Cybersecurity Research Acceleration Workshop and Showcase
October 18, 2017 | San Francisco, CA

ARTEMIS: Neutralizing **BGP Hijacking** within a Minute

Challenge:

Timely detect and neutralize BGP hijacking attacks *(including sophisticated attacks)*

Solution:

- Live BGP monitoring based on public infrastructure and CAIDA's *BGPStream*
- Leverage local knowledge of the network to protect
- Accurate detection rules and heuristics
- Approaches to rapidly mitigate attacks

Value proposition:

- Protect your network from hijacking and *man-in-the-middle* attacks
- No outsourcing for detection! Autonomously detect events, without sharing private info
- Flexible configuration adapts to your network needs

NSF CNS-1423659
Detecting and Characterizing Internet Traffic Interception based on BGP Hijacking

PI: Alberto Dainotti, *CAIDA, UC San Diego*
alberto@caida.org

Team:

- Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas Dimitropoulos — *FORTH / University of Crete*
- Danilo Cicalese — *Télécom ParisTech & University Pierre and Marie Curie*
- Alistair King, Jae Hyun Park — *CAIDA, UC San Diego*

What we need to TTP

- Setup *ARTEMIS* in your network (assisted pilot program)