

BGPSTREAM

An open-source software framework for live and historical BGP data analysis, supporting *scientific research, operational monitoring, and post-event analysis.*

BGPStream V2 (RC2) Available Now!

Powerful Tools & APIs

Quickly inspect raw BGP data from the command-line, develop Python apps, or build complex systems using a C/C++ API, etc. Designed to run anywhere, from laptops to clusters.

[Learn about the components »](#)

Seamless & Live Data Access

Give BGPStream a time range and it will automatically acquire and stream the right data to you. Enable realtime monitoring by changing a single parameter.

[See available data »](#)

Tutorials & Docs

Documentation includes software and API reference manuals as well as tutorials with fully-running code samples.

[Get started »](#)

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


Internet Initiative Japan

 **FORTH**
INSTITUTE OF COMPUTER SCIENCE
 Internet
Security &
Privacy
Intelligence
REsearch
Group

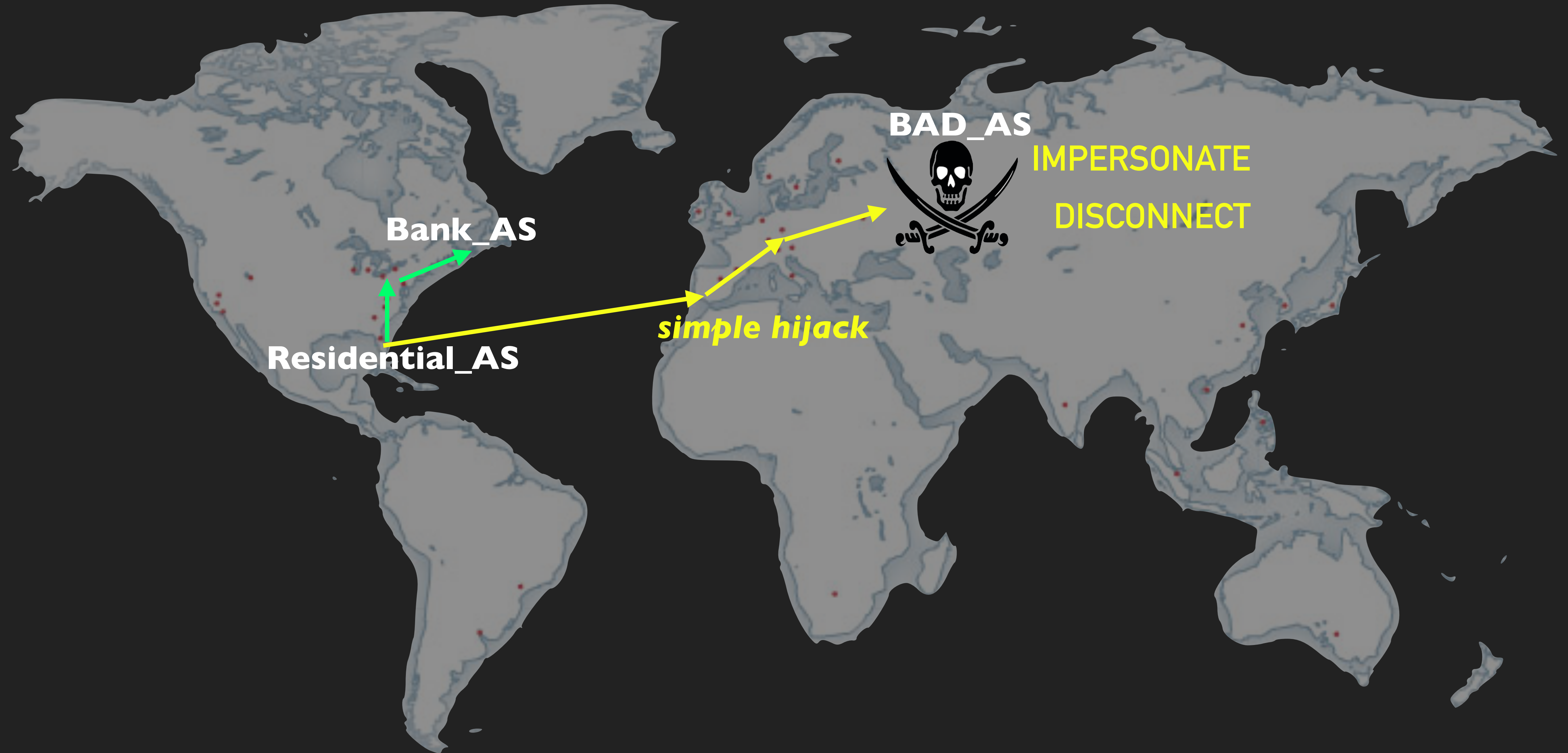


CSAIL

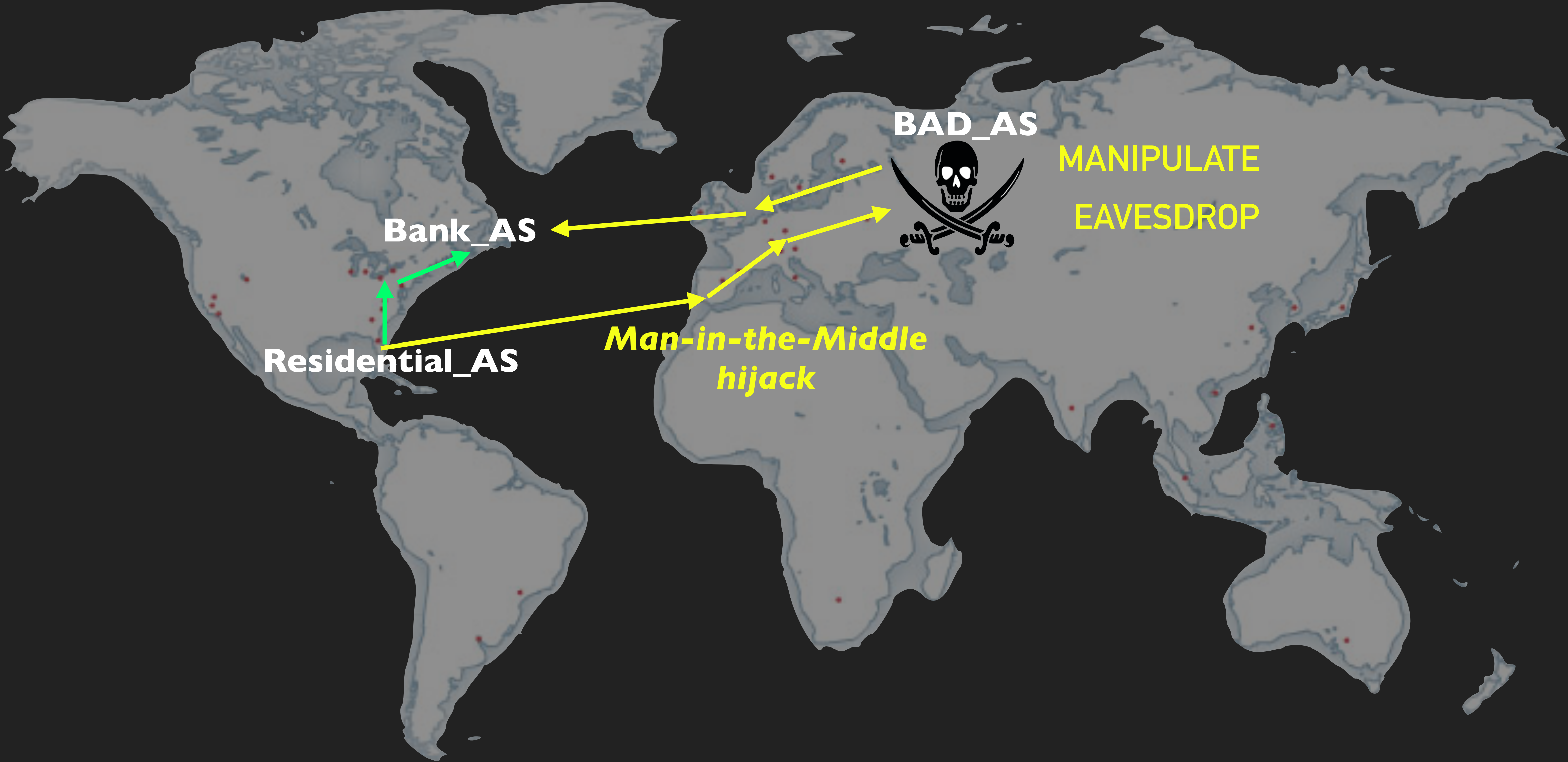
PROBLEM

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*

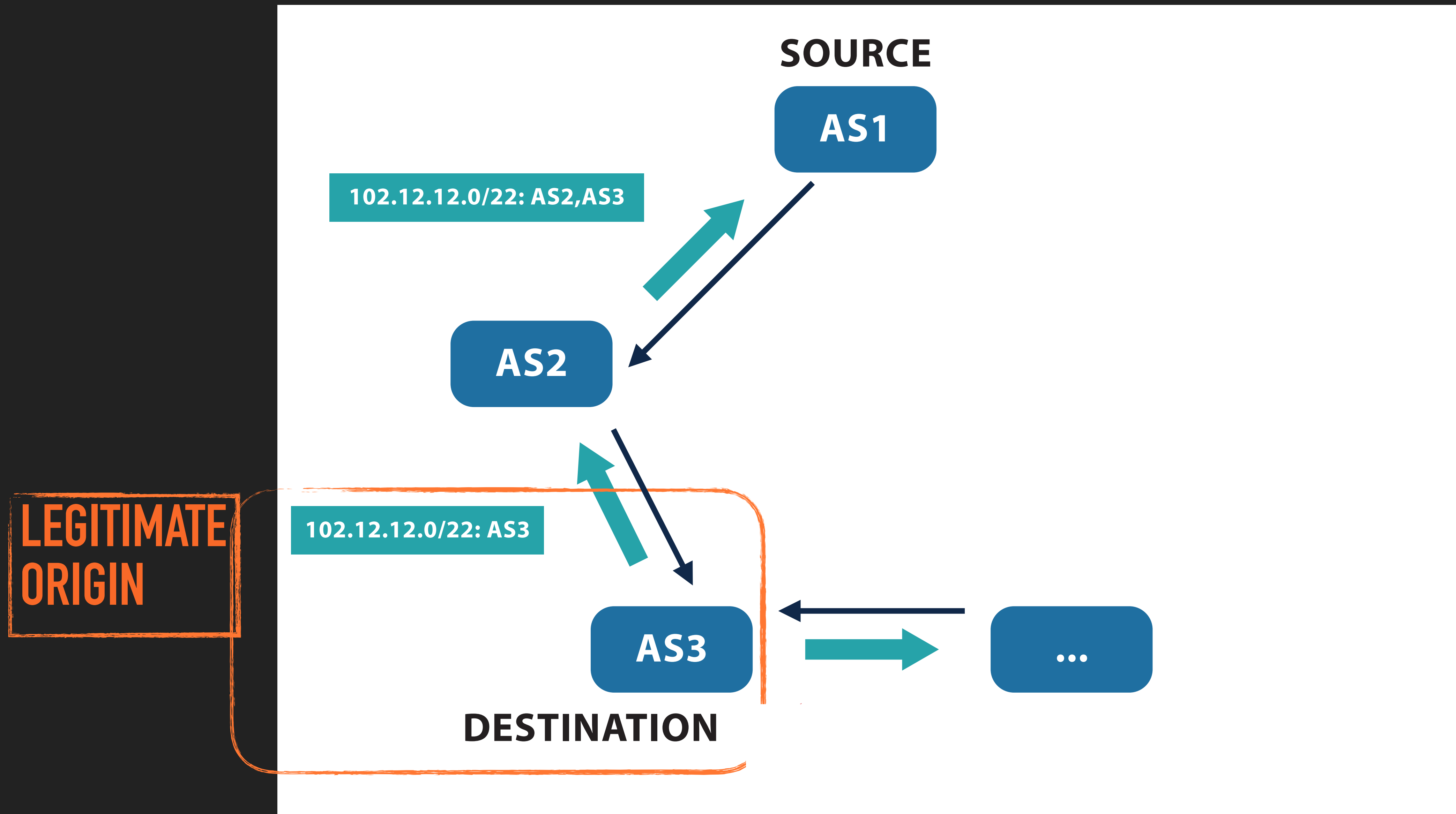
ROUTE HIJACKING

ATTACK TECHNIQUES

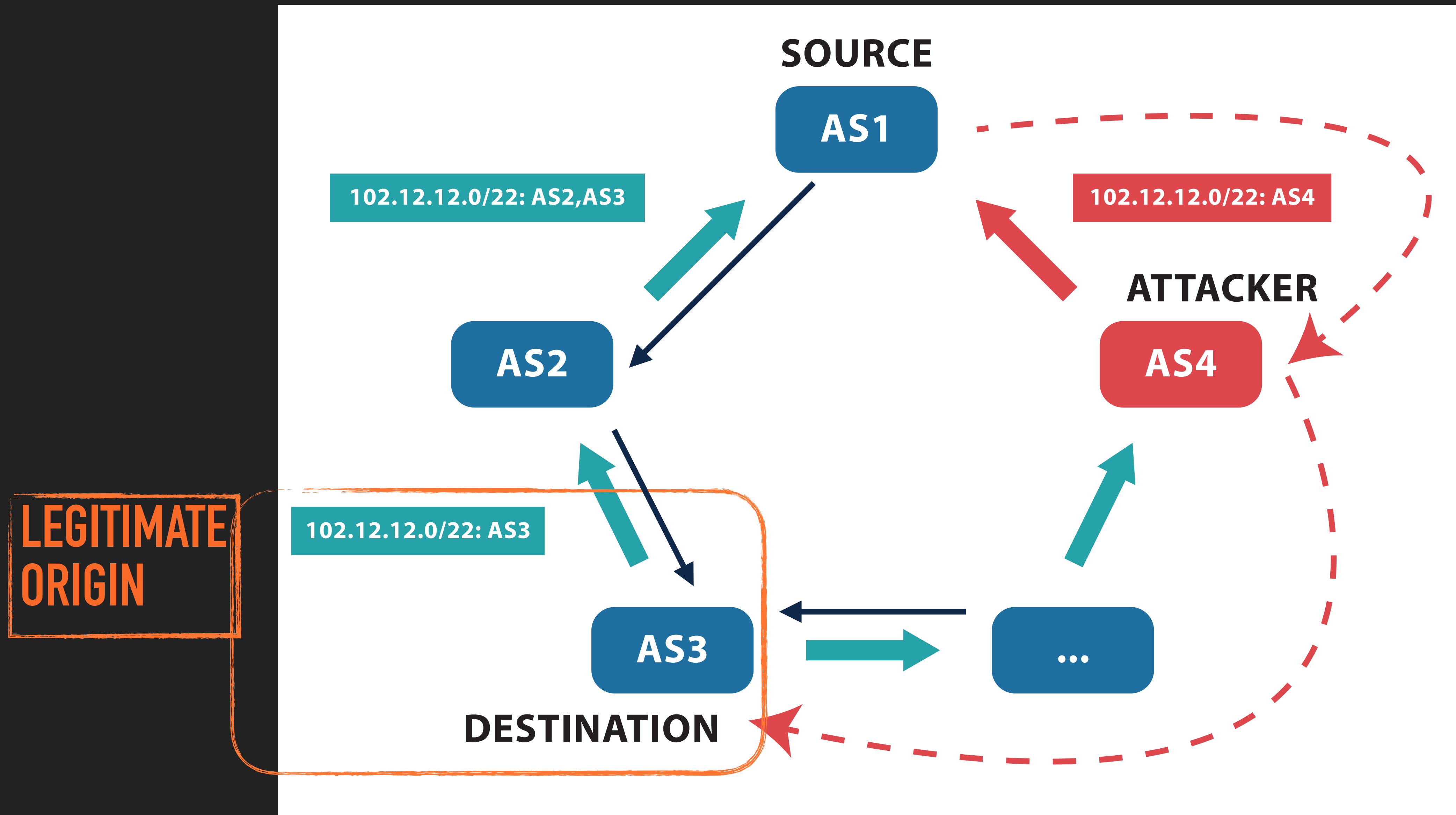
#1

ORIGIN HIJACKS

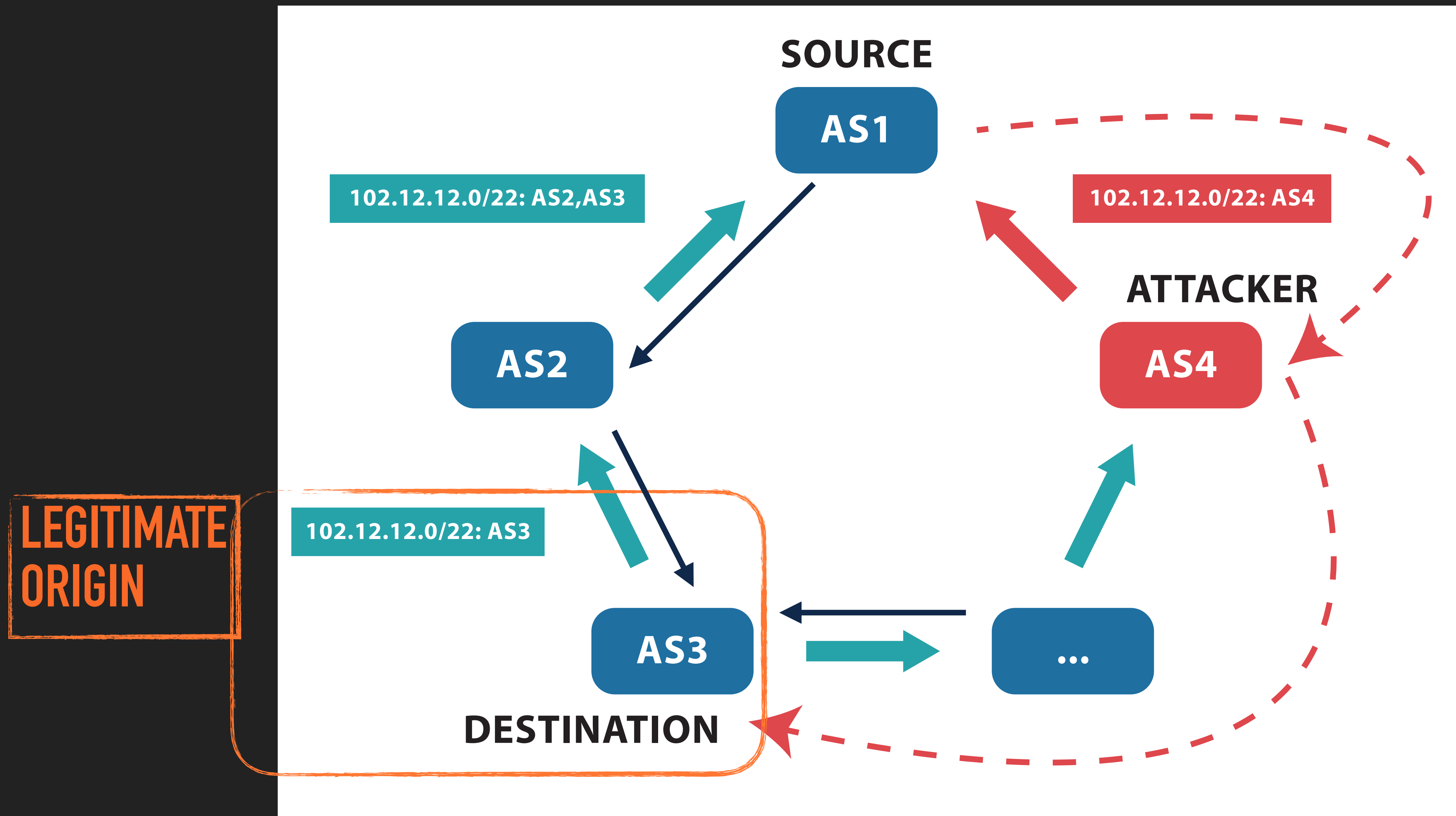
ORIGIN HIJACKS



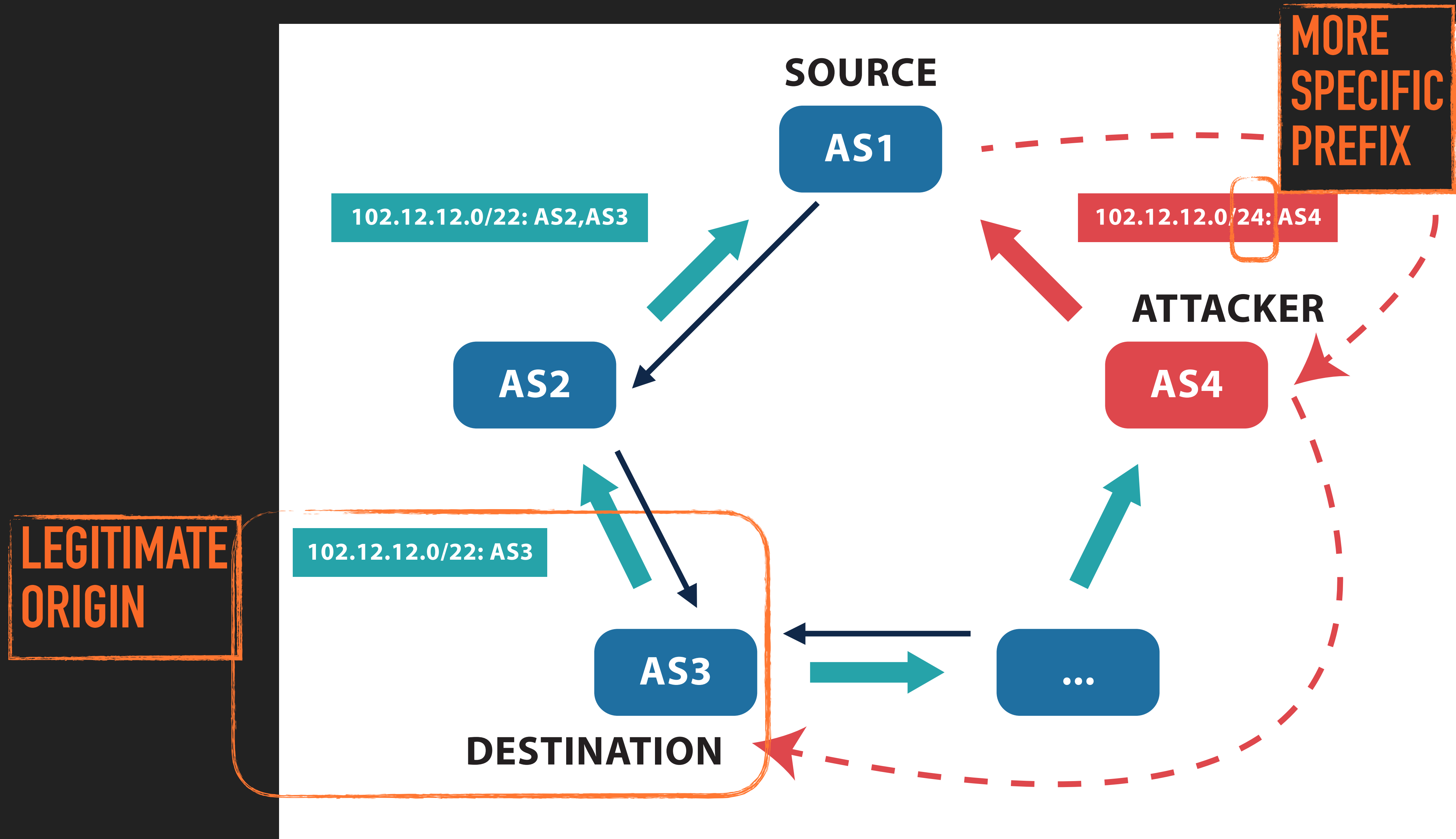
ORIGIN HIJACKS



ORIGIN HIJACKS: MOAS



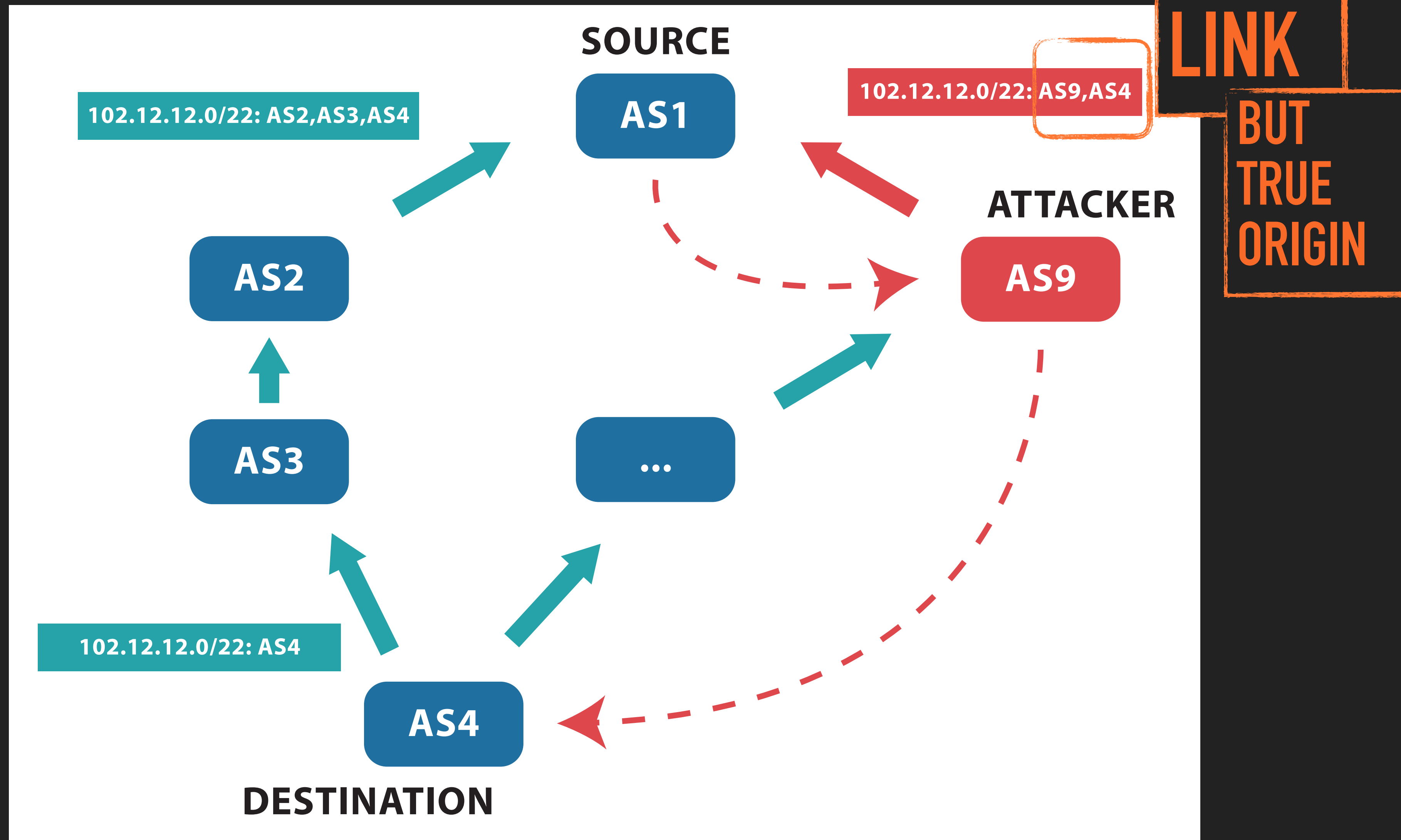
ORIGIN HIJACKS: "SUB"MOAS



#2

FAKE PATH HIJACKS

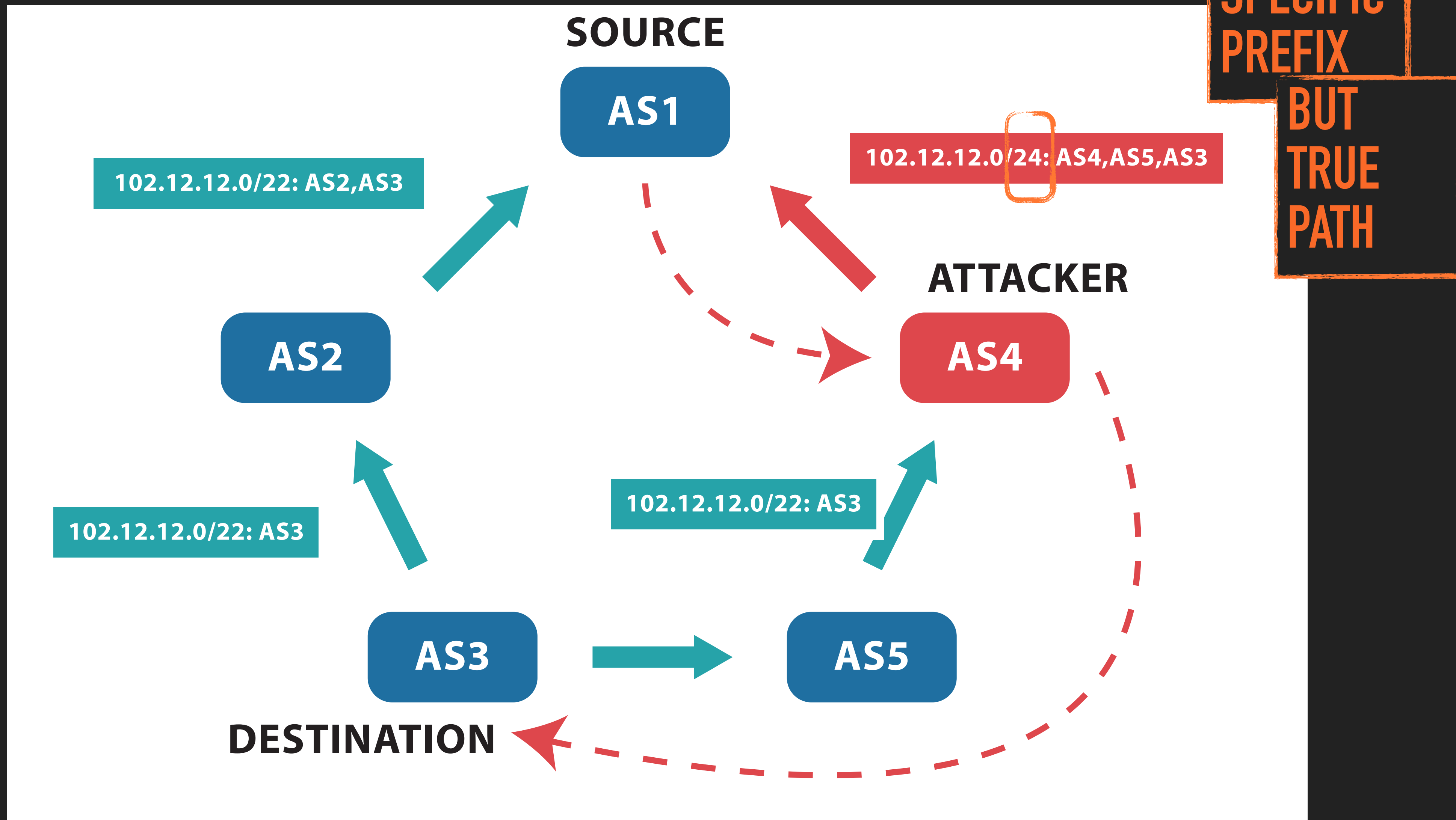
FAKE PATH HIJACKS



#3

“DEFCON #16” HIJACKS

"DEFCON #16" HIJACKS



RECAP:

“ORIGIN” (MOAS/SUBMOAS)

“FAKE PATH”

“DEFCON #16”

Prototype: Infrastructure

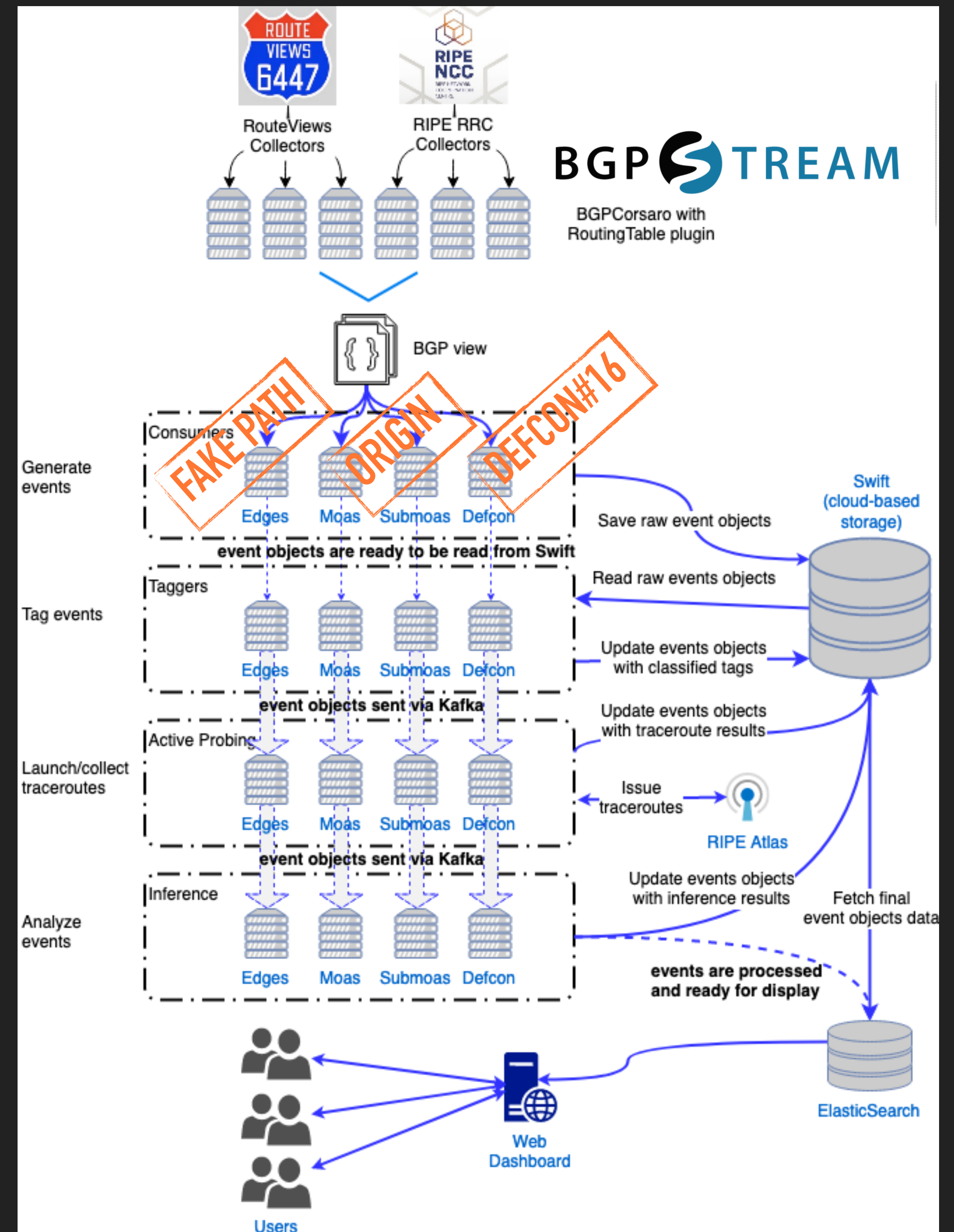
▶ Running 24/7

▶ > 300 BGP routers (RV + RIS)

▶ 5 min granularity

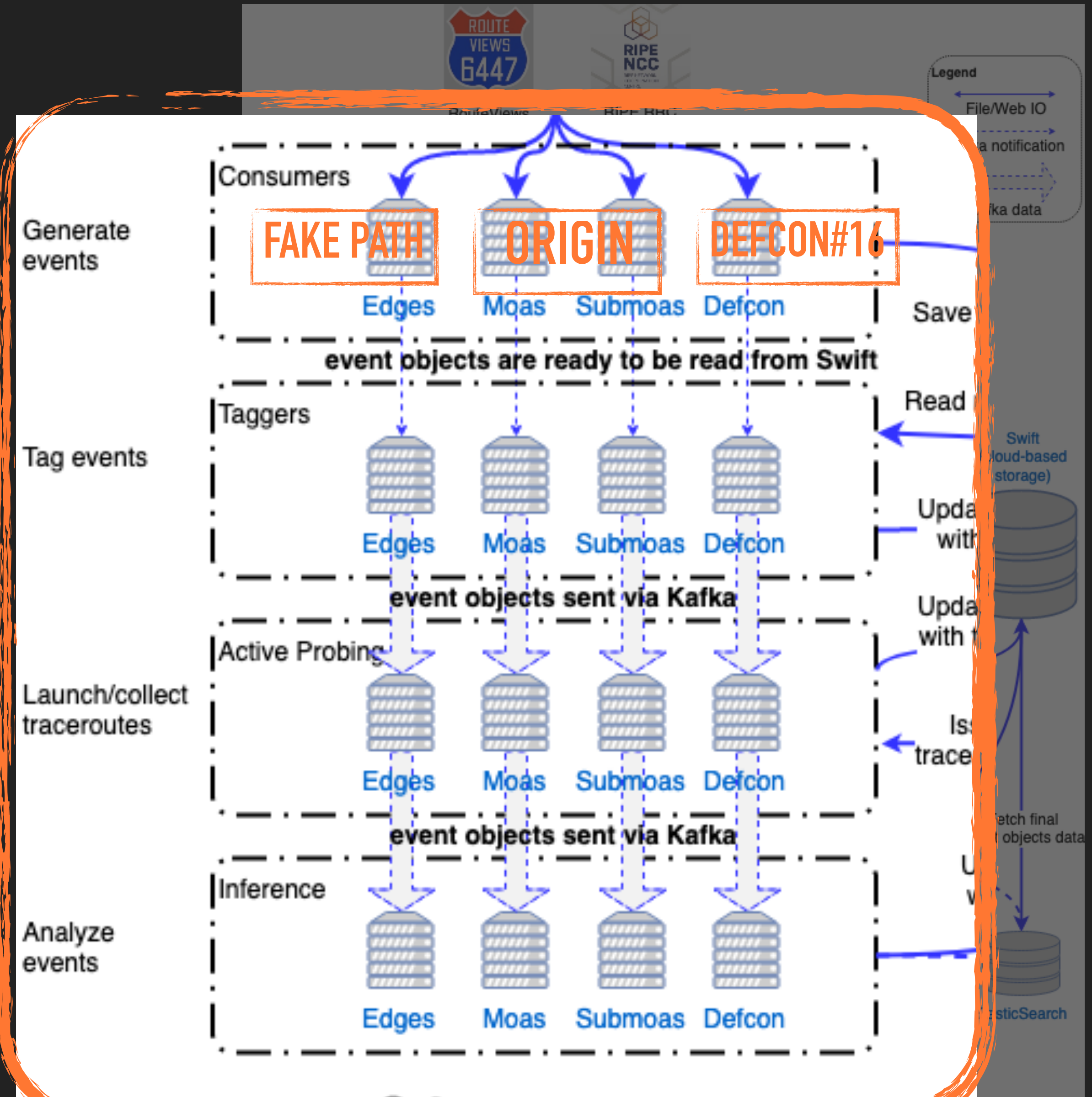
▶ ~30 min latency

▶ 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, ...

▶ ...



Correlation with other types of internet security data.

Select an event type: All MOAS Sub-MOAS New Edge Defcon

Select an event suspicion level: All Suspicious Grey Benign

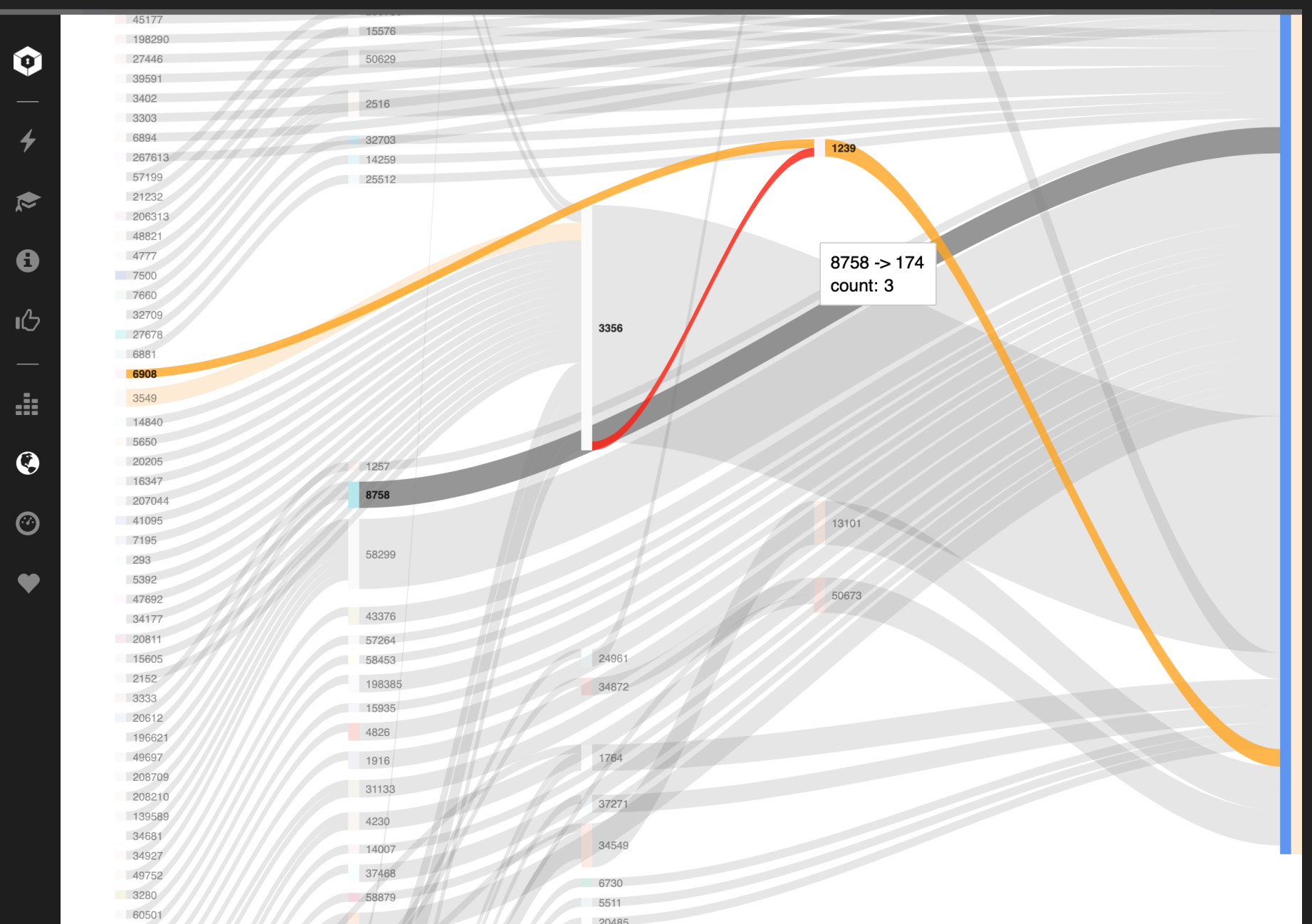
Select time period (UTC now: Feb 27, 2020 2:40 PM): Feb 26, 2020 2:40 PM - Feb 27, 2020 2:40 PM

Search for events by prefix/ASN/tags:

Events List

Potential Victims	Potential Attackers	Largest Prefix	# Prefix Events	Start Time	Duration	Suspicion Type	
AS201106 SPARTANHOST	AS7489 HOSTUS-GLOBAL-AS	202.5.31.0/24	1	2020-02-27 13:55	ongoing	80	moas
AS3302 AS-IRIDEOS-IN...NETAPP	AS34758 INTERPLANET-IT	185.103.80.0/22	1	2020-02-27 13:45	ongoing	80	moas
AS204356 HighSpeed	AS9051	185.252.103.0/24	1	2020-02-27 12:45	25 min	80	moas
AS138995 BILLY-AS-AP	AS134190 IPDC01-AS-AP	192.209.62.0/24	1	2020-02-27 11:45	ongoing	80	moas
AS1221 ASN-TELSTRA	AS38809 NXGNET-AS-AP	103.198.92.0/24	1	2020-02-27 11:25	1 hour	80	moas
AS133448 CHGPL-AS-AP	AS134190 IPDC01-AS-AP	103.101.188.0/24	1	2020-02-27 11:20	1 hour	80	moas
AS137550 POWERLINK-AS-AP	AS55406 HRCCTECH-01-AS-AP	103.112.237.0/24	1	2020-02-27 09:35	5 min	80	moas
AS210286 TEKATELECOM-AS	AS50113 SuperServersD...center	82.115.220.0/24	1	2020-02-27 09:10	ongoing	80	moas
AS12794 AKNET-AKBANK	AS18106 VIEWQWEST-SG-AP	217.169.192.0/24	1	2020-02-27 09:10	2 hour	80	moas
AS140090	AS136482 FAIRNET-AS-AP	103.148.98.0/24	1	2020-02-27 08:50	ongoing	80	moas

Rows per page: 10 1-10 of 31



THANKS



dev.hicube.caida.org/feeds
alberto@caida.org