SNAS: Monitoring BGP data

Presentation by: Philippe Davies
Agenda

- A little bit about me
- What are BGP and BMP?
- SNAS introduction
- SNAS system architecture
- SNAS use cases
- History of BGP hijacks
- SNAS demo and alerts
- Next steps for the project
Who am I?

Philippe Davies

• Networking student at Carleton University
  • BIT: Networking program

• Intern at CENGN: Summer 2018
  • Implemented SNAS cluster for Network Analytics

• Contributor to the SNAS project
What is BGP?

• Border Gateway Protocol (RFC1654)
  – Invented in the late 1980s
  – External routing protocol
  – Connects Autonomous Systems (ASes) together

• Connects the entirety of the Internet
  – Primarily used by ISPs and multi homed corporations

• Route advertisements with prefix and AS path
What is BMP?

- BGP Monitoring Protocol (RFC 7854)
- BGP enabled devices forwarding routing data to a centralized location
- Inspection of active and inactive BGP routes
Internet Governance

Internet Assigned Numbers Authority

Regional IR (RIR)

Internet Service Provider

End User
AS and Prefix Validation

• IRR (Internet Routing Registry)
  – Regional database for public routing entries
  – RIRs such as ARIN, RIPE, AFNIC, APNIC, etc..

• RPKI (Resource Public Key Infrastructure)
SNAS introduction

- SNAS (Streaming Network Analytics System)

- Linux Foundation Networking project
  - Created by Tim Evens - Principal Engineer at Cisco

- BMP collector

- BMP data analysis

- Grafana dashboards:
  - Peer analysis
  - Prefix history
  - BGP Security (RPKI/IRR and hijacks/leaks)
  - And many more graphs
SNAS System Architecture

- BMP collector (openbmp)
- Kafka bus (internal messaging)
- TimescaleDB (PostgreSQL)
- Grafana (graphs)
Use cases

• Identifying route leaks
• Identify noisy peers
• Track prefix history
• BGP security analysis
What is a BGP Route Hijack?

- Prefixes being redirected by malicious or unqualified network operators
- Prefix hijacked with more specific route
- Traffic rerouted for theft of information
- Inadvertent leak of country AS restrictions
Example Hijacks

- Youtube Hijack by Pakistan in 2008. [Link]

- Bitcoin mining hijack in 2014. [Link]

- DV-LINK (unknown Russian entity) rerouted traffic in 2017. [Link]

- Rostelecom (Russian telecom) rerouted financial traffic in 2017. [Link]

- China Telecom BGP hijacking from 2010 to 2017. [Link]
Since BGP relies on a transitive trust model, validation between customer and provider is important. In this case, PCCW (3491) did not validate Pakistan Telecom’s (17557) advertisement for 208.65.153.0/24. By accepting this advertisement and re-advertising to its peers and providers, PCCW was propagating the wrong route. Those who saw this route from PCCW selected it since it was a more specific route. YouTube was advertising 208.65.152.0/22 before the event started and the /24 was a smaller (and more specific) advertisement. According to usual BGP route selection process, the /24 was then chosen, effectively completing the hijack.
China Telecom route manipulation

China Telecom BGP hijacking from 2010 to 2017. [Link]
Peer Analysis Demo
Prefix History Demo
RPKI & IRR Demo
Hijack/Leak Demo
Hijack alerts

- Proof of concept applications
  - Identification of hijacks/leaks in real time
  - Available on Gitter. [link]
Future of SNAS

- Add BGPSec support to SNAS
- Increased efficiency in collector scripts
- Private AS notifications
- Hijack/Leak notification (beyond gitter)
OPEN SOURCE NETWORKING DAYS

SNAS