# ASSISTS TTA#2

# 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

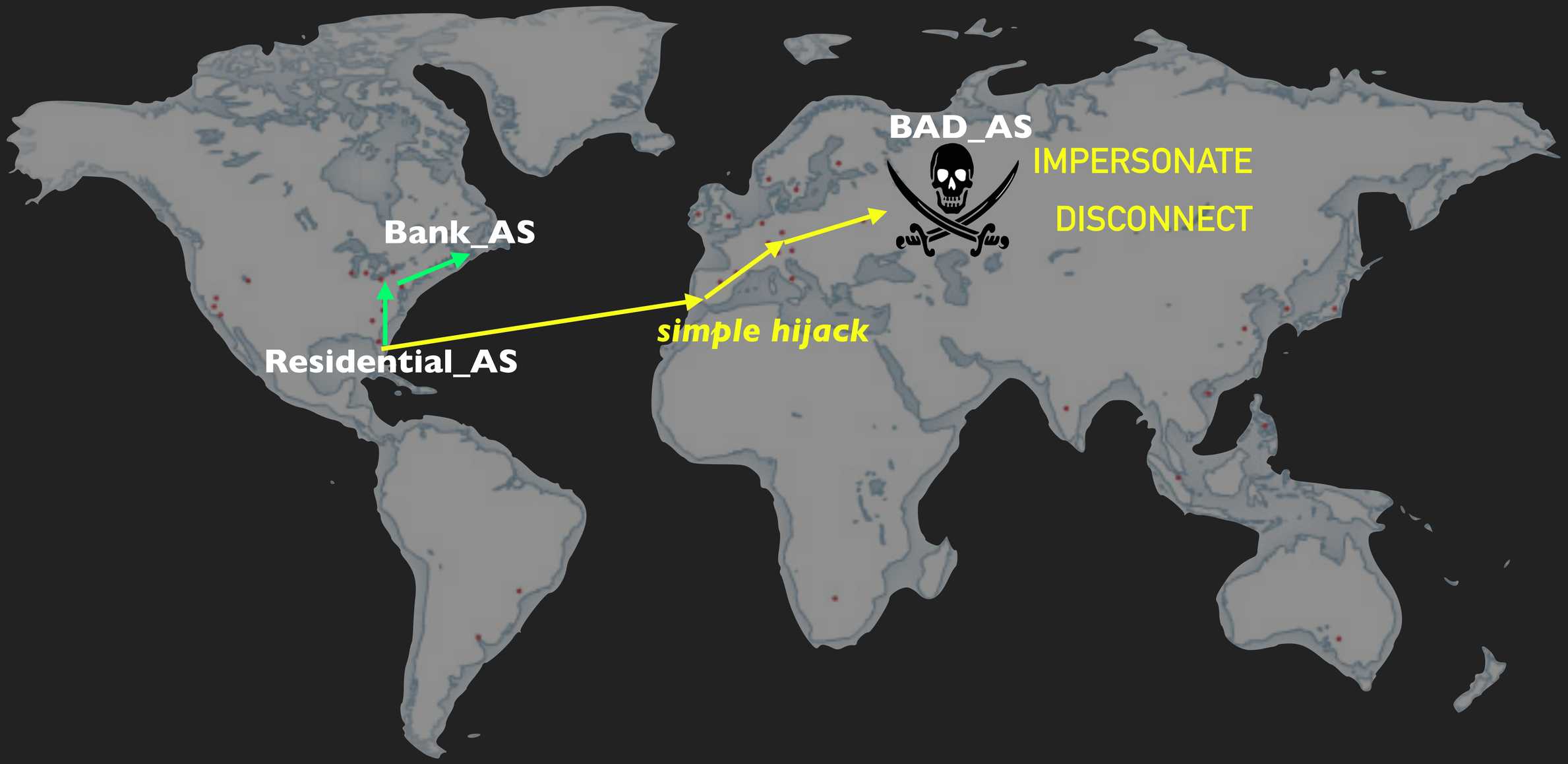
IIJ
Internet Initiative Japan

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

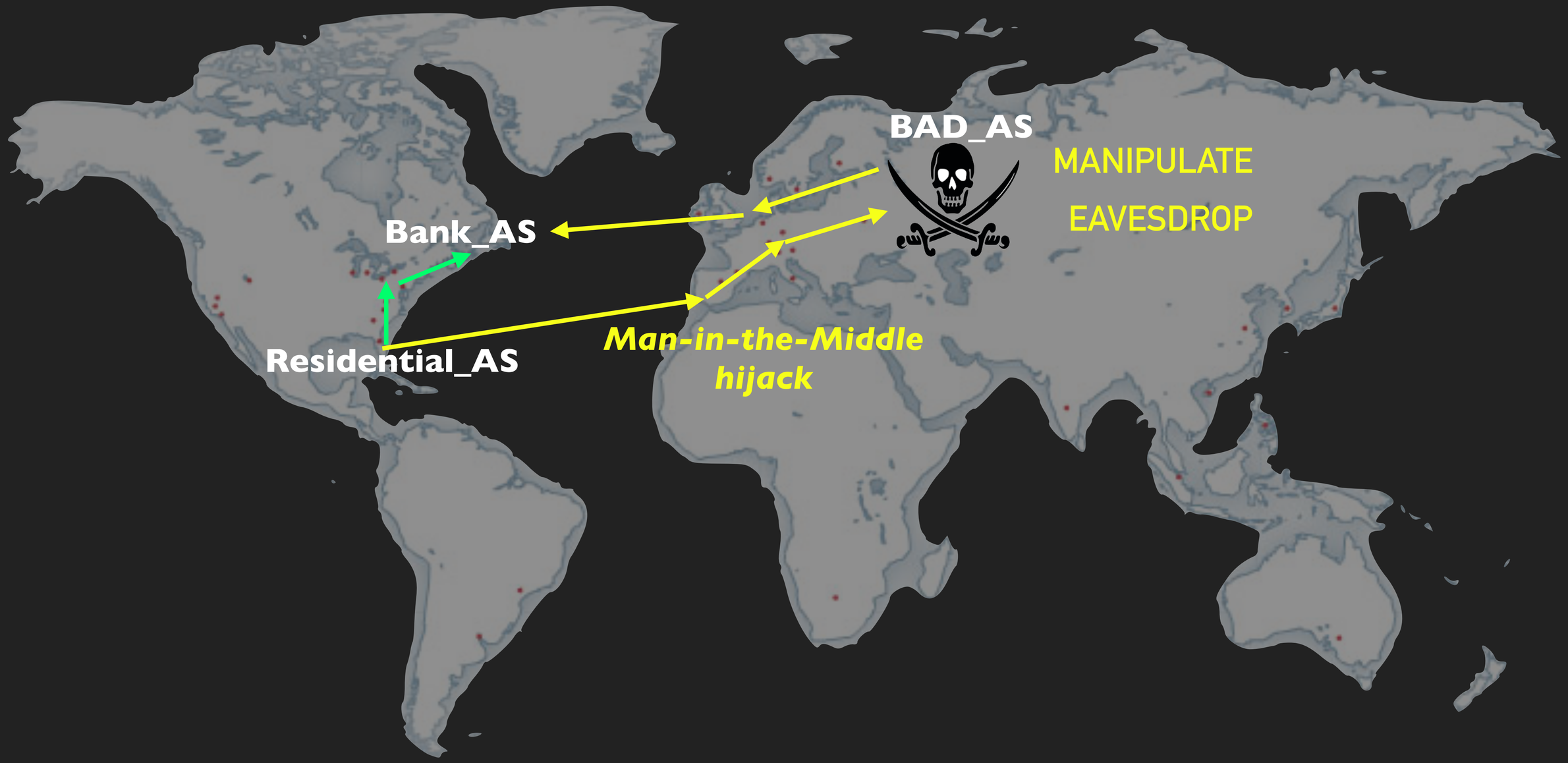
MIT CSAIL

# PROBLEM
# ROUTE HIJACKING

# ATTACKING GLOBAL (BGP) ROUTING



# ATTACKING GLOBAL (BGP) ROUTING



# CAIDA BGP (HIJACKING) OBSERVATORY

- EVENT DETECTION AND INVESTIGATION
- SITUATIONAL AWARENESS
- OPERATORS' DEBUG TOOL
- TESTBED FOR DEVELOPING NEW DEFENSE TECHNIQUES

HUB for Internet Incident Investigation

*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 - Dec 2019*
*ASSISTS - Advancing Scientific Study of Internet Security and Topological Stability*

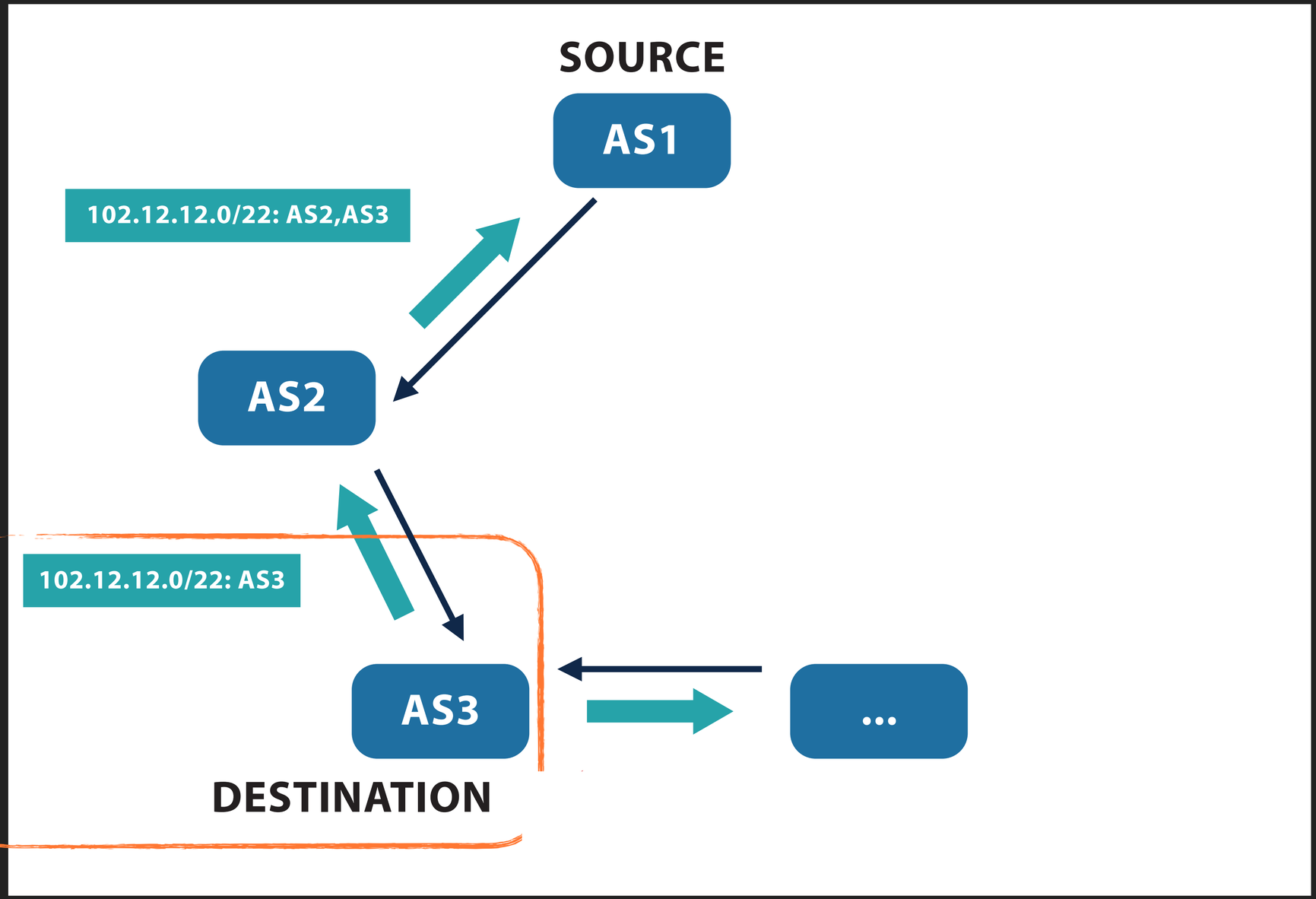
# CAIDA BGP (Hijacking) Observatory

1. Detects suspicious events by monitoring the Internet 24/7
   - Detects sophisticated attacks
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

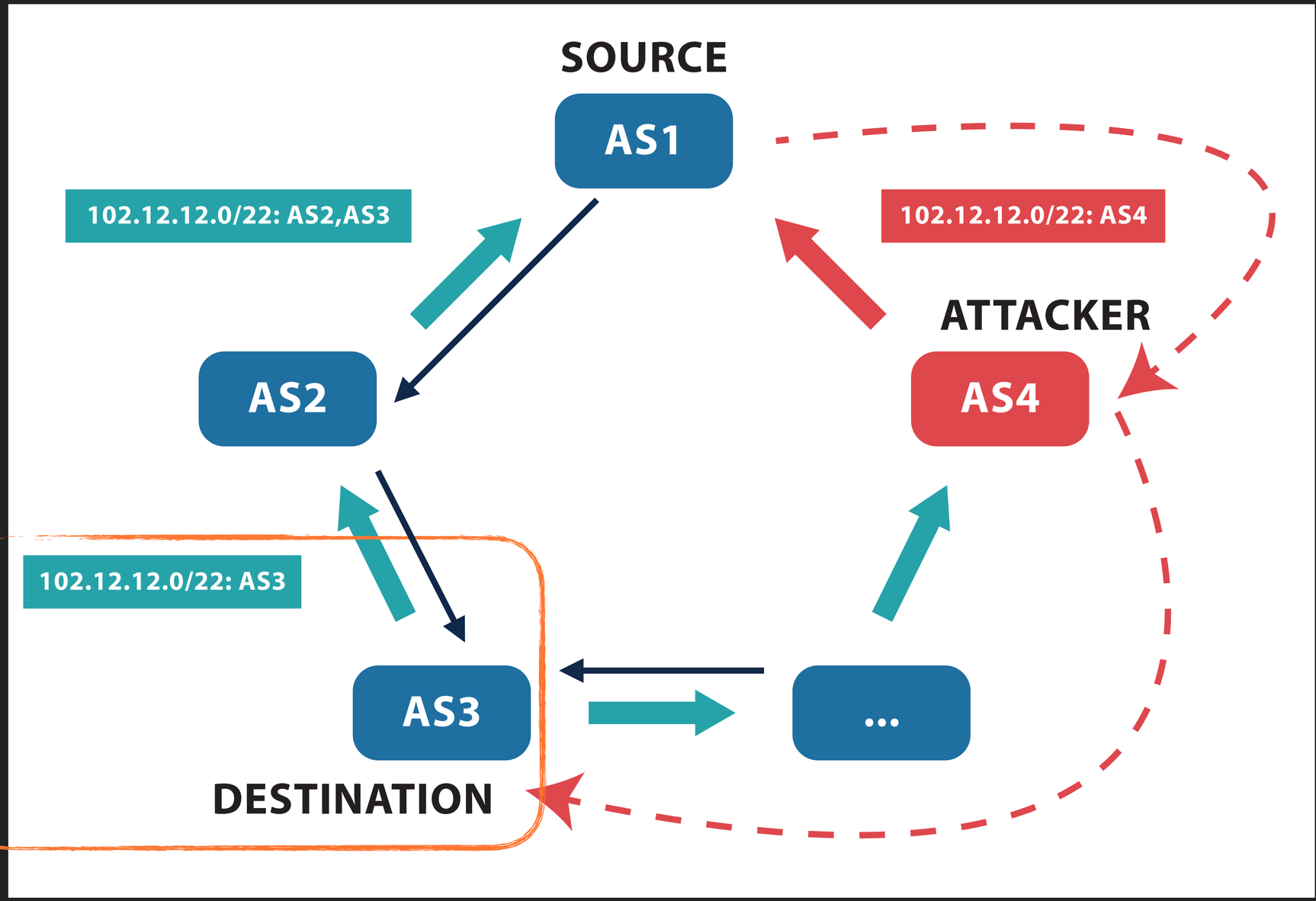
# ROUTE HIJACKING
# ATTACK TECHNIQUES

# #1
# ORIGIN HIJACKS

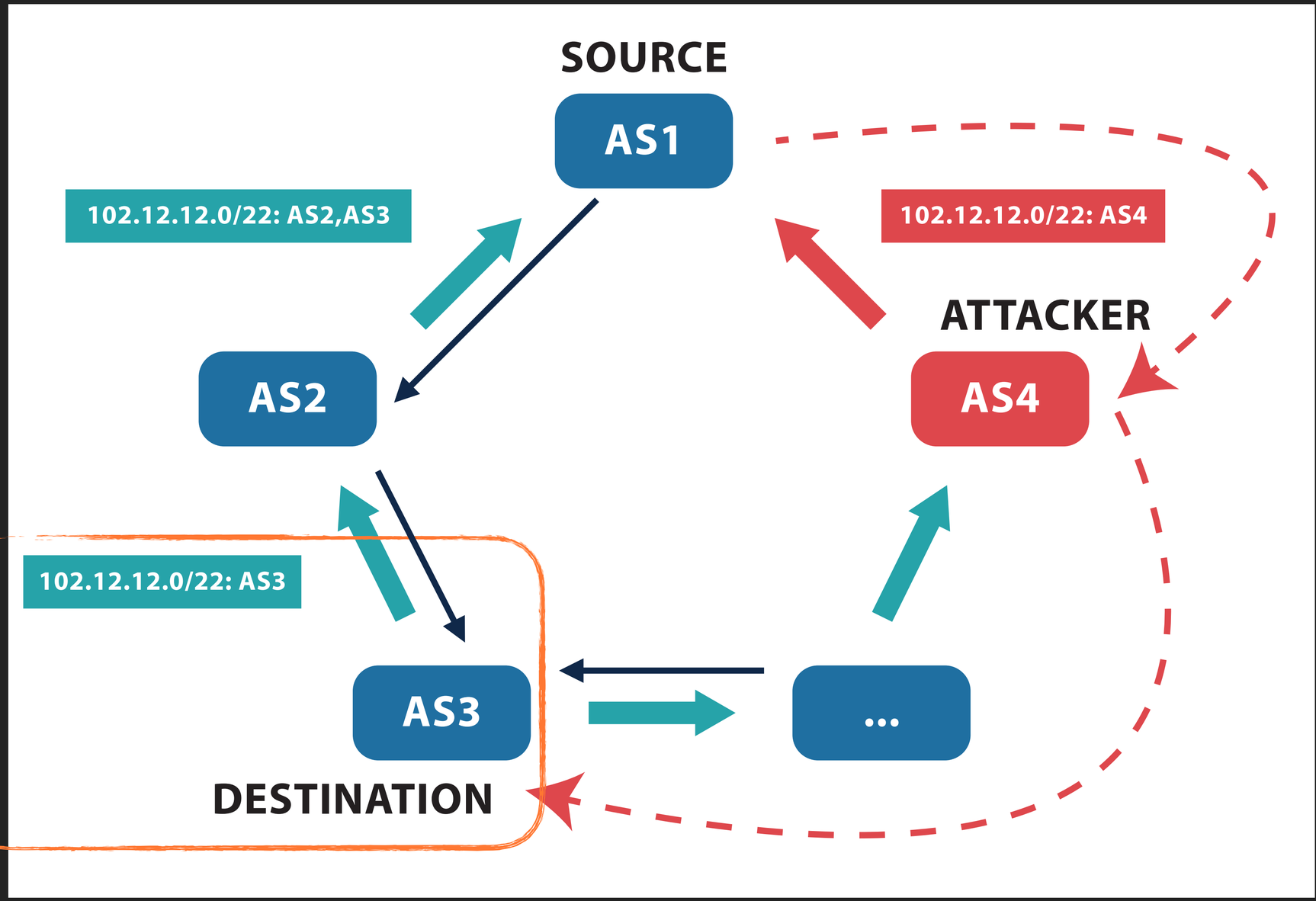
# ORIGIN HIJACKS



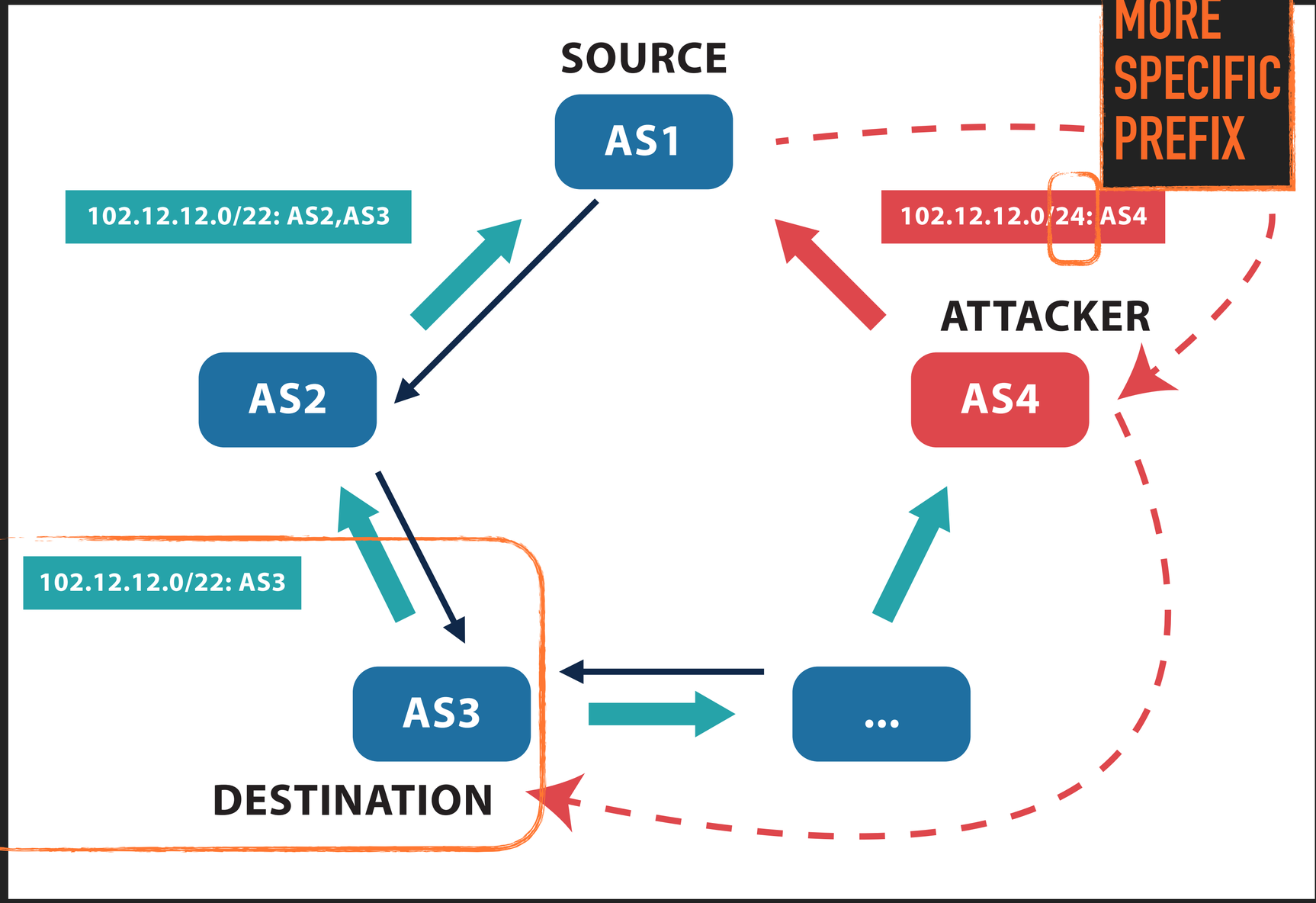
# ORIGIN HIJACKS



# ORIGIN HIJACKS: MOAS

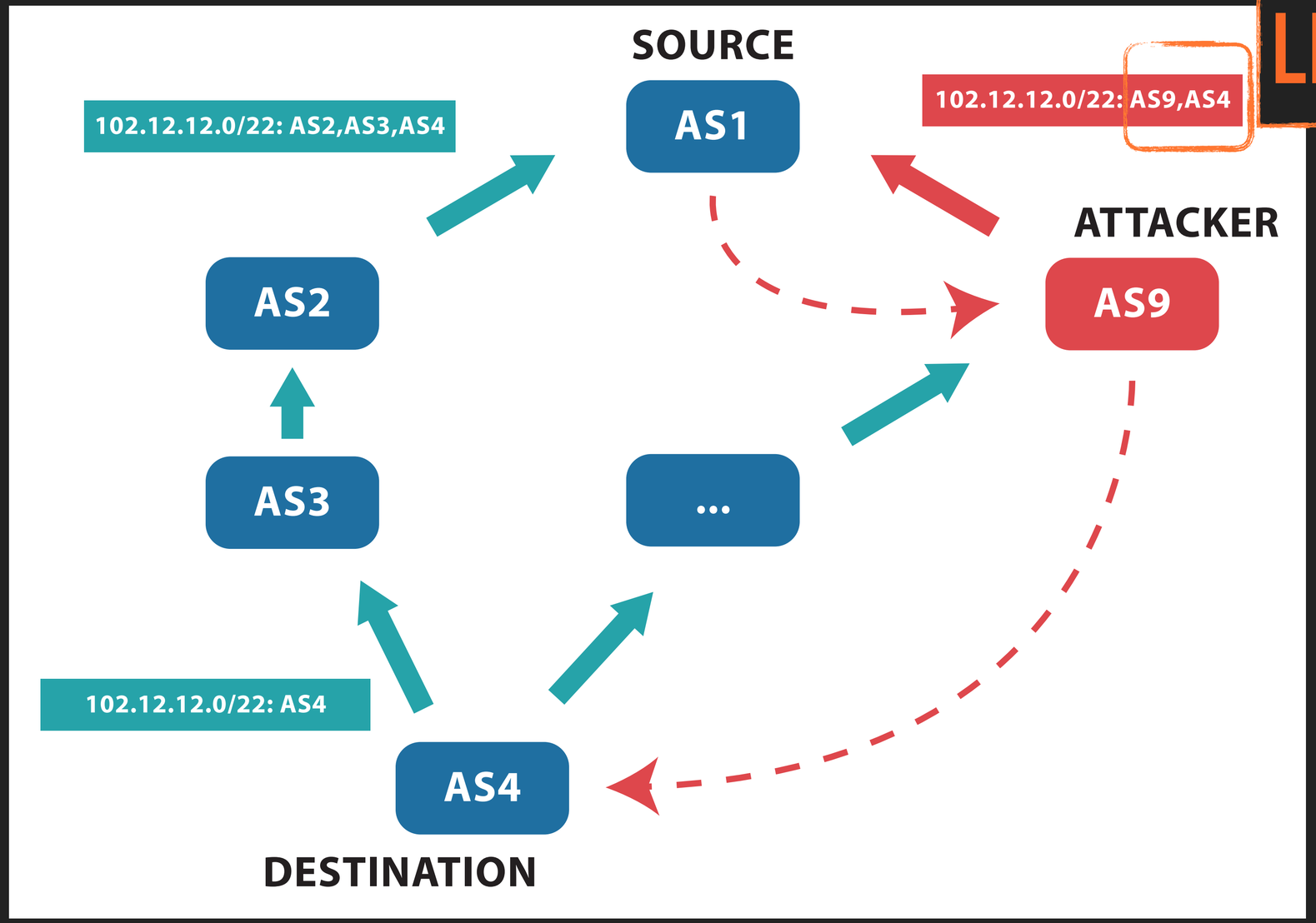


# ORIGIN HIJACKS: "SUB"MOAS



# #2
# FAKE PATH HIJACKS

# FAKE PATH HIJACKS

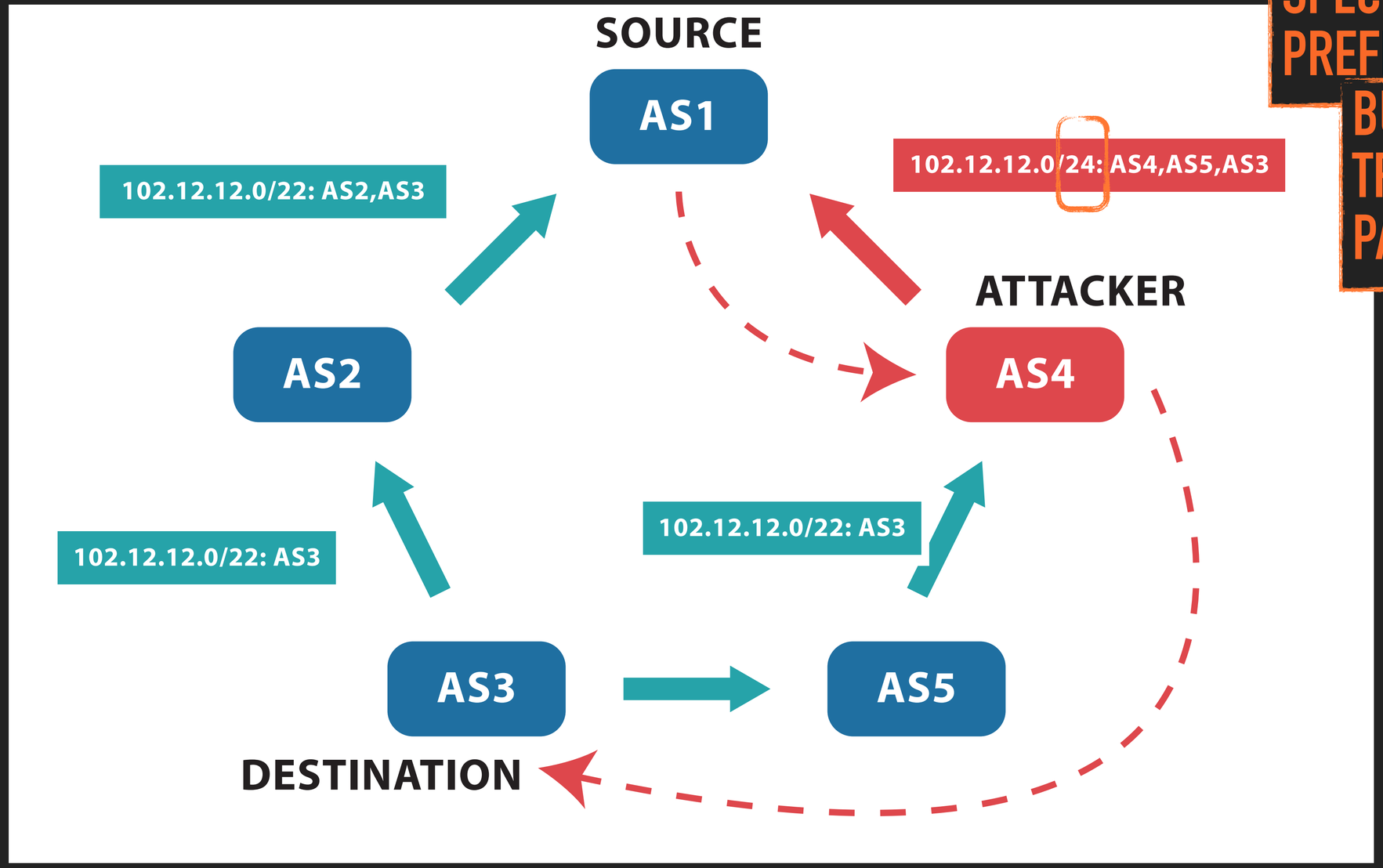



FAKE LINK

BUT TRUE ORIGIN

# #3
# "DEFCON #16" HIJACKS

# "DEFCON #16" HIJACKS




MORE SPECIFIC PREFIX

BUT TRUE PATH

# RECAP:

# “ORIGIN” (MOAS/SUBMOAS)

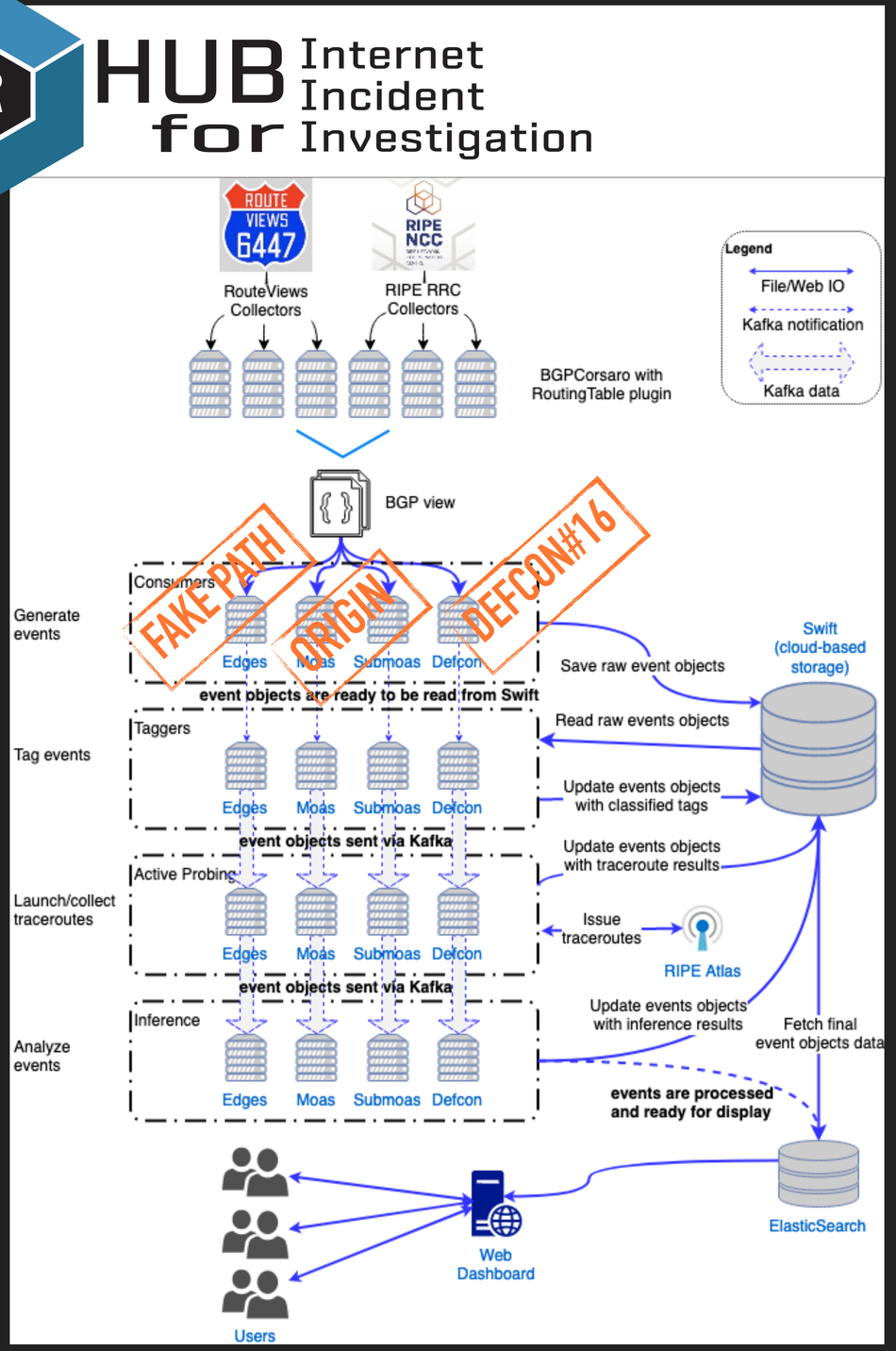
# “FAKE PATH”

# “DEFCON #16”

# Prototype: Infrastructure

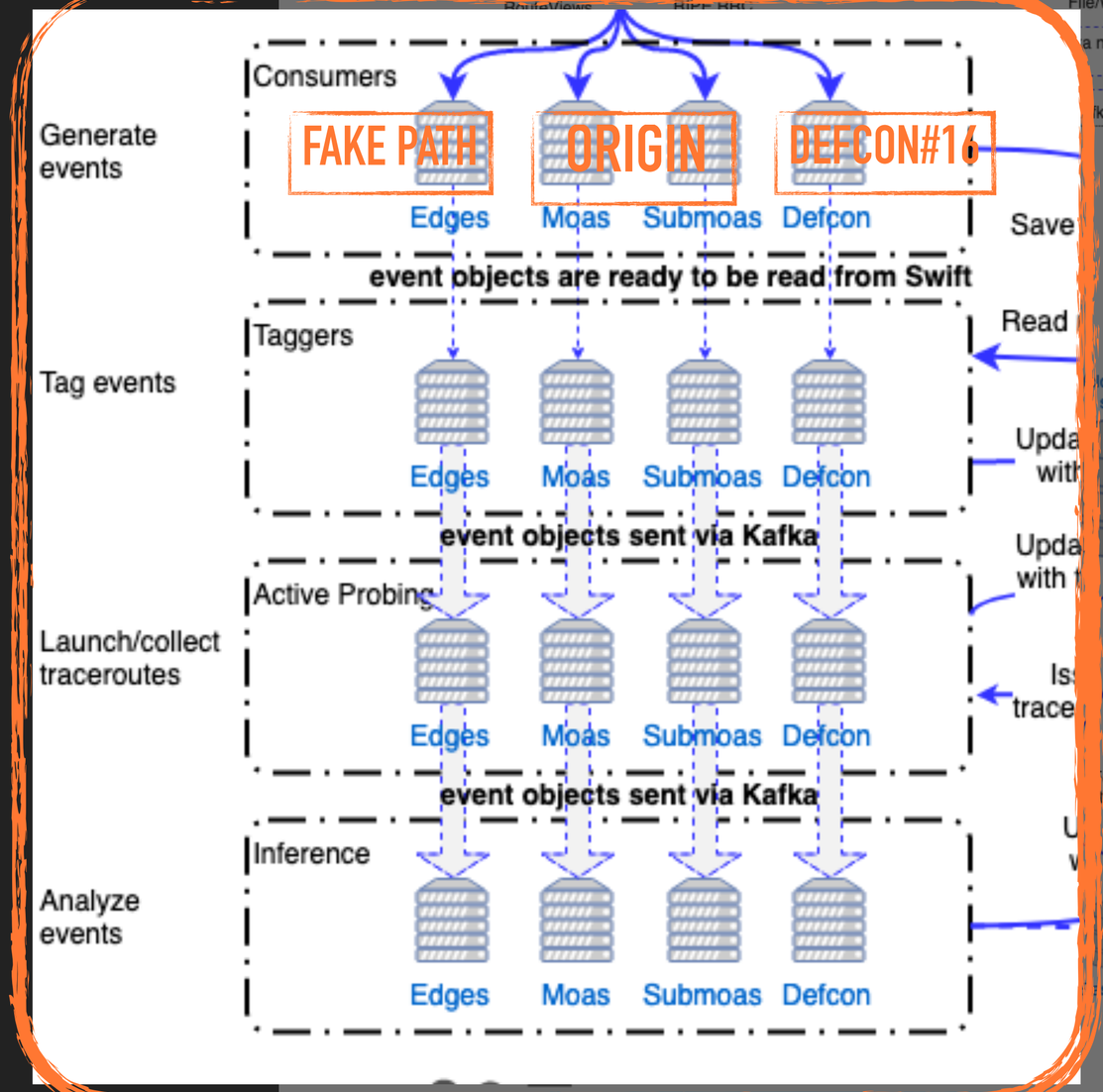
- Running 24/7
  - > 300 BGP monitors (RV + RIS)
  - RIPE Atlas for traceroutes
  - 5 min granularity
  - ~30 min latency
- Leveraging HI-CUBE infrastructure
  - JSON Event DB (Elastic Search)
  - Time Series DB (DBATS)
  - Web app. & Viz framework

HUB Internet Incident for Investigation



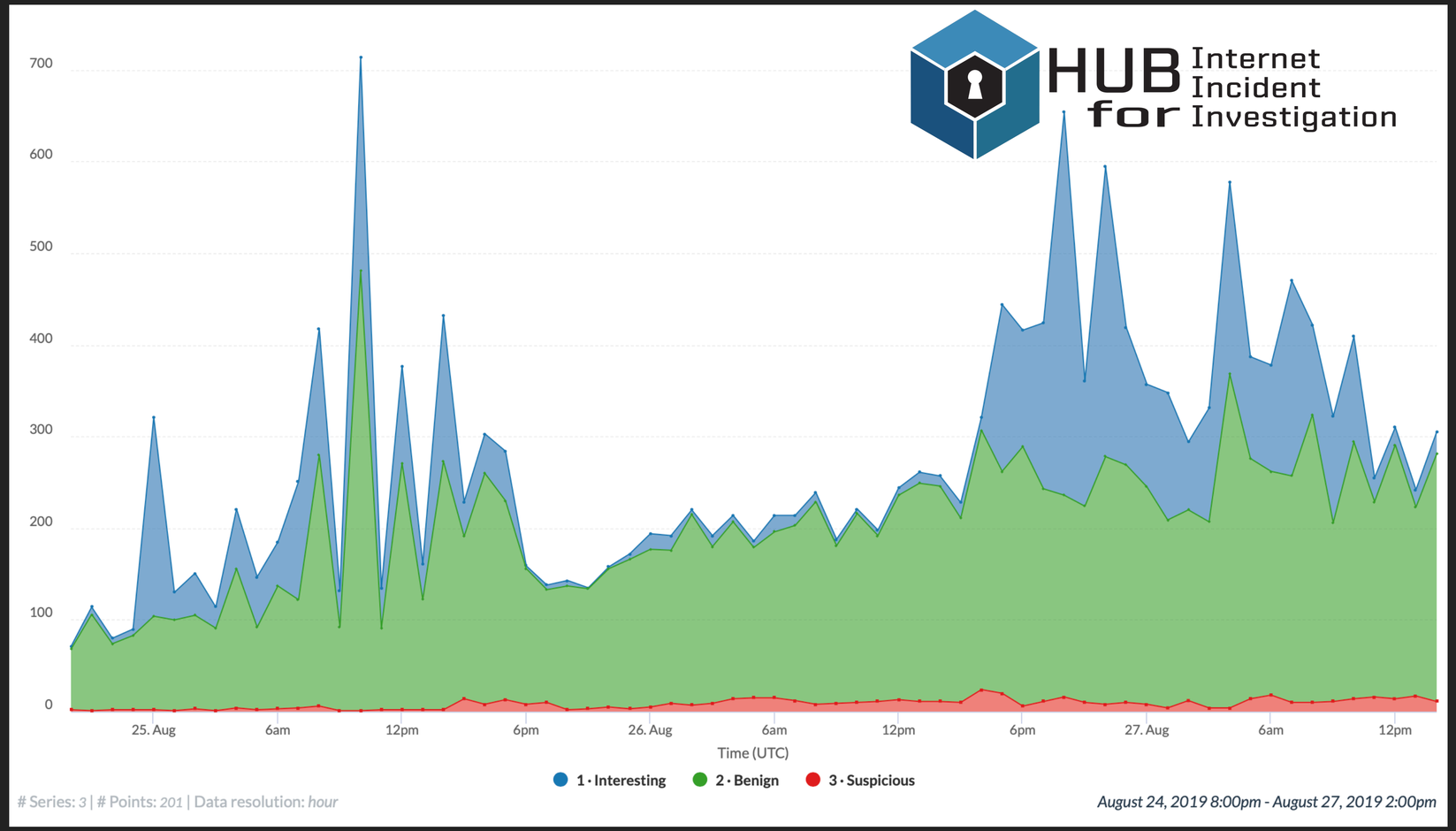
# Prototype: Methods

- 4 Pipelines detect all classes of attacks
- Event tagging (62 tags)
  - Based on AS2Org, AS Relationships, . . .
- Strategy for traceroute probe selection
- Inference:
  - Suspicious, Benign, Interesting
  - Misconfigurations



# Prototype: Methods

- Inference – Average Events per hour:
  - Benign: 31
  - Interesting: 7
  - Suspicious: 1



# Prototype: Dashboard

- bgp.caida.org 

- Leveraging HI-CUBE
  - Visualization interfaces
  - Porting to web app. framework to dev.hicube.caida.org
- Search by ASN, prefix, tag, . . .

# Prototype: Dashboard

- **Bad Actor**: Russian AS #57129 RU-SERVERSGET-KRSK, Optibit LLC:
  - Recent complaints on NANOG
  - Behavior visible through the Observatory
  - Suspicious: 17 events in August

2019-08-01T00:00 - 2019-08-31T23:59 | AS57129 | Go!

Show 10 entries

| Potential Victim | Potential Attacker | Largest Prefix | # Prefix Events | Start Time | Duration | Type |
|---|---|---|---|---|---|---|
| AS57129 RU-SERVERSGET-KRSK ⚠ | AS9009 M247 ⚠ | 158.46.196.0/22 | 1 pfx (1024 addrs) | 2019-08-07 12:15:00 | 5 min | origin hijack (moas) |
| AS9044 SOLNET | AS57129 RU-SERVERSGET-KRSK ⚠ | 62.130.0.0/16 | 1 pfx (65536 addrs) | 2019-08-07 12:15:00 | ongoing | origin hijack (submoas) |
| AS9044 SOLNET | AS57129 RU-SERVERSGET-KRSK ⚠ | 31.144.0.0/16 | 1 pfx (65536 addrs) | 2019-08-07 11:50:00 | 35 min | origin hijack (submoas) |
| AS9044 SOLNET | AS57129 RU-SERVERSGET-KRSK ⚠ | 213.5.72.0/22 | 1 pfx (1024 addrs) | 2019-08-02 02:40:00 | ongoing | origin hijack (submoas) |
| AS43260 AS43260 | AS57129 RU-SERVERSGET-KRSK ⚠ | 149.126.203.0/24 | 1 pfx (256 addrs) | 2019-08-01 08:35:00 | 5 min | origin hijack (moas) |
| AS48347 MTW-AS | AS57129 RU-SERVERSGET-KRSK ⚠ | 149.126.194.0/24 | 4 pfxs (1024 addrs) | 2019-08-01 08:10:00 | 50 min | origin hijack (submoas) |
| AS43260 AS43260 | AS57129 RU-SERVERSGET-KRSK ⚠ | 149.126.200.0/24 | 1 pfx (256 addrs) | 2019-08-01 08:10:00 | 5 min | origin hijack (moas) |

Showing 11 to 17 of 17 entries

Previous 1 2 Next

# COMPETITION & BENEFITS:
# A TAXONOMY OF BGP MONITORING/ ANALYSIS RESOURCES

# LANDSCAPE

- **Raw data collection**: RouteViews, RIPE RIS, CSU BGPMON, PCH, . . .
- **Per-AS detection service**: Cisco Bgpmon/Bgpstream, FORTH-CAIDA ARTEMIS, Cisco Network Insight, Thousand Eyes, . . .
- **Global monitoring and detection**: CAIDA BGP Observatory, Cisco Bgpmon/Bgpstream, . . .
- **Raw data analysis tools/APIs**: CSU BGP Observatory, CAIDA BGPStream, . . .

# LANDSCAPE

- **Raw data collection**: RouteViews, RIPE RIS, CSU BGPMON, PCH, . . .
- **Per-AS detection service**: Cisco Bgpmon/Bgpstream, FORTH-CAIDA ARTEMIS, Cisco Network Insight, Thousand Eyes, . . .
- **Global monitoring and detection**: CAIDA BGP Observatory, Cisco Bgpmon/Bgpstream, . . .
- **Raw data analysis tools/APIs**: CSU BGP Observatory, CAIDA BGPStream, . . .

# LANDSCAPE

LIMITED TO THE CUSTOMER PREFIXES

- **Raw data collection:** RouteViews, RIPE RIS, CSU BGPMON, PCH, . . .
- **Per-AS detection service:** Cisco Bgpmon/Bgpstream, FORTH-CAIDA ARTEMIS, Cisco Network Insight, Thousand Eyes, . . .
- **Global monitoring and detection:** CAIDA BGP Observatory, Cisco Bgpmon/Bgpstream, . . .
- **Raw data analysis tools/APIs:** CSU BGP Observatory, CAIDA BGPStream, . . .

CANNOT RELY ON GROUND TRUTH

# USE BY DHS?

LIMITED TO THE CUSTOMER PREFIXES

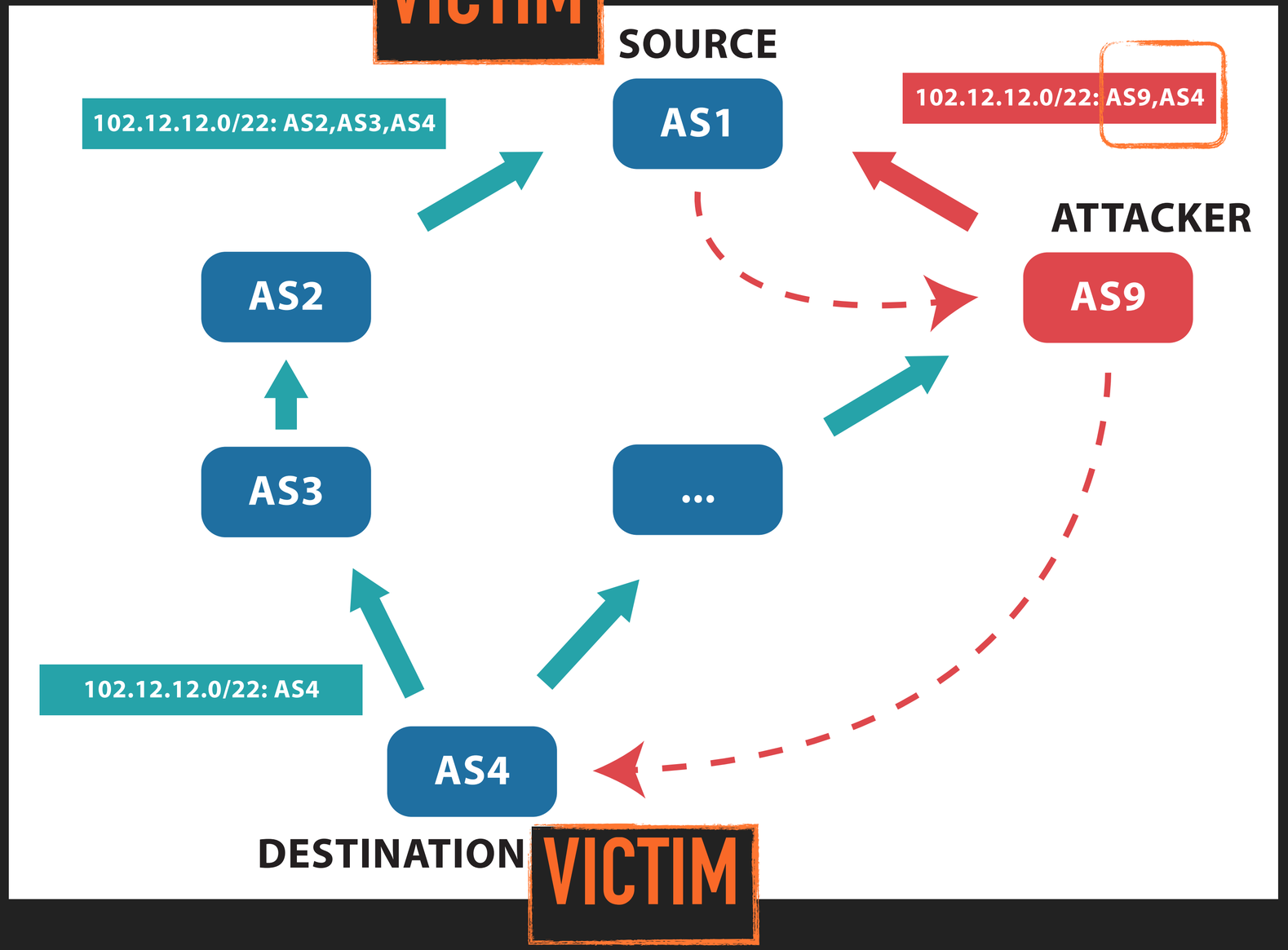
A limitation for applications in national security, or for e.g., cloud providers

- Raw data collection: RouteViews, RIPE RIS, CSU BGPMON, PCH, . . .
- Per-AS detection service: Cisco Bgpmon/Bgpstream, FORTH-CAIDA ARTEMIS, Cisco Network Insight, Thousand Eyes, . . .
- Global monitoring and detection: CAIDA BGP Observatory, Cisco Bgpmon/Bgpstream, . . .
- Raw data analysis tools/APIs: CSU BGP Observatory, CAIDA BGPStream, . . .

Useful for alerts, further investigation, forensic analysis, situational awareness, . . .

CANNOT RELY ON GROUND TRUTH

# FAKE PATH HIJACKS



# USE BY DHS?

LIMITED TO THE CUSTOMER PREFIXES

A limitation for applications in national security, or for e.g., cloud providers

- Raw data collection: RouteViews, RIPE RIS, CSU BGPMON, PCH, . . .
- Per-AS detection service: Cisco Bgpmon/Bgpstream, FORTH-CAIDA ARTEMIS, Cisco Network Insight, Thousand Eyes, . . .
- Global monitoring and detection: CAIDA BGP Observatory, Cisco Bgpmon/Bgpstream, . . .
- Raw data analysis tools/APIs: CSU BGP Observatory, CAIDA BGPStream, . . .

Useful for alerts, further investigation, forensic analysis, situational awareness, . . .

CANNOT RELY ON GROUND TRUTH

# USE BY DHS?

- Raw data collection: RouteViews, RIPE RIS, CSU BGPMON, PCH, . . .
- Per-AS detection service: Cisco Bgpmon/Bgpstream, FORTH-CAIDA ARTEMIS, Cisco Network Insight, Thousand Eyes, . . .
- **Global monitoring and detection: CAIDA BGP Observatory, Cisco Bgpmon/ Bgpstream, . . .**
- Raw data analysis tools/APIs: CSU BGP Observatory, CAIDA BGPStream, . . .

Advanced inference methods
E.g., detects more sophisticated attacks: “Fake Path”, “Defcon#16”

# SUCCESS STORIES & METRICS/ CHALLENGES & FUTURE WORK

# Success Stories:

- Collaborated with US Cyber Command
  - Interested in our methods
- Initial interest by Microsoft Azure
- Discussed collaboration with Internet Society
  - Use by operators + operators' feedback
  - Use by ISOC BGP Observatory through an API (need to develop)
- Enabled research on
  - Serial hijackers [IMC'19]
  - Fat-finger misconfiguration [TMA'19]

# Metrics:

- Classes of hijacking attacks covered: 3/3
- % events filtered out: 2% – 20%


- Avg # of most suspicious alerts per hour: 1


- Latency: 25 – 50 min
  - % events where latency prevented timely traceroutes
- % traceroutes correctly executed

# Challenges:

- Dealing with global data in the wild
  - methods are based on a model of reality and rationality
    - hard to fully predict impact of our methods
  - many cases hard to understand
- Validation of methods
- Debugging implementation
  - Complex distributed system
- Latency
- Assessing utility & prioritizing efforts

# Now working on:

- Debugging!
- Some changes to the data flow (leveraging ES earlier in the pipeline) to make the architecture more flexible and reliable
- Refine criteria used by the Inference Engine to assign severity levels
  - Also more/revise severity levels
- Complete porting to HI-CUBE web app. framework
  - Then extend features of dashboard and interfaces

# Future Work:

- More methods, tags, . . .
  - E.g., add RPKI validation
  - E.g., Route Leak detection (requested by ISOC)
- Extraction of statistics
  - Also extracting systematic bad actors
- HI-CUBE: correlating hijacks with outages, spam, scanning activity, . . .
- Work with operators to receive feedback+validation
- API
- Improve AS-Traceroute translation

# THANKS


https://bgp.caida.org

https://dev.hicube.caida.org

alberto@caida.org