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

Mert Saka
GDD Accounts Sr. Manager
ICANN

25 May 2024

Multifaceted Response to DNS Abuse

The ICANN org-wide program is built on 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 refers to these 5 broad 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.

Measurement

ICANN Org Projects: ICANN Domain Metrica

ICANN org supports technical programs to study and measure DNS abuse.

- At the end of February 2024, ICANN announced a new project and platform called ICANN Domain Metrica. Planned for launch in Q3 2024.
- This new system will provide a place to store, combine, and compare any metadata related to domain names. The platform will have a dynamic dashboard with relevant statistics and visuals.
- Domain Metrica will be modular, which means different information pieces about domain names will be added over time.
- The first module will include aggregated and non-aggregated data on DNS abuse concentrations as listed on a set of Reputation Block Lists, for both registrars and registries.
- This should give users access to more detailed and relevant information about DNS abuse concentration patterns.

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.

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

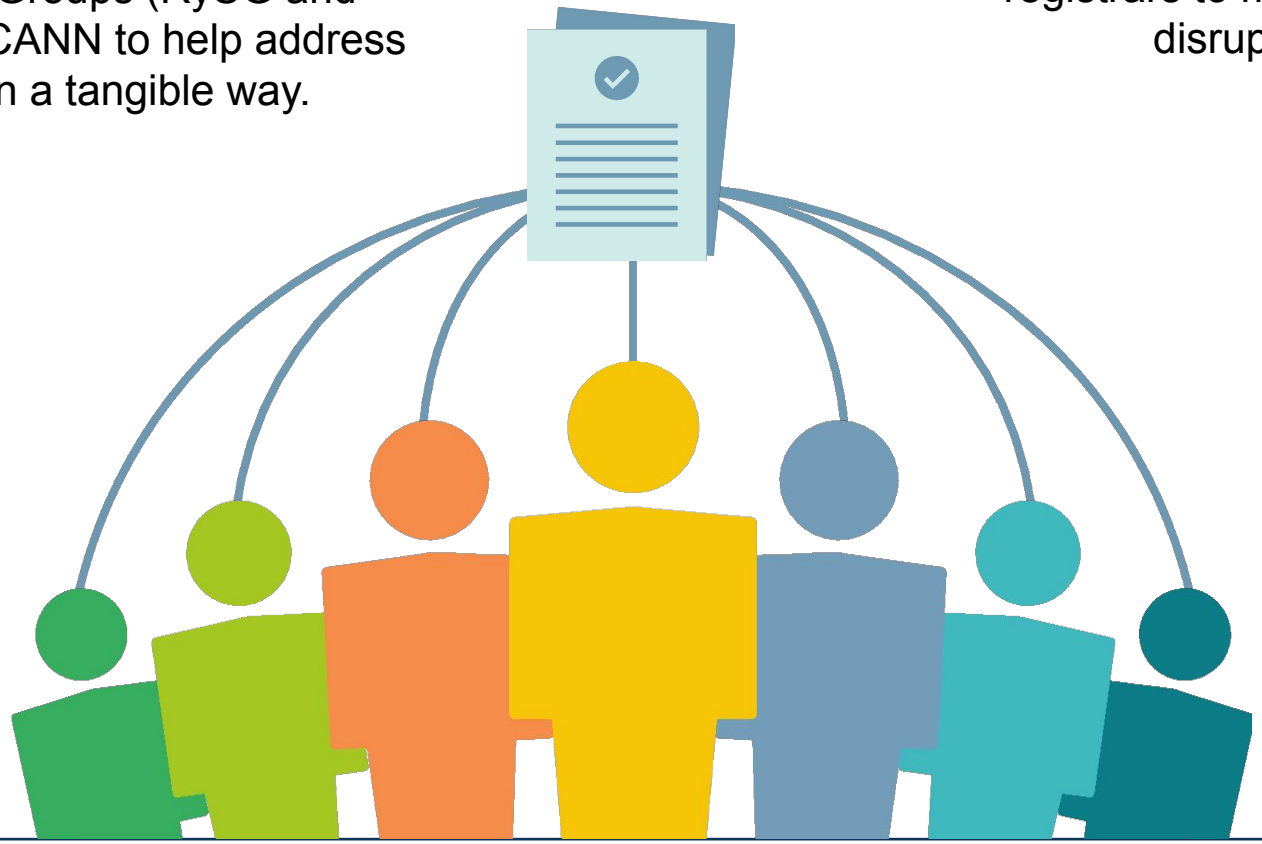
Visit icann.org/octo to access the course catalogue

Increasing Accountability

Collaboration with gTLD Registries and Registrars

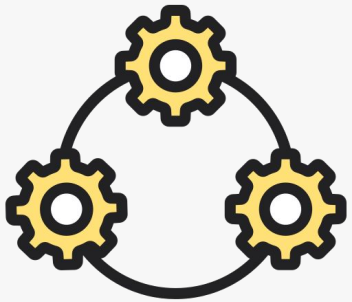
Important collaboration between the gTLD Registries and Registrars Stakeholder Groups (RySG and RrSG) and ICANN to help address DNS abuse in a tangible way.

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



Guiding Principles of the Resulting Amendments

- DNS abuse defined as phishing, malware, botnets, pharming, spam as a vector.
- Focus on the target outcome of stopping or disrupting the use of gTLD names for DNS abuse.
- Registrars and registries must take prompt action to mitigate domain names that are being used for DNS abuse.
- DNS abuse is highly contextual: the circumstances of each case are critical to determining the best approach to mitigate.
- Registrars and registries need discretion when taking action
  - Proportionality and collateral damage must be taken into consideration.
- Recognize the different roles between registrars and registries.



Amendments: Why is it important?

- This is about a safer Internet for everyone.
- Demonstrates responsibility and accountability by registrars, registries and ICANN.
- Raises the floor of what is acceptable and expected.
- Addresses the community's desire for more action and obligations for mitigating DNS abuse by registries and registrars and for ICANN to hold them accountable for mitigating DNS abuse.
- Sets up community discussions for what else is needed to further combat DNS abuse.
- Demonstrates that the multistakeholder model works and we can deliver!

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

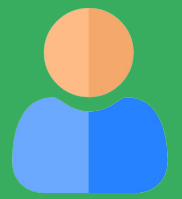
What Do I Do if I Encounter DNS Abuse?

Registrars Best Practices for DNS Abuse Reporting

Before notifying the registrar please determine:

Where the issue occurred?

What happened?



Who the reporter is?

What Do I Do if I Encounter DNS Abuse?

DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries

Prevention

Mitigation

Remediation

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

One World, One Internet

Thank you **and questions**

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg