ICANN 75
ANNUAL GENERAL
KUALA LUMPUR

SSAC Meeting with the GNSO Council
ICANN75 | September 2022

Agenda

- **SSAC topic(s)**
  - Security Practitioners’ & DNS Operators’ Involvement at ICANN
  - Roadmap for mitigating DNS abuse
- **GNSO topic?**

Security Practitioners’ & DNS Operators’ Involvement at ICANN

Security Practitioners' Involvement at ICANN

- **No home for security practitioners within ICANN**
    - SSAC has some expertise but serves a different and broader role, GAC PSWG is law enforcement focused.
    - In general, this community does not participate in ICANN work directly, but does provide occasional comments and input from afar.
- **Security practitioners have a need to access registration data**
    - For proactive response to security threats
    - For analysis - longitudinal trends and the future
- **We are all making assumptions about what they need and why from anecdotal inputs**

DNS Operator’s Involvement at ICANN

- **Over the last decade, the DNS operation landscape has changed.**
  - DNS used to be primarily operated by registrars and ISPs
  - Over the last decade, managed DNS services (e.g., cloudflare, amazon) and global recursive resolvers (e.g., google) have become industries of their own
  - It is impacting the security and stability of the DNS
- **No home for DNS Operators within ICANN**
  - Some may be in ISPCP, others in registrar stakeholders

Roadmap for Mitigating DNS Abuse

Review of ICANN’s Strategic Plan

OBJECTIVE: Strengthen the security of the Domain Name System and the DNS Root Server System.

- **GOAL 1:** Improve the shared responsibility for upholding the security and stability of the DNS by strengthening DNS coordination in partnership with relevant stakeholders.
- **GOAL 2:** Strengthen DNS root server operations governance in coordination with the DNS root server operators.
- **GOAL 3:** Identify and mitigate security threats to the DNS through greater engagement with relevant hardware, software, and service vendors.
- **GOAL 4:** Increase the robustness of the DNS root zone key signing and distribution services and processes.

Targeted Outcomes on DNS Abuse

Strategic Goal 1: Improve the shared responsibility for upholding the security and stability of the DNS by strengthening DNS coordination in partnership with relevant stakeholders.

- **Targeted Outcomes: ICANN, in partnership with relevant stakeholders, establishes and promotes a coordinated approach to effectively identify and mitigate DNS security threats and combat DNS abuse.**

Roadmap for Mitigating DNS abuse

The ICANN Board, the SSAC and other interested community groups to work collaboratively to develop a plan to bridge the gap between ICANN’s strategic goals related to DNS abuse and activities to address specific issues and implementations.

- ICANN has a few high-level strategic goals and several specific initiatives, but no unifying roadmap to strategically address the various elements of DNS abuse.
- Recent work taken on by ICANN community members in notification and distinguishing between malicious registrations and compromised domains helpful but not a holistic approach.
- A strategic plan to mitigate DNS abuse can drive specific work and/or policy development over the course of time.

Roadmap for Mitigating DNS abuse

A strategic plan should include at least these elements:

- **Explore all aspects of mitigating DNS Abuse** including proactive prevention, detection, information sharing, effective approaches, community standards, shared expectations, and overall goals.
- **Create a consistent, consensus baseline for market participants** and a regime to measure results to ensure such a baseline is met and maintained over the long term.
- **Develop and communicate a set of processes and expectations for the anti-abuse community** to utilize in order to effectively collaborate to mitigate DNS Abuse.
- **Create a work plan with a timeline and participants from the community to meet these goals.**

Thank you