# DDoS and Routing Security BoF

**Moderator: John Kristoff**

**<jtk@dataplane.org>**

**@jtkristoff**

FIRST 2022

# Three Themes for Today

- Unsolved **network** security problems:
  Specifically in: DDoS and BGP routing
  Others perhaps: DNS, protocol abuse, weak defaults
- CSIRT role(s) mitigating DDoS / routing issues
- Considerations for a NETSEC SIG within FIRST.org

# DDoS discussion topic examples

- DDoS info sharing, case studies, expertise
- CSIRT involvement, another group, or externally handled
- Traceback and attribution
- Monitoring tools and solutions
- Mitigation strategies
- Disclosure, reporting, and regulatory requirements

# BGP discussion topic examples

- Router system bugs, routerOS management challenges
- IP address resource management and usage monitoring
- External view of ASN/prefix expectations
- RX/TX route filtering practices
- BGP peer monitoring
- WHOIS
- IRR
- RPKI

# Possible Challenges for individual CSIRT engagement

- DDoS and routing events are sufficiently infrequent?
- Responsibility often falls to network engineering team
- CSIRT access to DDoS/BGP tools + data tend to be limited

# Why Do This in FIRST?

- Other places have done some of this, e.g.,
  - “old” FIRST, NOGs, nsp-sec, ops-trust, secret channels
  - netsec community may have splintered too much
- We already have a rich FIRST member base to draw from
  - But good opportunity to attract new netsec teams?
- FIRST org transparency, stability, and support
- Internationally diverse community
- Operational-oriented teams
- FIRST is a leading incident response authority

# What might a SIG do?  Possible ideas…

- Information sharing (e.g., mailing list, Slack, meetings)
- Maintain authoritative list of BCPs and netsec resources
- Advocacy and education (e.g., MANRS, peeringdb)
- Contribute to FIRST blog
- Training and workshops at FIRST TCs/Conferences
- Team directory extensions (e.g., assigned ASNs)
- Community tool building and monitoring services

# Next steps

- If agreed a SIG fills a need, and is of sufficient interest…
- Collect charter participant names, teams, emails
- Begin charter process
  - Outline mission/goals
  - Propose activities and deliverables
  - Propose participant requirements
  - Enumerate needs (e.g., mailing list, funds)
  - Review phase with charter members
  - Submit

# Proposed Mission

**To foster the deployment of inter-AS network security BCPs, coordinated mitigation, and information sharing.**

# Thank You!

**Shout outs to: Carlos Friacas, Aaron Kaplan, Max Stucchi, Francisco Monserrat, Shin Adachi, Merike Kaeo, Chris Butera, Brian DeWyngaert Je, Adrian Hendrik, SWITCH, and ISOC.**