ICANN and Domain Name System (DNS) Abuse

John Crain
Chief Technology Officer

04 May 2023

ICANN operates under a set of bylaws

- These by-laws lay out the mission, commitments and core values

They guide what is developed by the community (policy), adopted by the board and implemented by the organization. (Not just on DNSAbuse)

It is good to have them in the back of your mind,

- https://www.icann.org/resources/pages/governance/bylaws-en/#article1

Multifaceted Response to DNS Abuse

- The Internet Corporation for Assigned Names and Numbers (ICANN) organization's (org) response to DNS abuse is **multifaceted**

- The ICANN org-wide program is built upon these three pillars:
  - Contributing data and expertise to fact-based discussions
  - Providing tools to the ICANN community
  - Enforcing contractual obligations with registries and registrars

Baseline for DNS Abuse

- Within ICANN, DNS abuse currently refers to these broad 5 categories of harmful activity:
  1. Botnets
  2. Malware
  3. Pharming
  4. Phishing
  5. Spam (When acting as a mechanism for delivery of the above 4 vectors)

- ICANN neither regulates online content nor has the capabilities to remove content.
  - These limitations, however, do not prohibit ICANN from studying or aiding in the mitigation of DNS abuse.

Measurement

ICANN Org Projects: DAAR

ICANN org supports technical programs to study and help combat DNS abuse.

- The Domain Abuse Activity Reporting System (DAAR) provides verifiable and reproducible data to facilitate analyses that could be useful in making informed consensus policy decisions.
- DAAR assembles a composite of the domain name reputation data that the operational security community observes, reports, and uses.
- How to join DAAR: Interested country code top-level domain (ccTLD) and generic top-level domain (gTLD) registries can make a request by sending an email to globalsupport@icann.org.

ICANN Org Projects: INFERMAL

- A new research project called **Inferential analysis of maliciously registered domains (INFERMAL)**.

  The study aims to systematically analyze the preferences of attackers and possible measures to mitigate malicious activities across top-level domains (TLDs) in a proactive way.

Mitigation

ICANN Org Projects: DNSTICR

- The Domain Name Security Threat Information Collection and Reporting (DNSTICR) project identifies domain names that appear to have been used for malicious purposes and are related to the COVID-19 pandemic or the Russia-Ukraine war.

Capacity Building

- ICANN also provides subject-matter expertise to, and participates in, various external cybersecurity groups.
- ICANN offers **capacity development and training on mitigating DNS abuse.**

Visit icann.org/octo to access the course catalogue.

Increasing Accountability

Working with gTLD Registries and Registrars

Important collaboration between the gTLD Registries and Registrars Stakeholder Groups (RySG and RrSG) and ICANN to help address DNS abuse in a tangible way.

By creating clear contractual obligations for registries and registrars to mitigate and or disrupt DNS Abuse.

Increasing Accountability: Expected Timeline

- Jan –May 2023: ICANN org + working group have negotiated to define potential changes to the agreement.
- May-–July 2023: ICANN will publish the negotiated amendments on icann.org website for Public Comment
- July–September 2023: ICANN org + working group will consider the Public Comments and finalize an amendment proposal.
- October–December 2023: An amendment is provided to Registry Operators (ROs) and/or Registrars (Rrs) for approval by vote. A super majority of all the respective registries or registrars must approve the proposed amendment. The voting period will be open for 60 days. ICANN and the Contracted Party House (CPH) may mutually agree to extend the voting period up to an additional 60 calendar days beyond the first 60 calendar days.

Enforcement

- ICANN enforces, to the fullest extent possible, the existing contractual obligations related to DNS abuse.
- Enforcement actions arise from investigations resulting from external complaints, proactive monitoring, and audit-related activities.
- ICANN's Contractual Compliance team regularly publishes metrics and reports on complaints received and their resolution.

→ **Complaints can be filed at https://www.icann.org/compliance/complaint**

Call to Action: ICANN Community Efforts

- ICANN org continues to believe the ICANN community is best positioned to determine what policy recommendations, if any, may be needed to mitigate DNS abuse.

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg