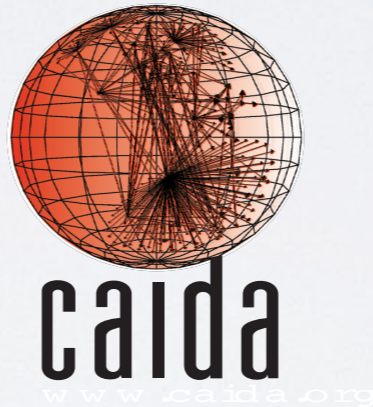


CAIDA's BGP Observatory


**Alberto Dainotti, Alistair King,
Chiara Orsini, Mingwei Zhang**
alberto@caida.org

Center for Applied Internet Data Analysis
University of California, San Diego



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

 
CSAIL

FUNDING SUPPORT

acks



NSF CNS-1423659. Aug 2014 - Jan 2019

HIJACKS - Detecting and Characterizing Internet Traffic Interception based on BGP Hijacking



DHS S&T HHSP233201600012C. May 2016 - Nov 2018

SISTER - Science of Internet Security: Technology and Experimental Research

DHS S&T FA8750-18-2-0049. Dec 2017 - Sep 2019

ASSISTS/HI-CUBE - Hub for Internet Incidents Investigation

ARTEMIS APPROACH

self-managed detection & mitigation



BAD_AS

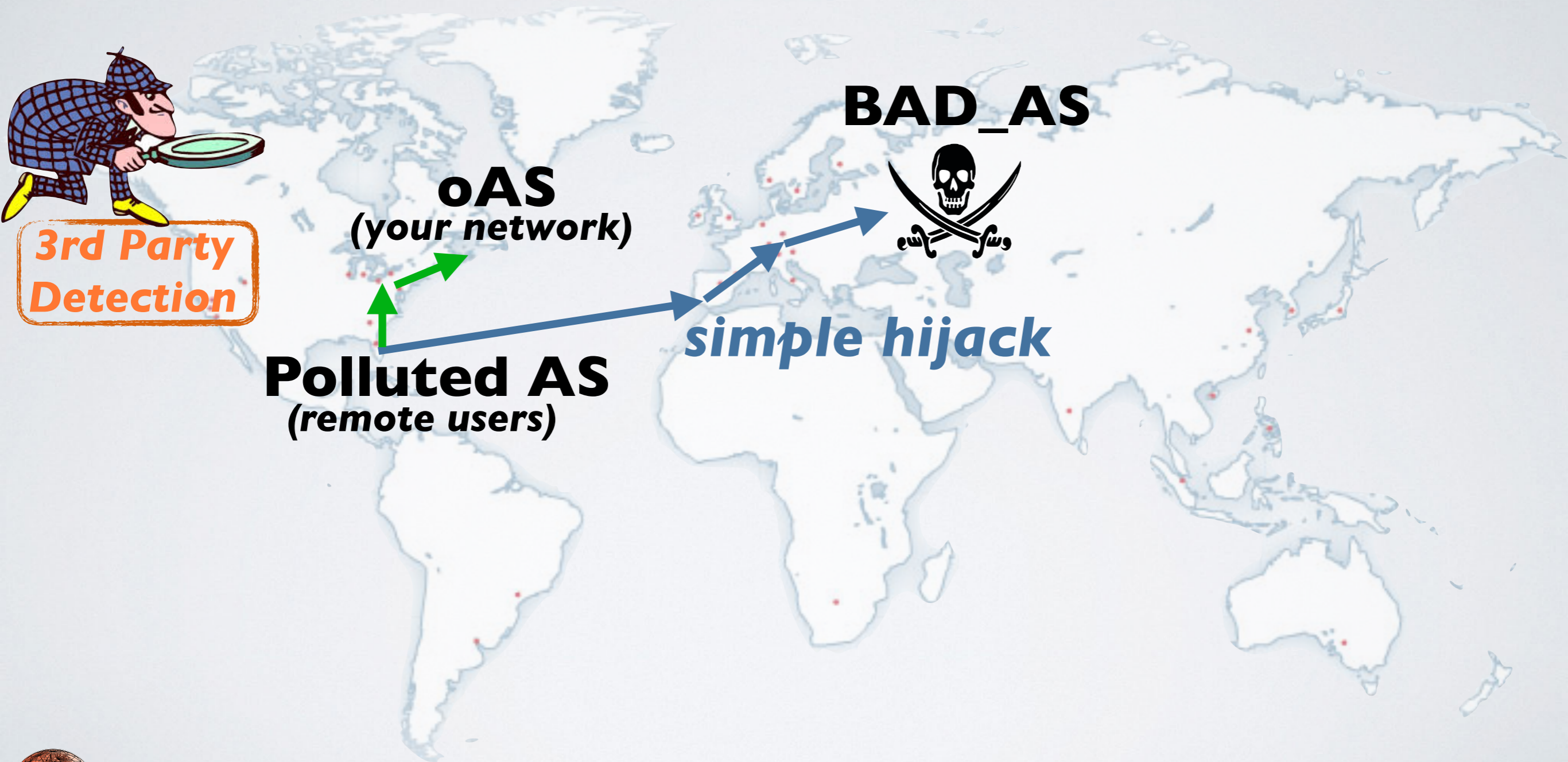


Polluted AS
(remote users)

simple hijack

DETECTION BY 3RD PARTIES

service targeting defense



A BGP OBSERVATORY *driven by scientific curiosity and experimentation*



Observatory

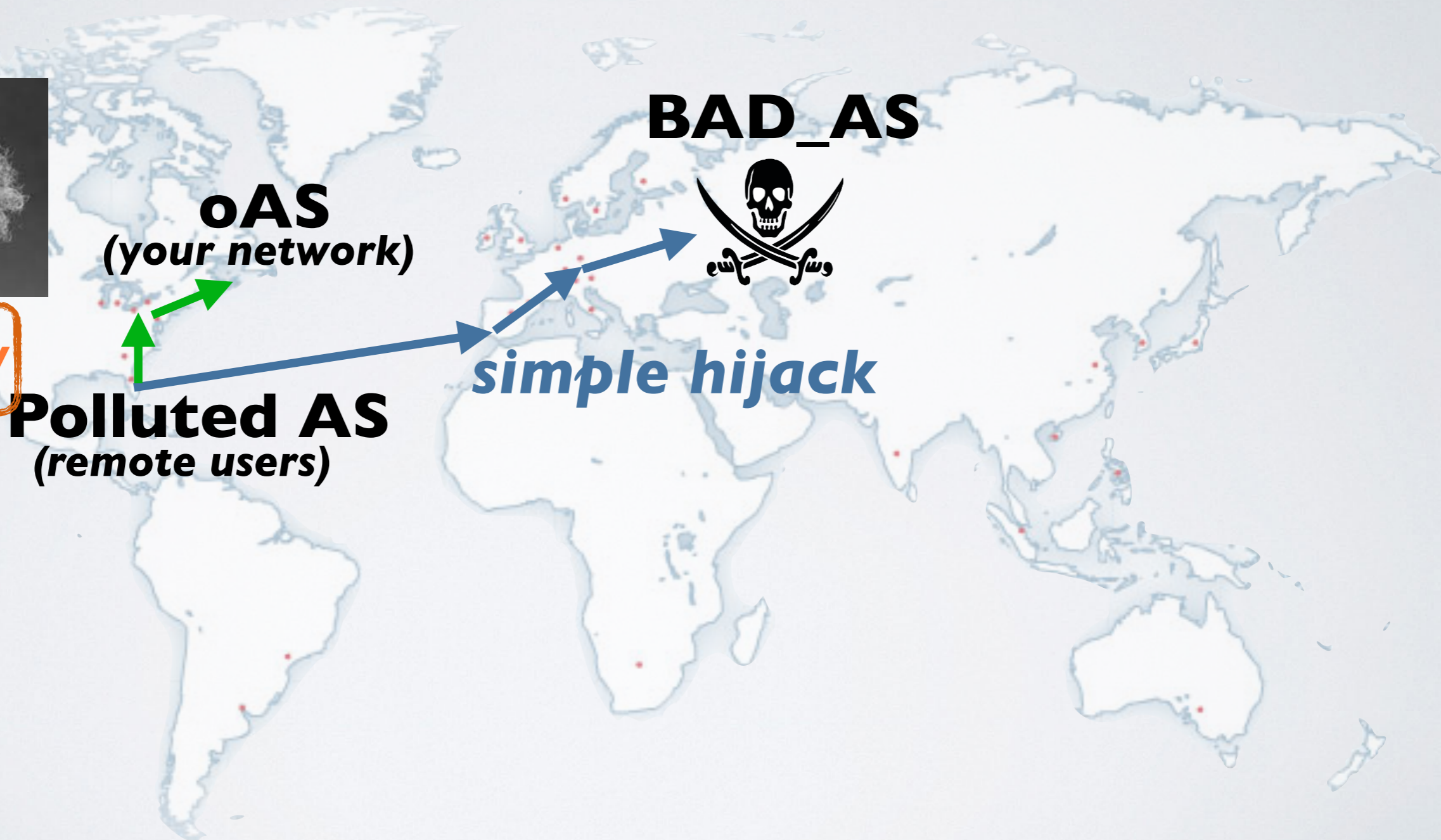


A BGP OBSERVATORY

“I’m a scientist, not a philosopher!”



Observatory



BGP OBSERVATORY



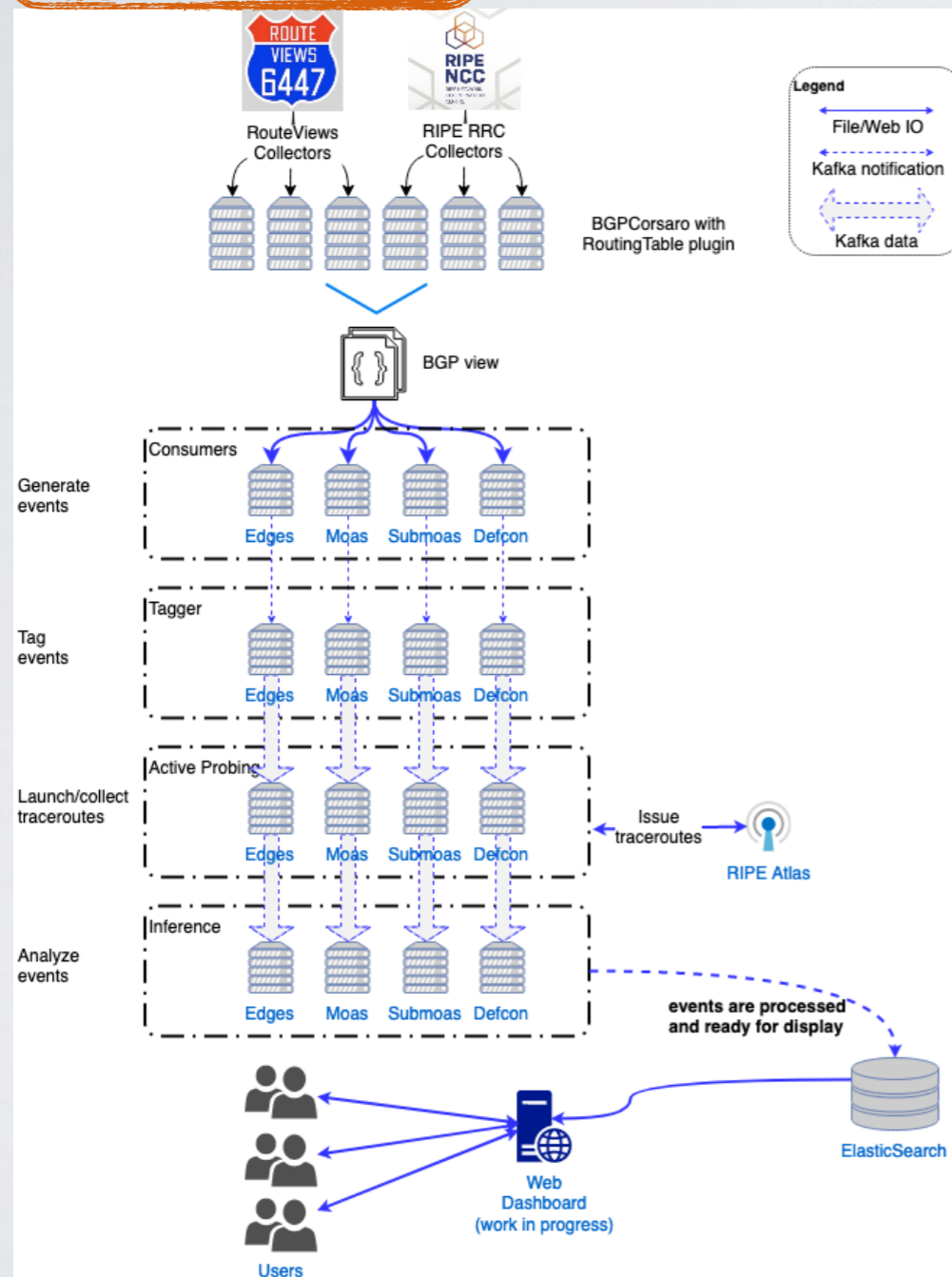
why?

- **Operators' debug tool**
- **Situational Awareness / Intelligence**
- **Research on Hijacks and BGP anomalies**
- **Testbed for developing new techniques**
- **Techniques useful when defending also from hijacks of prefixes not owned by user...**

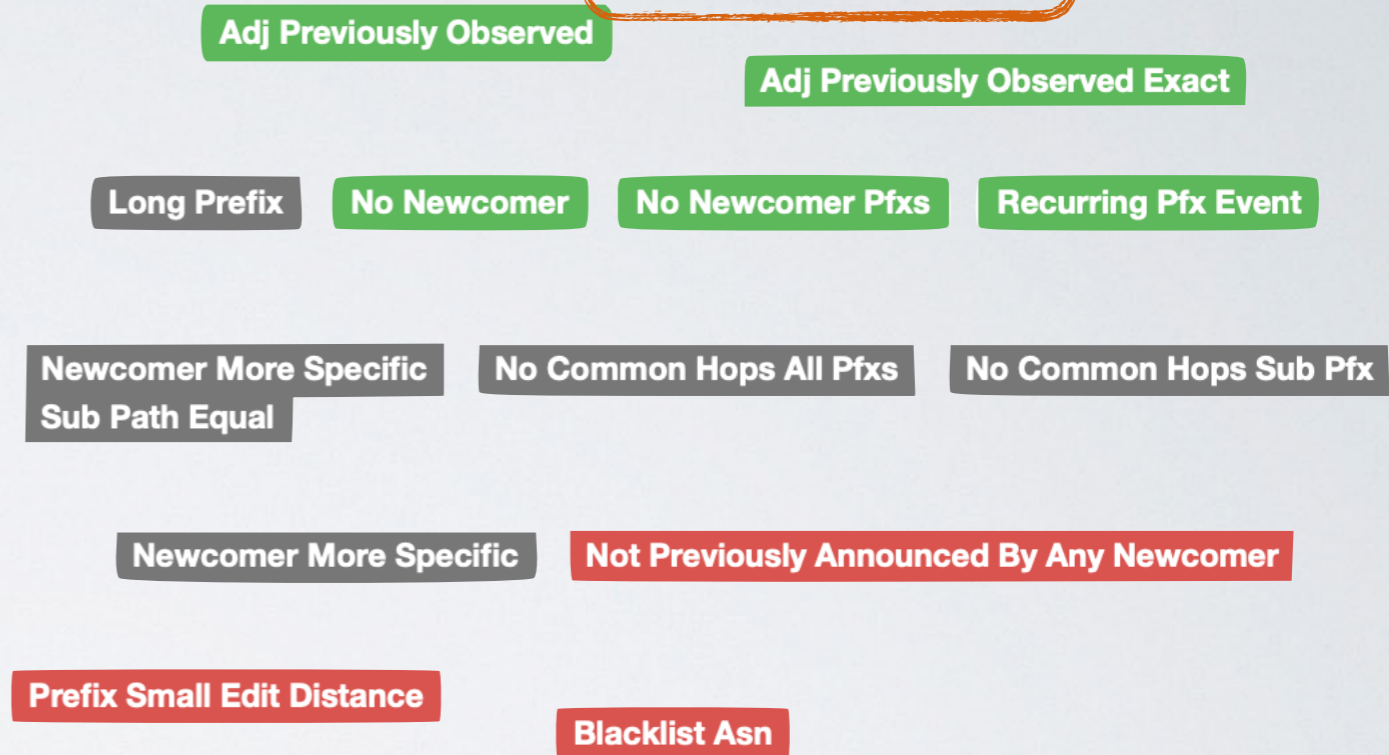
OBSERVATORY

overview

Architecture



Methods



Papers

A few papers in preparation / under submission — TMA, IMC, Usenix Security, ...

OBSERVATORY

demo

BGP Hijacks Observatory

The [BGP Hijacks Observatory](#) is a [CAIDA](#) project to detect and characterize BGP hijacking attacks, including stealthy man-in-the-middle (MiTM) Internet traffic interception attacks. The Observatory uses the [HI³ PaaS](#) offering to power its data collection and analytics platform, and provides event data to HI³ to allow correlation with other types of Internet security data.

591 Suspicious Events Today	244k Suspicious Events	27.0GB Dataset Size
61 Suspicious MOAS Events Today	7.66k Suspicious MOAS Events	12.1GB MOAS Dataset Size

Select visualization

- Event Feed
- Time Series Graphs

Select an event type

- All
- MOAS
- Sub-MOAS
- New Edge
- Defcon
- Correlate

2019-04-14T22:36-0700 - 2019-04-15T22:36-0700 Search by prefix and ASN, separate by space...

Show 10 entries

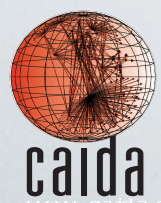
Potential Victim	Potential Attacker	Largest Prefix	# Prefix Events	Start Time	Duration	Type
zain-as	ISI-AS	197.190.0.0/16	1 pfx (65536 addrs)	2019-04-15 21:35:00	5 min	origin hijack (moas)
SOPRADO-ANY	IPHH	62.201.172.0/24	1 pfx (256 addrs)	2019-04-15 21:25:00	5 min	origin hijack (moas)
ANSASERVERS	VIRTUTEL-AS-AP	103.39.248.0/24	1 pfx (256 addrs)	2019-04-15 20:20:00	5 min	origin hijack (moas)
EZECOM-AS-AP	IPDC01-AS-AP	49.156.2.0/24	1 pfx (256 addrs)	2019-04-15 19:05:00	25 min	origin hijack (moas)
ENTEKHAB-AS	Imen_Sanat	78.111.7.0/24	1 pfx (256 addrs)	2019-04-15 18:40:00	ongoing	origin hijack (moas)
GRD	AS9051	80.79.145.0/24	7 pfxs (1792 addrs)	2019-04-15 17:00:00	15 min	origin hijack (moas)
DNIC-ASBLK-	DNIC-ASBLK-	55.192.0.0/16	1 pfx (65536 addrs)	2019-04-15 16:00:00	5 min	origin hijack (moas)

Data & Analytics provided by

CAIDA's BGP Hijacks Project



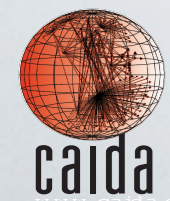
UC San Diego



WANTED / FUTURE WORK

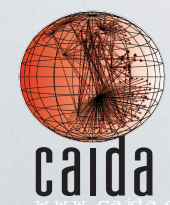


- **GT / Human in the Loop**
 - **also leveraging ARTEMIS**
- **Better data: AS Relationships, AS2Org, AStraceroute, ...**
- **Faster data: RouteViews, ...**
- **More data: more BGP monitors**



THANKS

alberto@caida.org



Center for Applied Internet Data Analysis
University of California San Diego

www.caida.org