DNS Abuse

An At-Large Perspective

Jonathan Zuck, NARALO/ALAC

DNS Abuse Definition

- No Accepted Definition
- Basically
  - Abuse = attacks on the DNS (ex DOS)
  - Misuse = using the DNS for attacks (ie Phishing)
- Often strays into content
- Accepted
  - Abuse
  - Malware, Phishing

CCT

- Findings
  - Safeguards did not work in 2012
  - DNS Abuse just shifted to new gTLDs
  - Central problem was the lack of a wholistic approach
- Recommendations
  - Create incentives for best practices
  - Set thresholds
  - Give new tools to Compliance

At-Large Recommendations

- Implement CCT Recommendations
- Drastically reduce bulk sales
  - Perhaps price minimum
  - Perhaps some accreditation process?

Contracted Party Concerns

- DNS Abuse Definitions can become too broad

- It's a moving target

- More "regulation" not helpful

At-Large Position

- Critical issue to Individual End Users
- More can be done in terms of best practices
- We NEED to get to BAD actors
- Compliance is the way there