DNS Ecosystem Security Efforts at ICANN

A Brief Introduction

David Conrad
CTO, ICANN

2020 FIRST Technical Colloquium, Melbourne AU
20 February 2020
ICANN’s DNS Security Efforts

- Bad guys are increasingly leveraging the DNS for attacks
  - Ubiquitous and critical functionality
  - Unfortunately easy to attack

- ICANN’s Bylaws:
  
  **ARTICLE 1 MISSION, COMMITMENTS AND CORE VALUES**

  **Section 1.1. MISSION**

  (a) The mission of the Internet Corporation for Assigned Names and Numbers ("ICANN") is to ensure the stable and secure operation of the Internet's unique identifier systems [...]
DNS Abuse Activity Reporting

- From https://www.icann.org/octo-ssr/daar

  “The overarching purpose of DAAR is to develop a robust, reliable, reproducible, and replicable methodology for analyzing security threat activity that can then be later used by the ICANN community to facilitate informed policy decisions.”

- Security threats defined to be:
  - Phishing, Malware, Botnet C&C, Spam

- Uses 14 reputation lists from 6 RBL providers
  - Abuse.ch, APWG, Malware Patrol, PhishTank, Spamhaus, SURBL

- Monthly reports going back to Jan 2018
  - All gTLDs (contractual obligation)
  - Now incorporating some ccTLDs (voluntarily)

DNS Security Facilitation Initiative

- New project created partially in response to DNSpionage, Sea Turtle, and other attacks leveraging the DNS
  - Early in project definition: we know there is an issue, we, in conjunction with the community, are trying to figure out how best to address that issue.

- Goal is to establish and promote best practices, facilitate communications between ecosystem participants, and implement processes to help the community handle threats.
  - NOT to handle incidents/threats
Summary

- ICANN’s Bylaws require us “ensure the stable and secure operation of the Internet's unique identifier systems”
- In the context of the DNS, we have two main efforts:
  - Domain Abuse Activity Reporting
    - In operation since Jan 2018
    - [https://mm.icann.org/mailman/list info/dns-abuse-measurements](https://mm.icann.org/mailman/list info/dns-abuse-measurements)
  - DNS Security Facilitation Initiative
    - Just now spinning up
- Input welcome and encouraged on both!
Thank You and Questions
Visit us at icann.org
email: david.conrad@icann.org