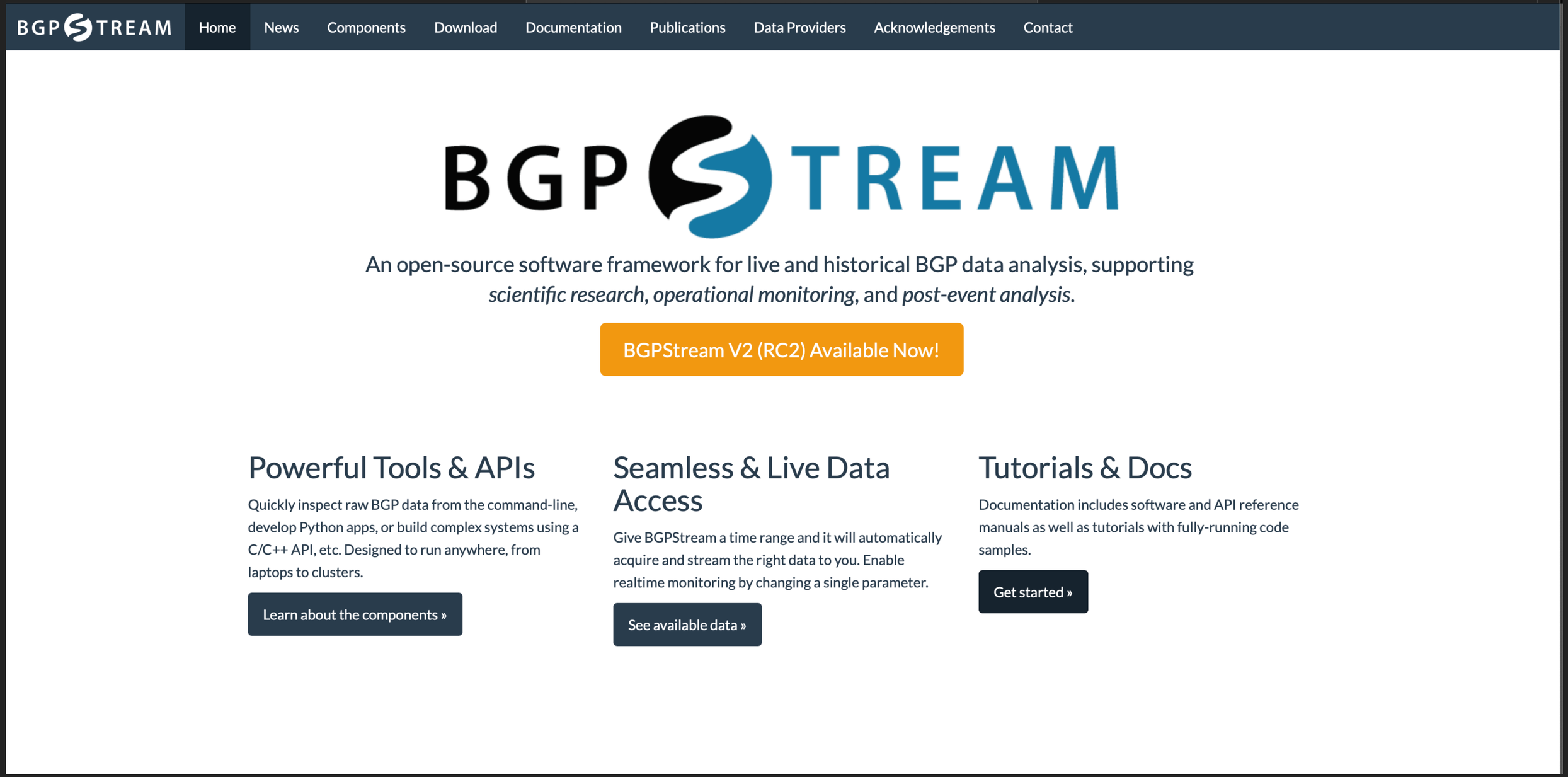


bgpstream.caida.org

CAIDA'S BGP (HIJACKING) OBSERVATORY

Alberto Dainotti
alberto@caida.org

Center for Applied Internet Data Analysis
University of California San Diego

IN COLLABORATION WITH

University of Massachusetts Amherst

UNIVERSITY OF TWENTE.

Consiglio Nazionale delle Ricerche
Istituto di Informatica e Telematica

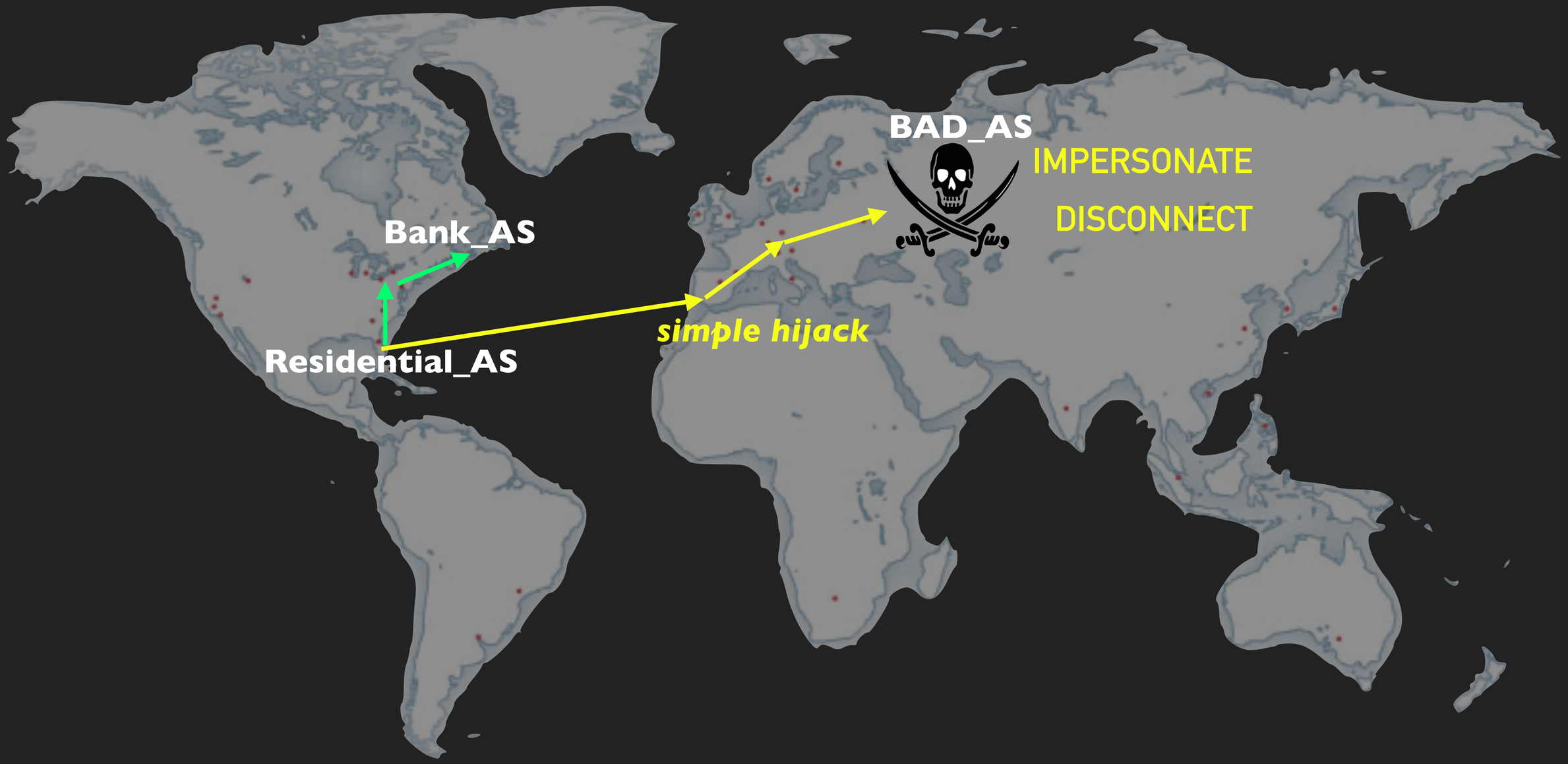
IIJ
Internet Initiative Japan

FORTH
INSTITUTE OF COMPUTER SCIENCE
INternet Security & Privacy Intelligence REsearch Group

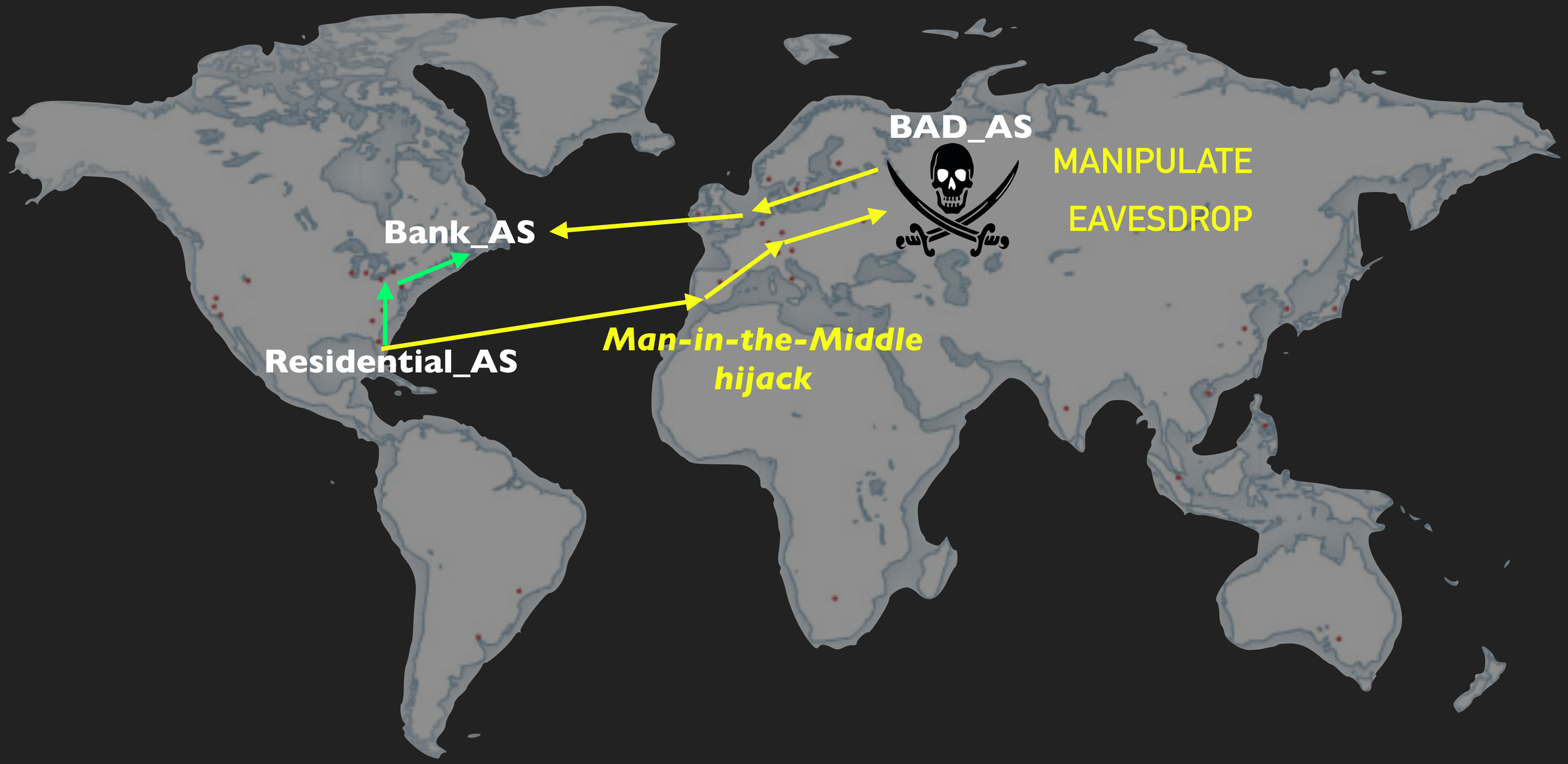
MIT CSAIL

PROBLEM
ROUTE HIJACKING

ATTACKING GLOBAL (BGP) ROUTING



ATTACKING GLOBAL (BGP) ROUTING



Problem

- There is no full solution deployed
- How is Internet global routing abused?
  - characteristics of attacks
    - techniques used
    - scope and significance
    - timing
    - perpetrators and motivation

CAIDA BGP (Hijacking) Observatory

1. Detects suspicious events by monitoring the Internet 24/7
   - including more sophisticated attack types
2. Executes traceroutes on-the-fly during a detected event
   - Provides unique view of data-plane + control-plane
3. Dashboard enables DB queries and provides visualization interfaces

CAIDA BGP (Hijacking) Observatory

- Situational Awareness / Intelligence
- Research on Hijacks and BGP anomalies
- Operators' debug tool
- Testbed for developing new inference methods

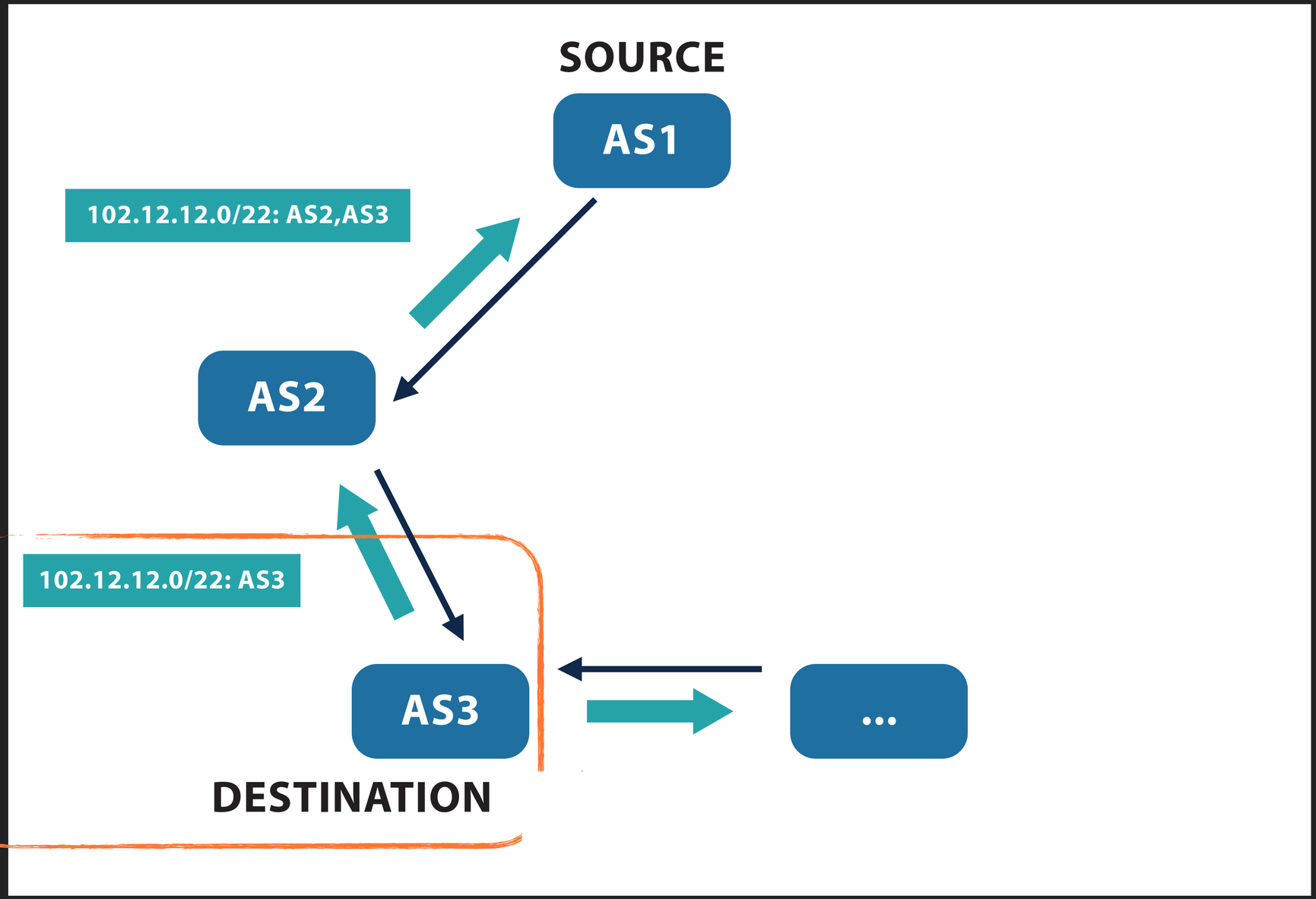
NSF CNS-1423659. Aug 2014 - Jan 2019
HIJACKS - Detecting and Characterizing Internet Traffic Interception based on BGP Hijacking

DHS S&T FA8750-18-2-0049. Dec 2017 - Aug 2020
ASSISTS - Advancing Scientific Study of Internet Security and Topological Stability

ROUTE HIJACKING
ATTACK TECHNIQUES

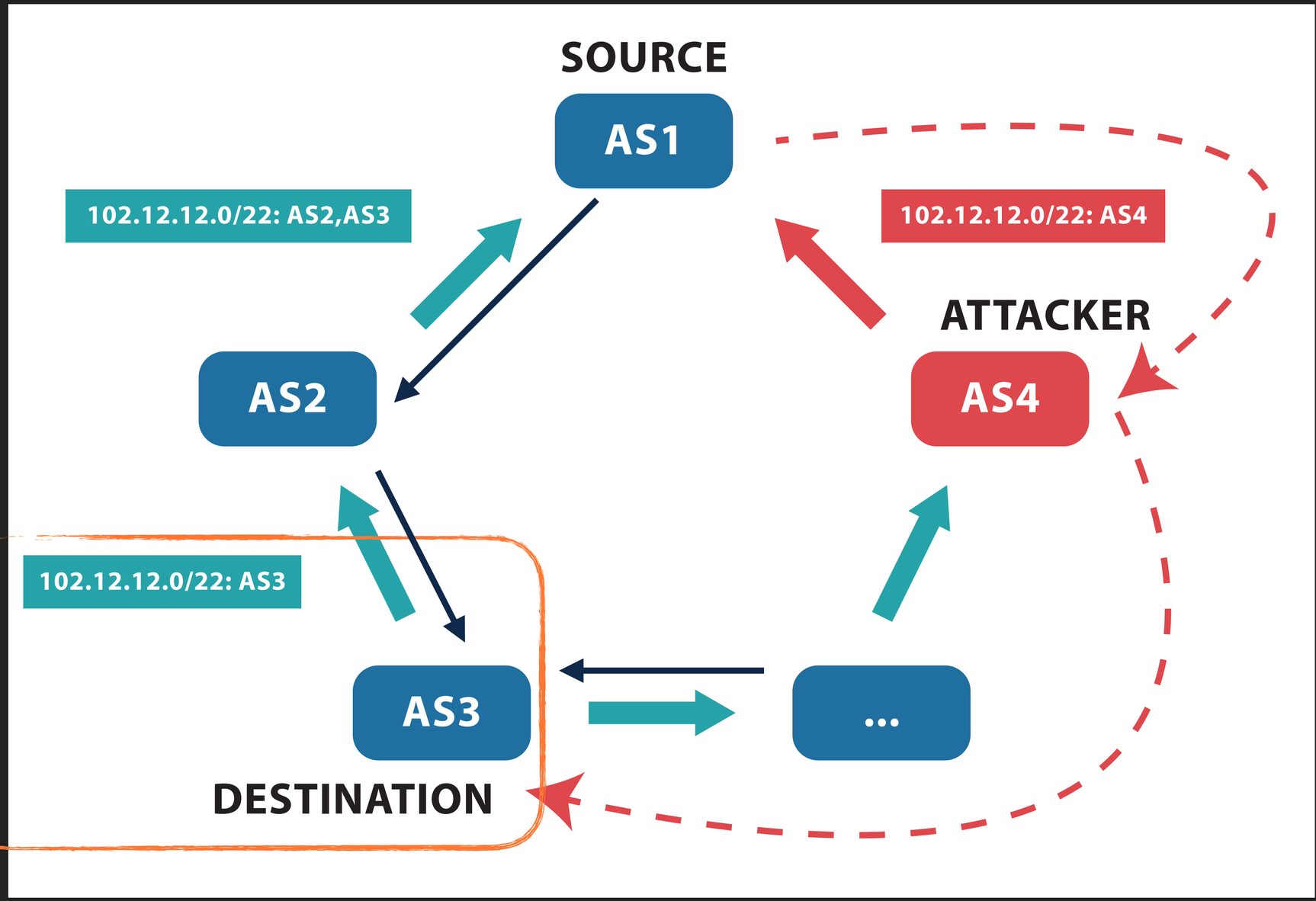
#1
ORIGIN HIJACKS

ORIGIN HIJACKS

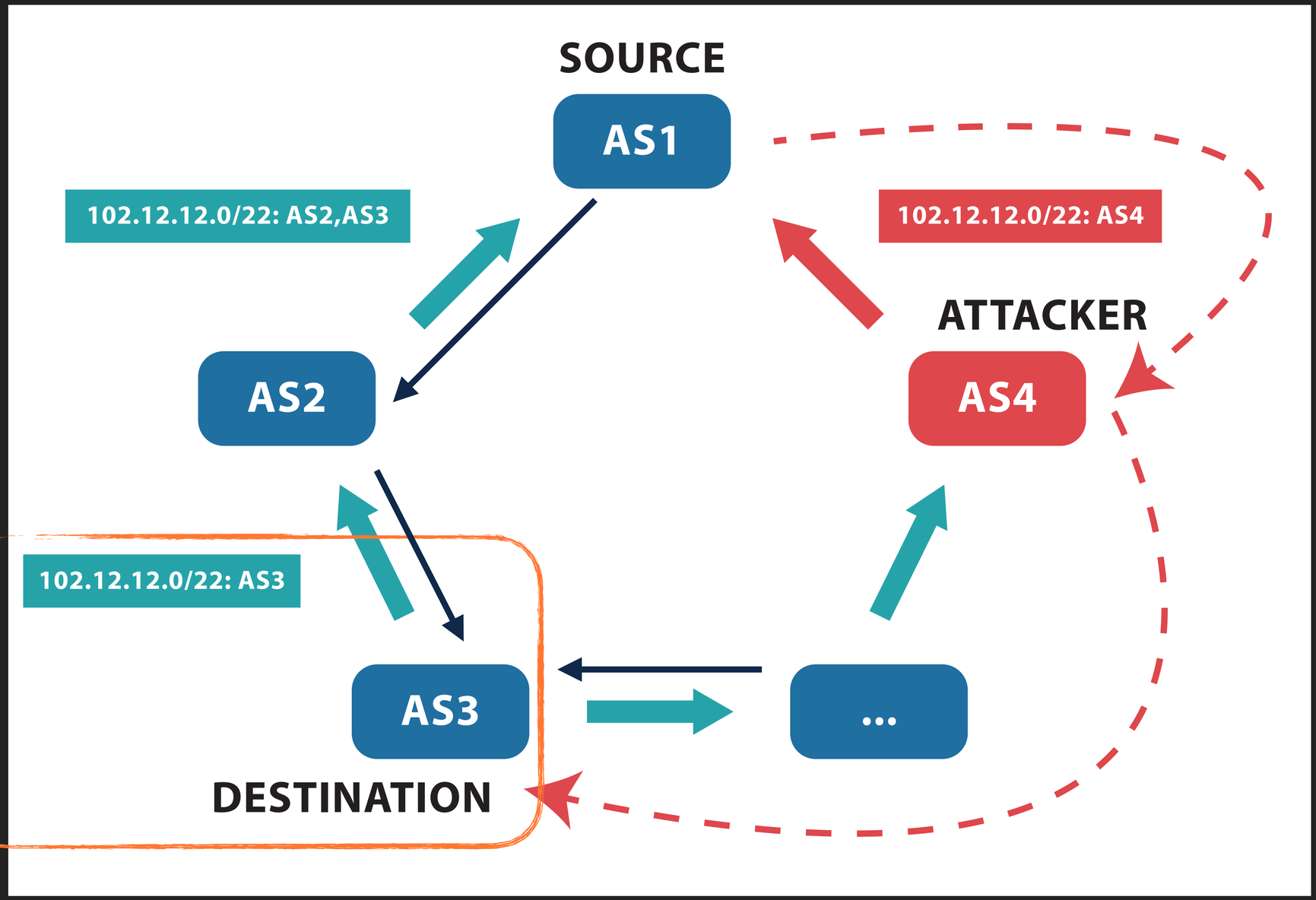


LEGITIMATE ORIGIN

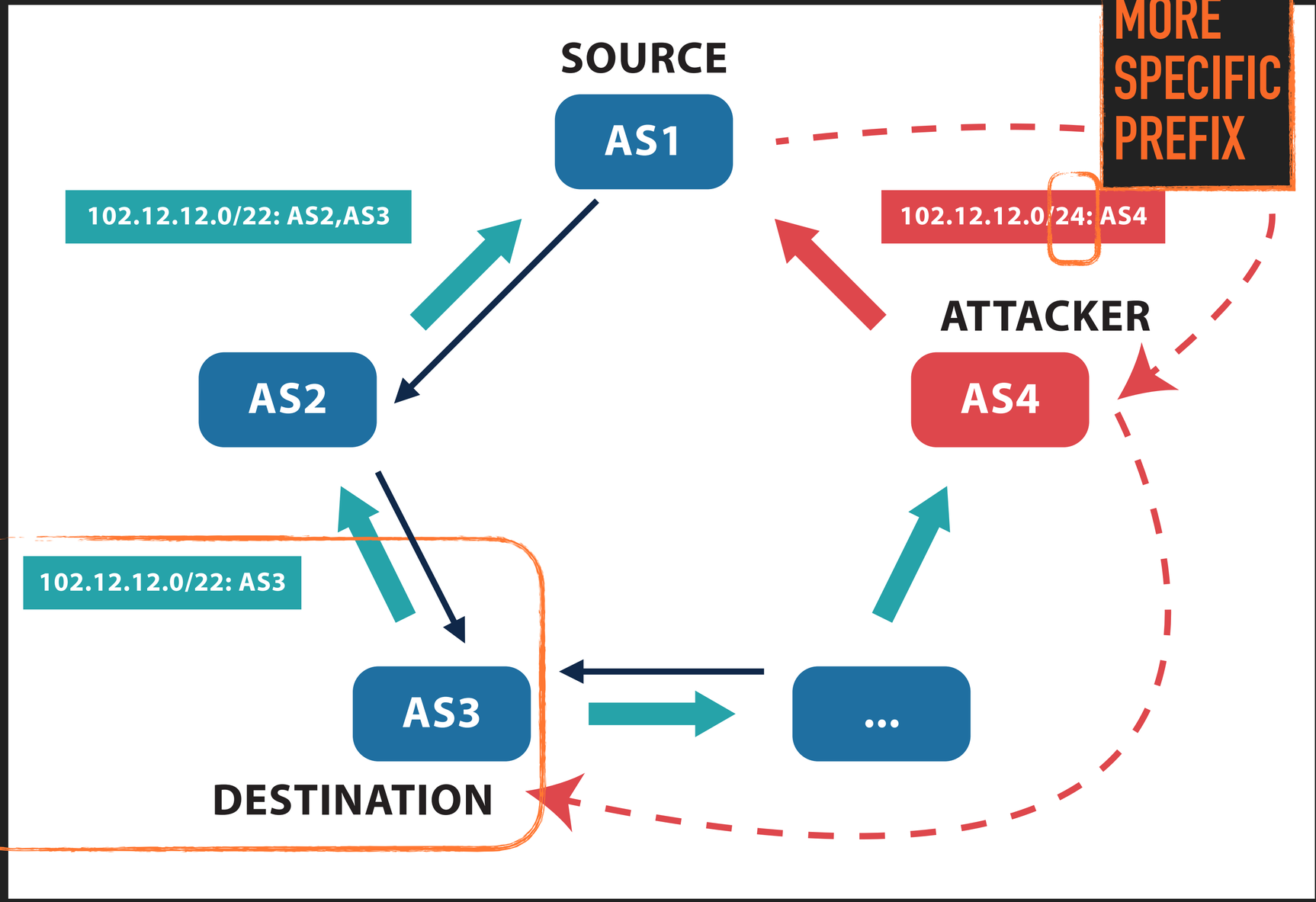
ORIGIN HIJACKS



ORIGIN HIJACKS: MOAS

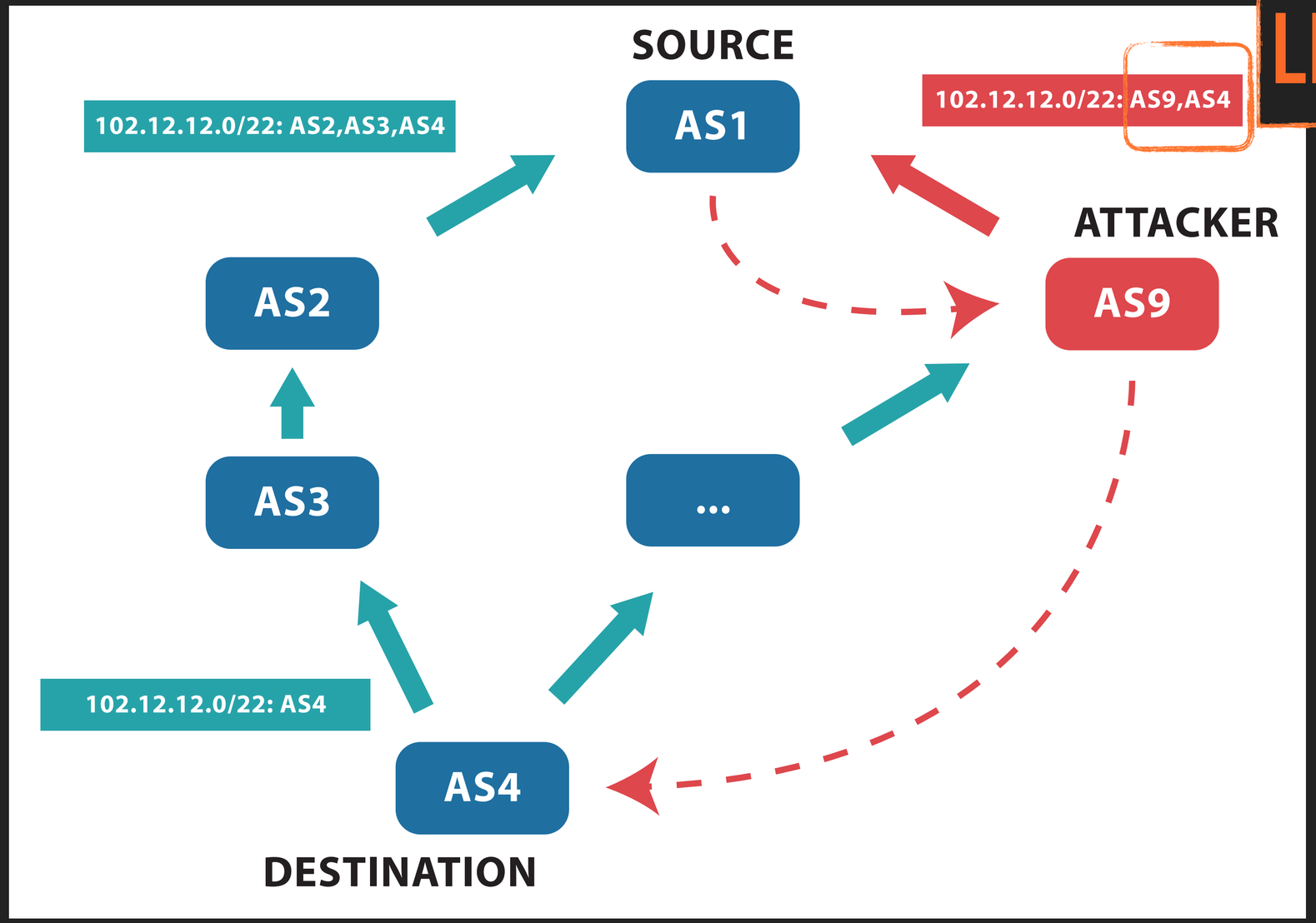


ORIGIN HIJACKS: "SUB"MOAS



#2
FAKE PATH HIJACKS

FAKE PATH HIJACKS

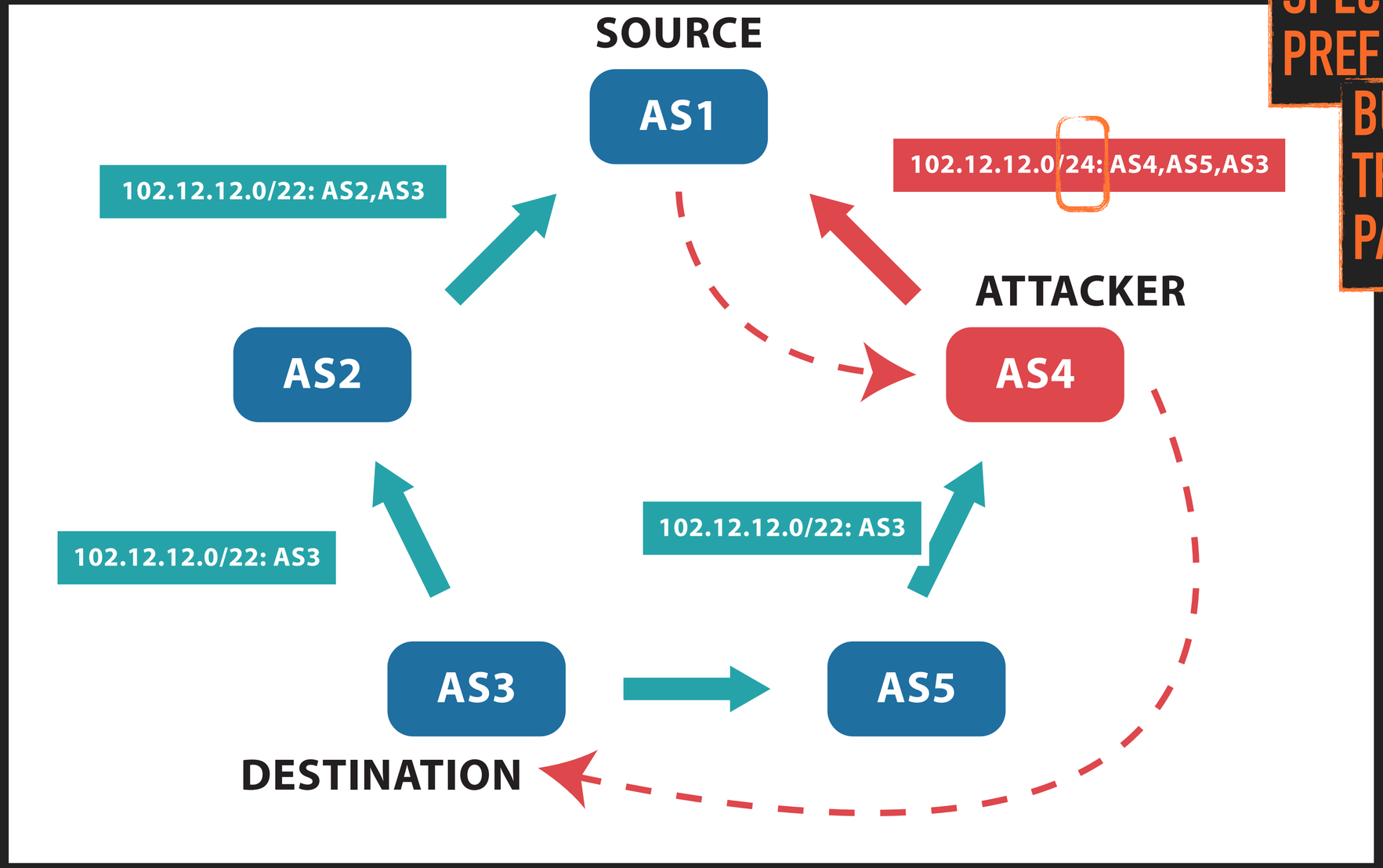


FAKE LINK

BUT TRUE ORIGIN

#3
"DEFCON #16" HIJACKS

"DEFCON #16" HIJACKS



MORE SPECIFIC PREFIX

BUT TRUE PATH

RECAP:

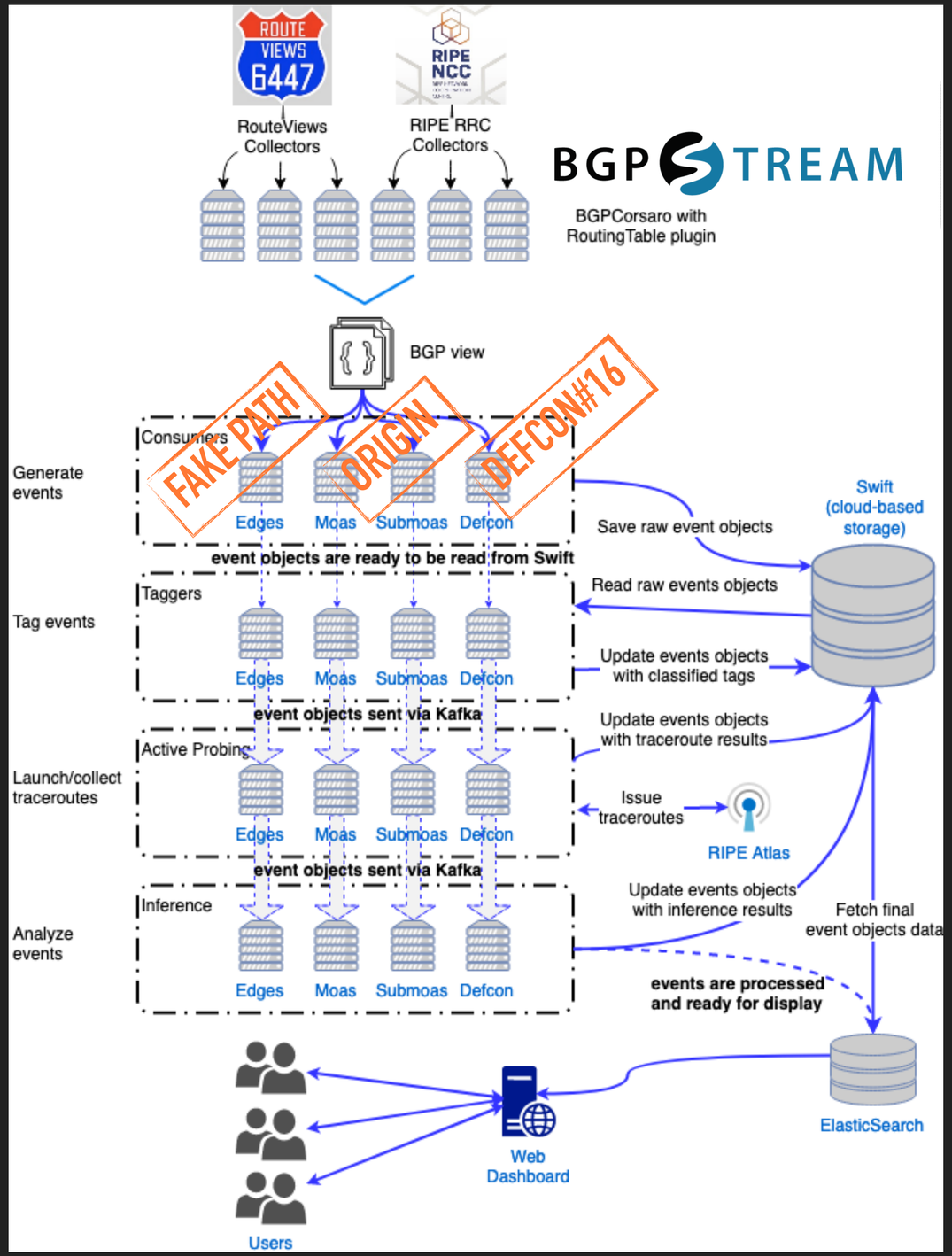
“ORIGIN” (MOAS/SUBMOAS)

“FAKE PATH”

“DEFCON #16”

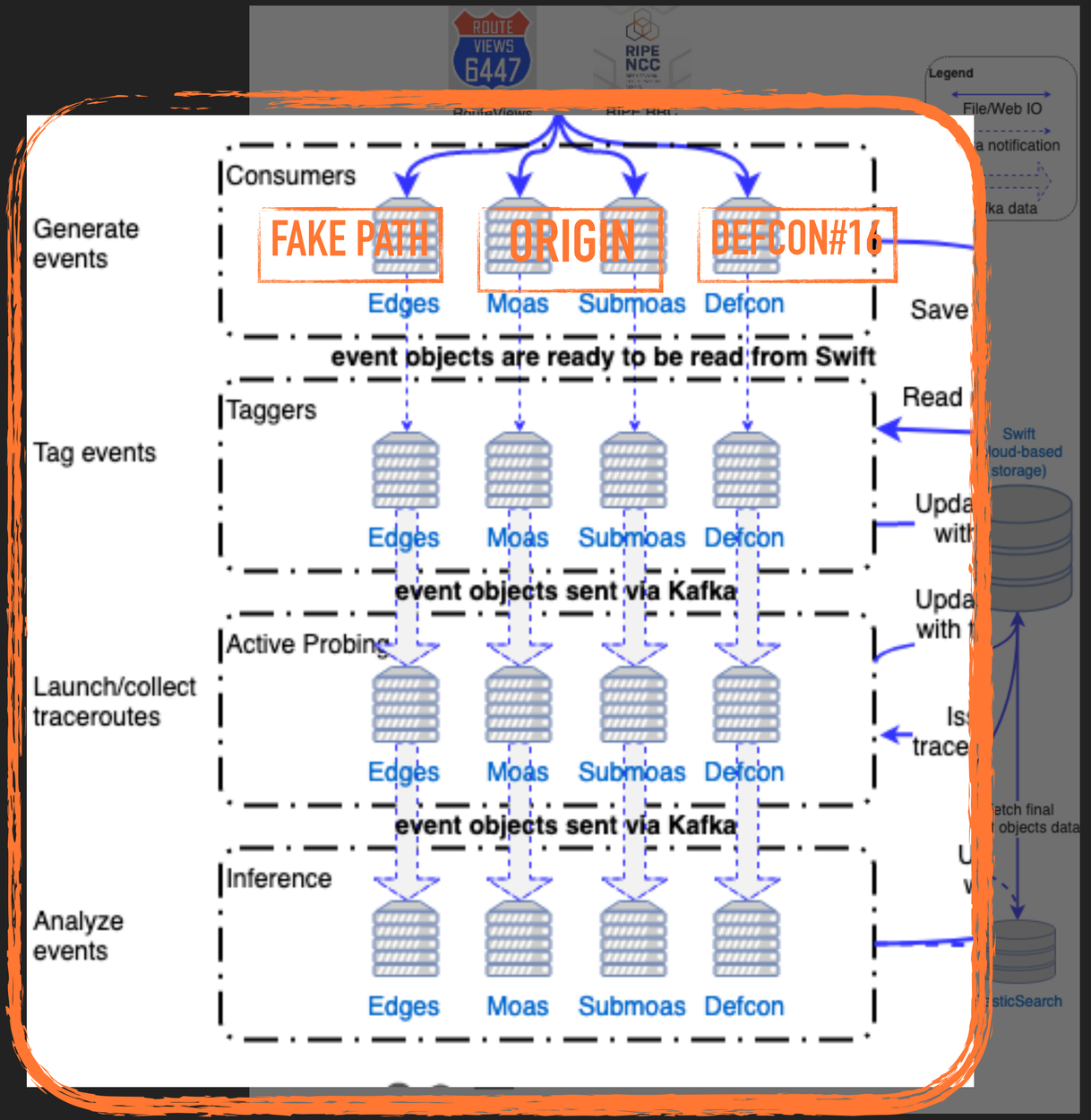
Prototype: Infrastructure

- Running 24/7
  - > 300 BGP routers (RV + RIS)
    - 5 min granularity
    - ~30 min latency
  - RIPE Atlas for traceroutes



Prototype: Methods

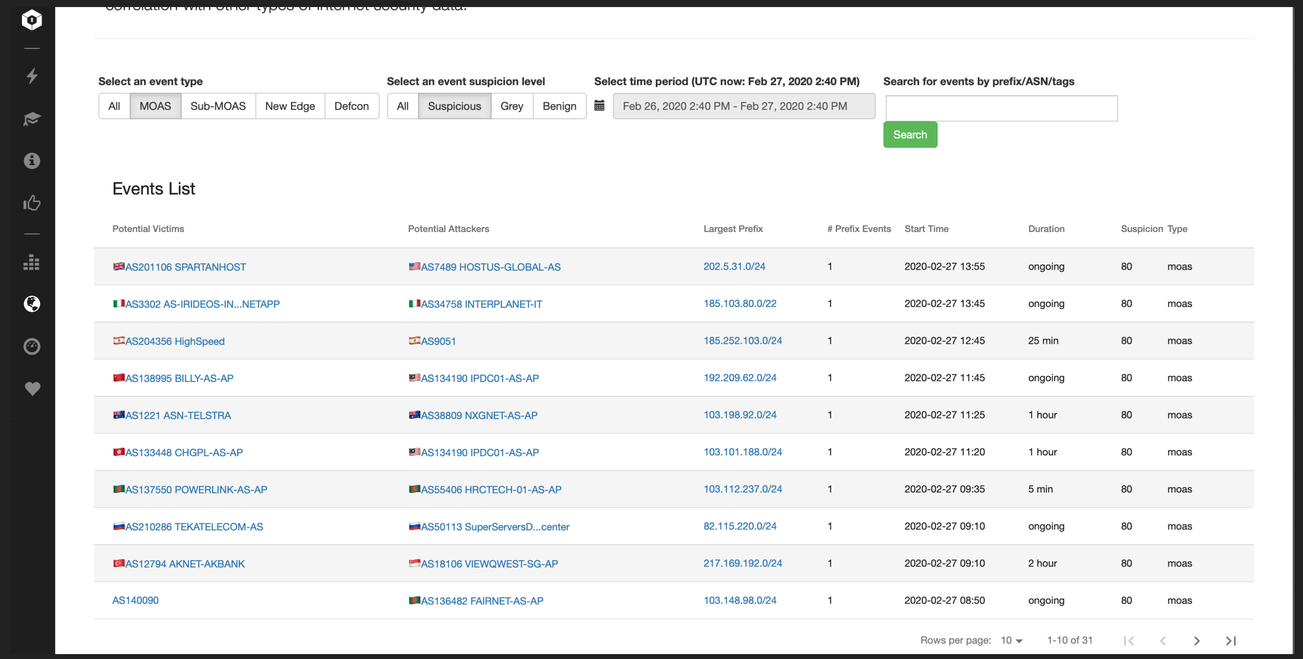
- 4 Pipelines detect all 4 classes of attacks
- Event tagging (>70 tags)
  - Based on AS2Org, AS Relationships, . . .
- Strategy for traceroute probe selection
- Inference:
  - Suspicious, Grey, Benign
  - Misconfigurations

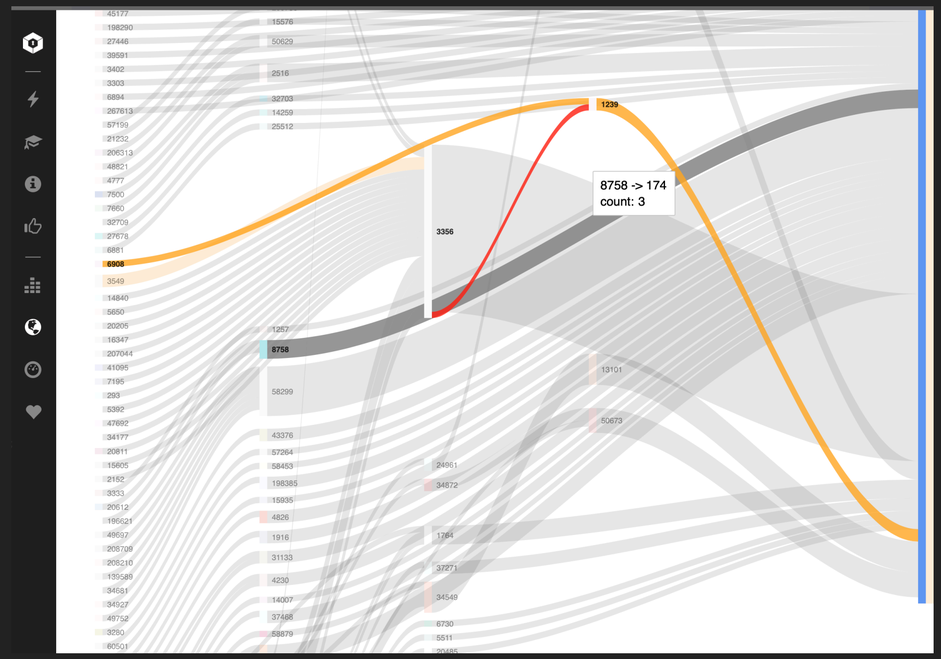


Prototype: Dashboard

- dev.hicube.caida.org/feeds 

- Search by ASN, prefix, tag, . . .
- . . .





THANKS

dev.hicube.caida.org/feeds

alberto@caida.org