2022
TECHNOLOGY
exchange

BGPalerter
Monitoring your BGP Prefixes

Ryan Harden
Senior Cyberinfrastructure Security Architect
Internet2 - Network Services

INTERNET2

What is BGPalerter?

- Simple tool to monitor your routing assets
- Uses Public BGP data repositories (Like RIPE RIS)
- Super easy to setup and run
- Free/Open Source Software
- Developed by NTT

https://github.com/nttgin/BGPalerter

Features: Monitoring

- New Prefixes
- More Specifics of Existing Prefixes
- Visibility
    - Expected prefixes no longer visible
- Hijack Detection
    - Prefixes announced by another ASN
- RPKI
    - Expiring ROAs
    - Prefixes not covered by a ROA
    - Changes to ROAs
- AS-PATH Changes
    - Upstream/Downstream Changes

Features: Alerting

- Log to File / Email / Syslog / Kafka
- Slack / Webex / Telegram / Mattermost / MS Teams
- HTTP URL (Push)
- REST API (Pull)
- Pushover

BGPalerter APP 19:17

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The prefix 165.254.225.0/24 (description 1) has been withdrawn.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The prefix 2a00:5884::/32 (alarig fix test) has been withdrawn.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

Customizable Settings
- Only alert once every N minutes/hours

Easy to Deploy

- Download binary
- Edit Config File
- Auto-Generate a prefix file
- Run!

Run from binary, compile from source, use Debian packages, or Docker!
- (Internet2 runs it with Docker, in AWS)

Auto-Generate Prefix file? What do you mean?

- Includes a tool to generate a YAML file from your existing BGP announcements
- ./bgpalerter-linux-x64 generate -a ASN(S) -o OUTPUT_FILE
- Manually verify!

  - Does output match your _intent_?

Things to Consider…

- Monitor DarkNet/Unannounced Space
- Monitor Unused ASNs
- Configuration Hints
    - notificationIntervalSeconds
        - Defines Repeated Alert Intervals
    - persistStatus
        - Keeps log of existing alerts after restart (in concert with above setting)

Future thinking…(Internet2)

- Automated Configuration/Prefixes
  - Auto-Generated is fine, but not necessarily accurate
  - More accurately reflect intent
- Community Instances
  - Connected to/Instantiated by Insight Console

PacketVis

https://packetvis.com/

- Hosted BGPalerter
- Free!
- Check it out!

I2 Routing INTEGRITY

"Each of us protecting all of us"

Ensuring packets arrive at their destinations with no detours, no delays, and no outages

manrs@internet2.edu

INTERNET2

2022 TECHNOLOGY exchangə

Thanks!

Questions?
Find me anytime this week
or email me below.

rharden@internet2.edu