ICANN's Efforts in Response to Domain Name System (DNS) Abuse

Athena Foo
Stakeholder Engagement Manager - APAC

30 June 2023

ICANN

Baseline for DNS Abuse

Within ICANN, DNS abuse refers to these broad 5 categories of harmful activity:

1. **Botnets**
2. **Malware**
3. **Pharming**
4. **Phishing**
5. **Spam** when used as a vector for one or more of the other four types of DNS abuse

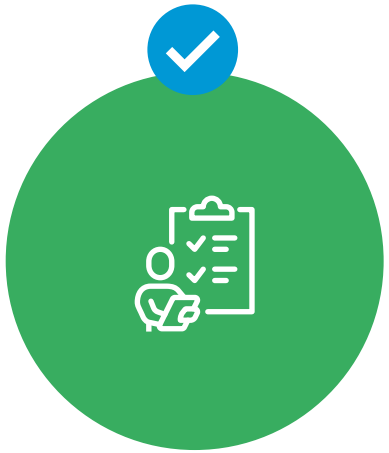
ICANN neither regulates online content nor has the capabilities to remove content. These limitations, however, do not prohibit ICANN from studying or aiding in the mitigation of DNS abuse.

Multifaceted Response to DNS Abuse

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

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) registries can make a request by sending an email to globalsupport@icann.org.

Analysis

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.

ICANN sends well evidenced reports of abuse to Sponsoring Registrar.

Capacity Building

ICANN offers **capacity development and training on mitigating DNS abuse**

ICANN also provides subject-matter expertise to, and participates in, various external cybersecurity groups

Visit icann.org/octo to access the course catalogue

Increasing Accountability

Collaboration 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: Target Timeline

ICANN org and contracted party working group negotiating potential changes to the base Registry Agreement and Registrar Accreditation Agreement to create specific obligations concerning DNS Abuse

ICANN will publish the negotiated amendments on icann.org website for Public Comment

ICANN org + working group will consider the Public Comments and finalize an amendment proposal

An amendment is provided to Registry Operators (ROs) and/or Registrars (Rrs) for approval by vote

Board consideration

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

What Do I Do if I Encounter DNS Abuse?

Registrars Best Practices for DNS Abuse Reporting

Before notifying the registrar please determine:

Where the issue ocurred?

What happened?

Who the reporter is?

Call to Action: ICANN Community Efforts

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

ICANN

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