

### **Eccomi!**



Massimo Candela Senior Software Engineer NTT

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
  - No data collection needed
  - Zero dependencies

### **Motivations**



- 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

### **Motivations**



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The prefix 165.254.225.0/24 (description 1) has been withdrawn.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The prefix 2a00:5884::/32 (alarig fix test) has been withdrawn.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

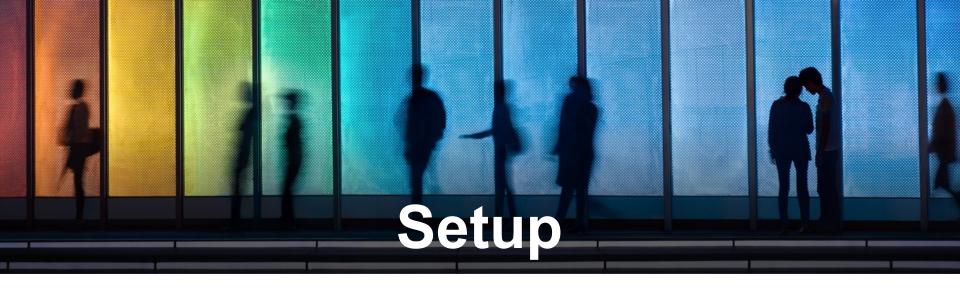
A new prefix 2a00:5884:ffff:/48 is announced by AS208585. It should be instead 2a00:5884::/32 (alarig fix test) announced by AS204092, and AS45

#### hijack

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

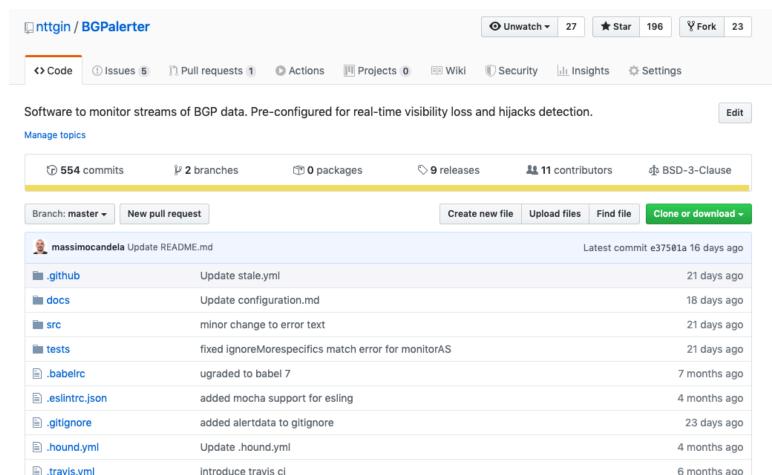
#### newprefix

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



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



# 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 1.22.72.0/24 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 1.23.88.0/24 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 1.23.88.0/24 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

# config.yml



```
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
- 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: <a href="https://stat.ripe.net/widget">https://stat.ripe.net/widget</a>

/bqplay#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

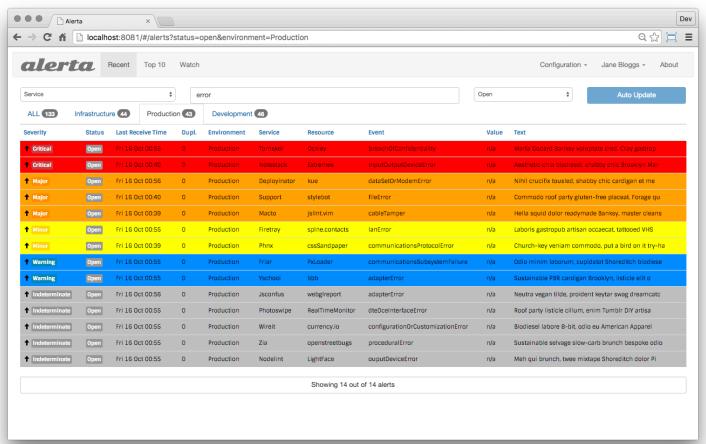
The prefix 2a00:5884::/32 (alarig fix test) is announced by AS15563 instead of AS204092, and AS45

#### 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





## **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
  - <a href="https://github.com/nttgin/BGPalerter">https://github.com/nttgin/BGPalerter</a>



### Massimo Candela

Senior Software Engineer

Network Information Systems Development

massimo@ntt.net

www.gin.ntt.net

@GinNTTnet #globalipnetwork #AS2914