DNS Abuse

5 November 2019

Session 1/2

ICANN | GAC
Governmental Advisory Committee

ICANN

ICANN66 - GAC Plenary Meeting - Agenda Item 21

DNS Abuse Remains #1 Public Safety Priority

- **Permanent and growing threat**
  - Global cost of cybercrime growing exponentially
  - Notable increase in circulation of CSAM Content
- **Compounded by impediments on WHOIS, a key tool in addressing DNS Abuse**
  - unavailability of contact information in gTLD Registration Data
  - failure of the reasonable access requirement to meet the needs of law enforcement and other legitimate requestors of data
  - No clear prospect of an access model to non public data

Definitions Already Exist

- **GAC Beijing Advice (11 April 2013)**

  3. Security checks— While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate ***security threats, such as pharming, phishing, malware, and botnets.*** *If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.*

  ○ Incorporated in **ICANN's Registry Agreements**

  ○ ICANN's **Domain Abuse Activity Reporting** Tool (DAAR) tracks "Phishing, Malware, Botnet command-and-control & Spam"

Definitions Already Exist

- **Competition, Consumer Trust and Consumer Choice Review** (8 September 2018)
  - DNS Abuse as "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names."
  - DNS Security Abuse: more technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse.

- **Internet & Jurisdiction Policy Network** Operational Approaches (April 2019)
  - Technical Abuses: Spam, Malware, Phishing, Botnets, Fast-flux hosting
  - Website Content Abuses: CSAM, Controlled substances, violent extremist content, Intellectual Property Infrigement
  - Action at the DNS level may be justified against both types of Abuse with higher threshold for Content Abuses

What Contracted Parties Can Do

- **Reactive Measures** at the DNS Level available to Registries
  - Deleting the domain
  - Suspending the domain (will not resolve anymore)
  - Lock the domain (no more changes possible)
  - Transfer domain or redirect services (allowing investigations)

- **Preventative Measures** are available to Registries and Registrars
  - Identity verification
  - Pre-emptive blocking of registrations based on patterns recognition (homoglyph, DGA, bulk) and predictive approaches
  - Registration and pricing policies influence levels of abuse

- **Cooperative Approaches** can be effective
  - Financial incentive by Registries to reward safe Registrars
  - Trusted Notifiers Programs

- **Egregious Content** can be addressed at DNS Level

What ICANN Can Do

- **Implementation of CCT Recommendations**
  - Incentivize the adoption of proactive anti-abuse measures (Rec. 14)
  - Contractual provisions aimed at preventing systemic use of specific registrars or registries (Rec. 15)
  - Thresholds of abuse at which compliance inquiries are automatically triggered (Rec. 15)
  - Publication of entire chain of ownership (Rec. 17)
- **Contract Negotiations**
  - Upon renewals of legacy gTLD and existing New gTLD Contracts
  - Registry Agreements for subsequent rounds of New gTLDs
  - Registrar Agreements
- **Enforcement of existing requirements**
  - Example: Failure of Reasonable Access requirement
  - Targeted Audits
    - Follow-up on Registries audit expected
    - Start of Registrars audit delayed
  - Close the compliance process loophole (3 strikes)
- **More detailed Domain Activity Abuse Reporting (DAAR) data to be made available to the public**

What the GAC Can Do

- Follow-up on the consideration and implementation of CCT Review Recommendations
- Continue to assess effectiveness of previous GAC Advice in Q&A (per Hyderabad and Copenhagen Communiqué)
- Identify and Promote ccTLD Best Practices
- Work with other stakeholders on proposals (SSAC, BC, etc.)
- Report Non-Compliance with Reasonable Access

ICANN66 Leadership Proposal for GAC Action

1. **Clarify what constitutes DNS Abuse for the GAC** in relation to ICANN's mission, consistent with GAC Beijing Communiqué (11 April 2013) and CCT Review Team's definition of both DNS Abuse and DNS Security Abuse
2. **Consider accepted best practices regarding proactive anti-abuse measures** by domain name registries and registrars, across both the ccTLDs and gTLDs space, with a view to define and promote elevated contractual standards
3. **Review actions taken to date on the CCT Review Recommendations** related to DNS Abuse (Recommendations 14 to 19), including their consideration by the ICANN Board

Next Steps at ICANN66

Meeting with the ICANN Board - Tue. 5 Nov. 15:15

As it sets out to implement new strategic objectives relating to DNS Abuse, can the Board elaborate on the operational steps it intends to take to:

1. promote "*a coordinated approach to effectively identify and mitigate DNS security threats and combat DNS abuse*" ?
2. maintain itself as a "*source of unbiased, reliable, and factual information on DNS health"* ?

   In particularly does ICANN intend to take steps to:

   a. increase transparency about actors responsible for systemic abuse (especially in connection with DAAR and ICANN Compliance complaints and dispositions)?
   b. convene relevant stakeholders for discussions on new contractual provisions in ICANN's contracts, consistent with the relevant CCT Review Recommendations?

Cross Community Session on DNS Abuse - Wed. 6 Nov. 10:30

GAC Plenary Discussion on DNS Abuse 2/2 - Wed. 6 Nov. 13:30