ICANN 65
POLICY FORUM
MARRAKECH
24–27 June 2019

DNS Abuse Mitigation

25 June 2018

ICANN | GAC
Governmental Advisory Committee

ICANN

ICANN65 - GAC Plenary - Agenda Item 5.1

Agenda

1. What is DNS Abuse?
2. Why should we care?
3. What Are The Applicable ICANN Policies?
    - *ICANN Contractual Compliance and Consumer Safeguards Presentation*
4. What Can Registries and Registrars do to better prevent DNS Abuse?
5. What can ICANN org and Community Do?

Definition of DNS Abuse

No specific definition contained in ICANN Bylaws or contracts

CCT Review Deliberations and Recommendations

- ICANN Report on New gTLD Program Safeguards to Mitigate DNS Abuse (18 July 2016): "*Intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names.*"
- CCT Review Final Report, p.88 (8 September 2018)
  - CCT Review Consensus on what constitutes '*DNS Security Abuse*' or '*DNS Security Abuse of DNS infrastructure*'
  - Understood as including "*more technical forms of malicious activity*", such as malware, phishing, and botnets, as well as spam "*when used as a delivery method for other forms of abuse*."

GAC Safeguards Advice

- GAC Beijing Communiqué (11 April 2013)
- Safeguards Applicable to all New gTLDs

  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.*

DNS Abuse - Impact and Status Quo

Why should we care?

- Example: Business Email Compromise
- Key Investigative Needs: Attribution & Notification of Victims (Reverse WHOIS query)
- Key tool: Accuracy of WHOIS Data

What Are The Applicable ICANN Policies?

- *ICANN Contractual Compliance and Consumer Safeguards Presentation*

Past work of the GAC with the Community

- Security Framework

DNS Abuse - Prevention and Mitigation

What Can Registries and Registrars do to better prevent DNS Abuse?

- CCT Review Team recommendations
  - Incentivize the adoption of proactive anti-abuse measures (Recommendation 14)
  - Prevent systemic use of specific registrars or registries for DNS Security Abuse (Recommendation 15)
- Pricing policies correlate to DNS Abuse
- Some Privacy/Proxy Services enable DNS Abuse
- Validation of contact information deters DNS Abuse (.DK Example)

What can ICANN org and Community Do?

- RDS Data Accuracy (Across Field Address Validation, EPDP Phase 2)
- Privacy/Proxy Accreditation Policy Implementation vs. EPDP
- Implementation of CCT Review recommendations
- Leveraging Domain Abuse Activity Reporting (DAAR) data

Possible Next Steps for the GAC

Follow-up on previous GAC Advice

- GAC Hyderabad Communiqué (8 November 2016)
  - GAC Advice to provide responses to questions listed in Annex 1
  - Annex 1 - Questions to the ICANN Board on DNS Abuse Mitigation by ICANN and Contracted Parties
- GAC Copenhagen Communiqué (15 March 2017)
- ICANN Org draft responses (30 May 2017) for further discussion

Follow-up on Implementation of CCT Review Recommendations

- GAC Kobe Communiqué (14 March 2019)

  The GAC notes with concern the recent Board resolution in response to the Final Recommendations of the Competition, Consumer Trust and Consumer Choice Review Team, which approved only 6 of 35 consensus recommendations.

  a. The GAC advises the Board to:

  i. Promptly meet with the CCT Review Team leadership to discuss the Board's resolution

  ii. Possibly reconsider certain decisions on recommendations if appropriate.

Continue community discussion: consider cross-community session at ICANN66