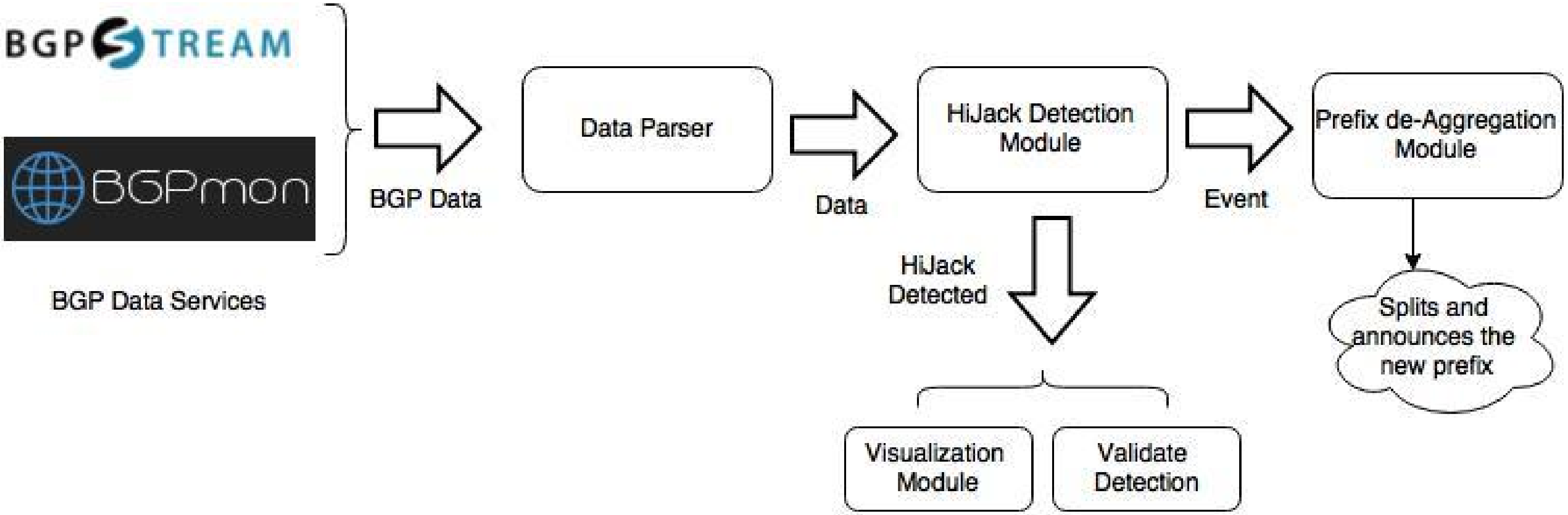
Automated prefix deaggregation as a defense mechanism

Gavriil Chaviaras, Petros Gigis, Andrew Weiner, Mingwei Zhang

Goal:

actively fight the prefix hijackings

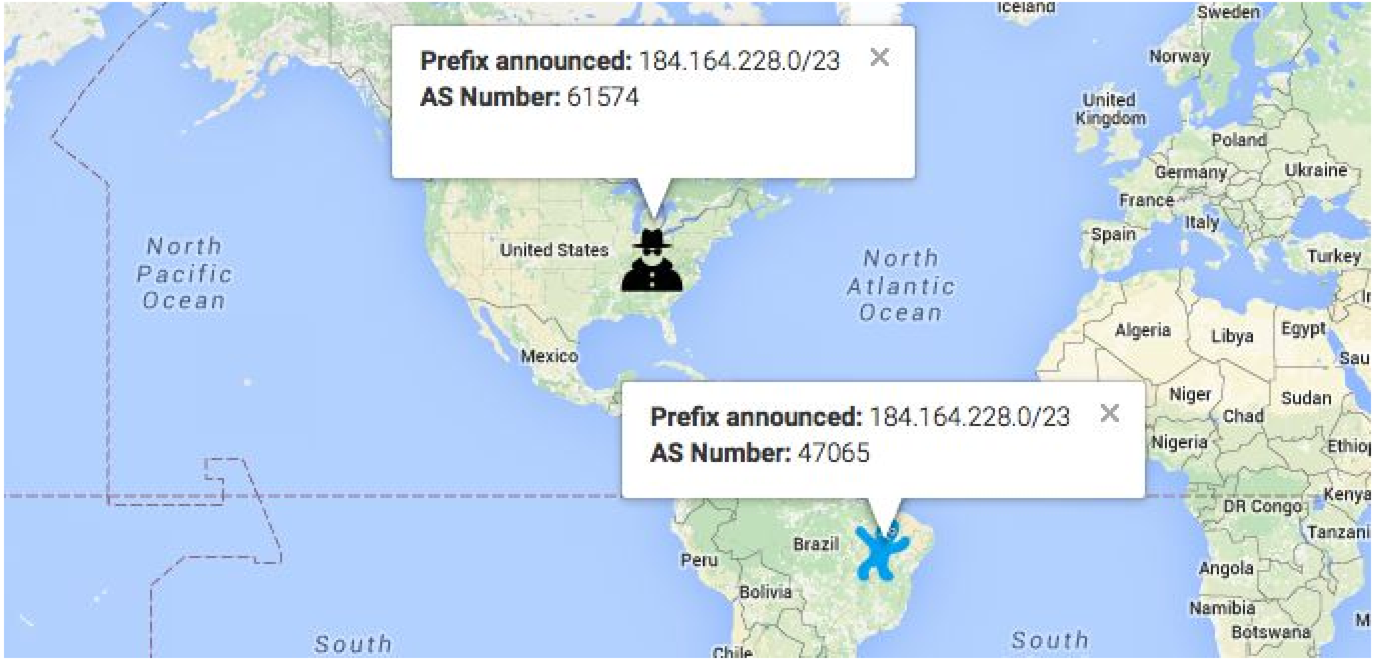
HIJACKS-1 Architecture



What we did

- Taps to detection mechanisms
  - Hijacks-2 Challenge
  - BGPMon
  - BGPStream (BGPReader)
- Detection result validation
  - Control-plane: looking glass (manually), periscope (automatically)
  - Data-plane: traceroutes from and to the victim prefix (automatically)
- Automatic de-aggregation to grab back the traffic
  - Peering testbed
  - Announce sub-prefixes for the victim
  - Monitor the status

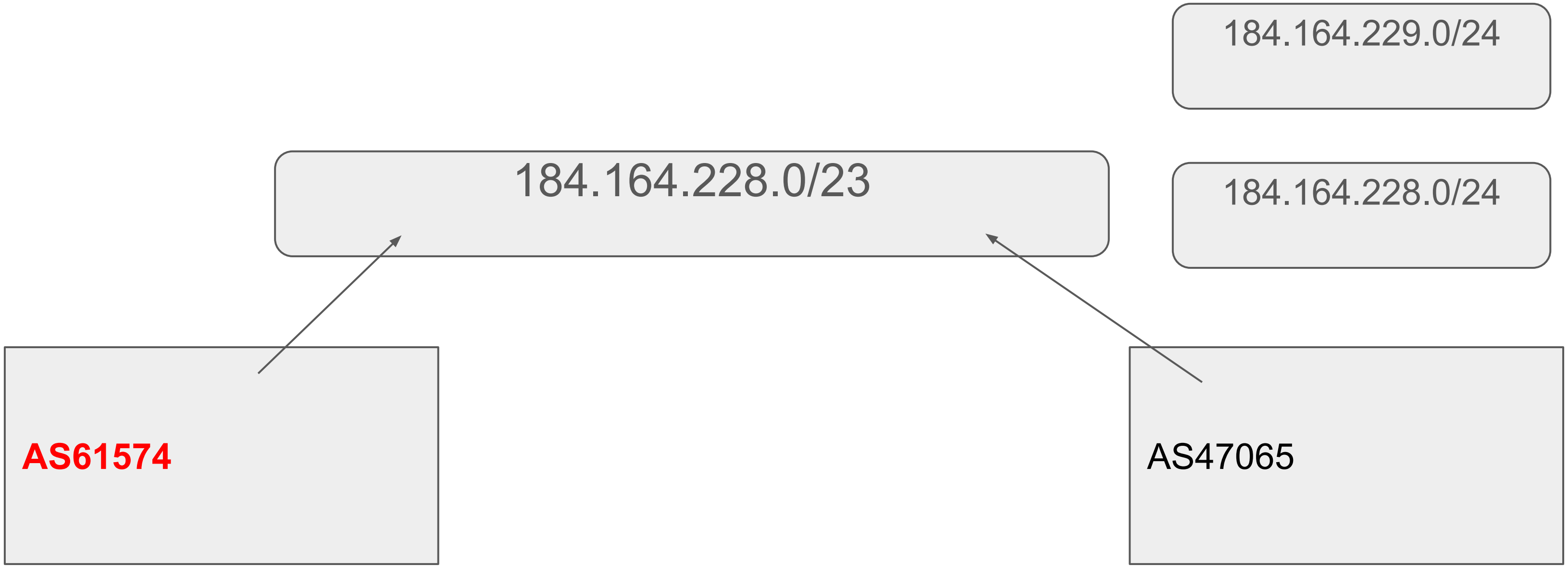
Visualization



Prefix announced: 184.164.228.0/23
AS Number: 61574

Prefix announced: 184.164.228.0/23
AS Number: 47065

Geolocation of victim and attacker using the AS number.



184.164.229.0/24

184.164.228.0/23

184.164.228.0/24

AS61574

AS47065

The Demo - what you will see

Situation: **AS47065** (victim) has announced prefix 184.164.228.0/23. All is well…
We will use Hurricane Electric’s routing table to observe the following events:

Event 1: **AS61574** (hijacker) announces 184.164.228.0/23 (the same prefix)
Observation: A route to **AS61574** appears at Hurricane Electric.

Event 2: **AS47065** is notified of the hijack and announces two /24 prefixes.
(184.164.228.0/24 and 184.164.229.0/24)
Observation: Route to **AS47065** is immediately restored at Hurricane Electric.
REMARKABLE!

The Demo