'Production 43', and 'Development 46'. The main area is a table of alerts with columns for Severity, Status, Last Receive Time, Dupl., Environment, Service, Resource, Event, Value, and Text. The table contains 14 rows of alerts, with the first two being 'Critical' and the rest ranging from 'Major' to 'Indeterminate'. A footer bar at the bottom indicates 'Showing 14 out of 14 alerts'.

Severity	Status	Last Receive Time	Dupl.	Environment	Service	Resource	Event	Value	Text
Critical	Open	Fri 16 Oct 00:55	0	Production	Tornskel	Ockey	breachOfConfidentiality	n/a	Marfa Godard Banksy voluptate cred, Cray gastrop
Critical	Open	Fri 16 Oct 00:40	0	Production	Notestack	Extremes	inputOutputDeviceError	n/a	Aesthetic chia biodiesel, shabby chic Brooklyn Mar
Major	Open	Fri 16 Oct 00:56	0	Production	Deployinator	kue	dataSetOrModemError	n/a	Nihil crucifix tousled, shabby chic cardigan et me
Major	Open	Fri 16 Oct 00:40	0	Production	Support	stylebot	fileError	n/a	Commodo roof party gluten-free placeat. Forage qu
Major	Open	Fri 16 Oct 00:39	0	Production	Macto	jslint.vim	cableTamper	n/a	Hella squid dolor readymade Banksy, master cleans
Minor	Open	Fri 16 Oct 00:55	0	Production	Firetray	spline.contacts	lanError	n/a	Laboris gastropub artisan occaecat, tattooed VHS
Minor	Open	Fri 16 Oct 00:39	0	Production	Phnx	cssSandpaper	communicationsProtocolError	n/a	Church-key veniam commodo, put a bird on it try-ha
Warning	Open	Fri 16 Oct 00:55	0	Production	Friar	PxLoader	communicationsSubsystemFailure	n/a	Odio minim laborum, cupidatat Shoreditch biodiese
Warning	Open	Fri 16 Oct 00:55	0	Production	Yschool	bbb	adapterError	n/a	Sustainable PBR cardigan Brooklyn, listicle elit o
Indeterminate	Open	Fri 16 Oct 00:56	0	Production	Jscnfus	webglreport	adapterError	n/a	Neutra vegan tilde, proident keytar swag dreamcatc
Indeterminate	Open	Fri 16 Oct 00:55	0	Production	Photoswipe	RealTimeMonitor	dteDceInterfaceError	n/a	Roof party listicle cillum, enim Tumblr DIY artisa
Indeterminate	Open	Fri 16 Oct 00:55	0	Production	Wireit	currency.io	configurationOrCustomizationError	n/a	Biodiesel labore 8-bit, odio eu American Apparel
Indeterminate	Open	Fri 16 Oct 00:55	0	Production	Zia	openstreetbugs	proceduralError	n/a	Sustainable selvage slow-carb brunch bespoke odio
Indeterminate	Open	Fri 16 Oct 00:55	0	Production	Nodelint	LightFace	ouputDeviceError	n/a	Meh qui brunch, twee mixtape Shoreditch dolor Pi

# Summary

- Monitor hijacks and visibility loss
- Monitor more specifics you were not supposed to announce
- Monitor whatever your AS is announcing
- Detect AS\_Paths with(out) specific conditions
- Log BGP messages (e.g. 'persistAlertData')
- Auto configuration
- Monitor process status/uptime (api, heartbeat)
- Run source, binary, or docker



# Contribute!



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

The background of the slide features a series of vertical panels in various colors (red, orange, yellow, green, cyan, blue) that create a vibrant, multi-colored backdrop. In front of these panels, the silhouettes of several people are visible, some walking and some standing in pairs, suggesting a busy office or public space environment.

# Questions?

## **Massimo Candela**

Senior Software Engineer  
Network Information Systems Development

[massimo@ntt.net](mailto:massimo@ntt.net)

[www.gin.ntt.net](http://www.gin.ntt.net)

@GinNTTnet #globalipnetwork #AS2914