DNS Abuse Mitigation

GAC PSWG Speakers:
Laureen Kapin (US Federal Trade Commission, Co-Chair GAC PSWG)
Gabriel Andrews (US Federal Bureau of Investigation)

GAC Speaker:
Masamichi Takeda (Japan, Ministry of Internal Affairs and Communications)

ICANN72

25 October 2021

ICANN | GAC
Governmental Advisory Committee

Agenda

1. **Why DNS Abuse is Important to the GAC**
   - Cybercrime facilitated by domain name system abuse causes harms
   - Identified as priority by GAC and other SG's
2. **Recent Developments**
   - Studies
   - Registrar Audit
   - SSAC Interoperable Approach to Abuse Handling
   - Board Scorecard on Security and Stability Review Team Recommendations
   - Voluntary Initiatives
   - Board Informational session on DNS Abuse
3. **Presentation and proposal by Japan on Registrar Hoping**
4. **ICANN72 Objectives**

DNS Abuse Mitigation: Background

Why this is important for the GAC?

- **Cybercrime surging and components of cybercrime are fueled by DNS Abuse**
  - frequency and severity of cybercrime attacks across the globe rose steeply in 2020
  - "If impact of cybercrime were measured in the same way as we measure the gross domestic product (GDP) of nations, then with a value of $6 trillion it would be the third largest economy, after the US and China." (VISA)
- DNS Abuse constitutes:
  - **A threat to consumers and Internet users (individual and commercial) and their trust in the DNS**
  - **A threat to the security, stability and resiliency of the DNS and its Infrastructure**

What is DNS Abuse?

- Security Threats such as *Phishing, Malware, Botnets* (GAC Beijing Safeguard Advice) and as "*intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names*" (CCT Review definition quoted in the GAC Statement on DNS Abuse, 18 Sep. 2019)

The GAC, the GAC Public Safety Working Group and **many ICANN stakeholder groups prioritize curbing DNS Abuse**, recognizing in particular that **current ICANN contracts do not provide sufficiently clear and enforceable obligations** to mitigate threats to the DNS and its infrastructure and need to be improved. This is has been evidenced in:

- Community discussions with - and statements from - ICANN Contractual Compliance
- Board correspondence (in particular with the Business Constituency in 2020/2019, see 12 Feb. 2020)
- GAC Inputs in Reviews (CCT, RDS-WHOIS2, SSR2) and in GNSO PDPs (New gTLD Subsequent Procedures)

DNS Abuse Mitigation: ICANN's Role and Contracts

What is ICANN's role?

- **Defined in Articles of Incorporation, Bylaws and Contracts with Registries/Registrars**
  - Not-for-profit public benefit corporation, promoting the global public interest in the operational stability of the Internet
  - Mission: ensure the stable and secure operation of the Internet's unique identifier systems
  - May negotiate, enter into and enforce agreements, including public interest commitments, with any party in service of its Mission
  - Commits to duly taking into account the public policy advice of governments and other public authorities
- **Current contracts:**
  - ICANN's standard Registry Agreement required new gTLD registry operators to include provisions in their Registry-Registrar Agreements (RRA) that prohibited registrants from:
    - distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law
      - but need more than obligations to include language in downstream contracts; need required consequences for breach
  - Registry Operators must "periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, **such as** pharming, phishing, malware, and botnets."
    - but what needs to happen next?
  - ICANN's standard contract for Registrars requires registrars to promptly "investigate and respond appropriately to any reports of abuse"
    - Board 2/20 letter: "The RAA does not define, with any specificity, what "reasonable and prompt steps to investigate and respond appropriately" means.

DNS Abuse Mitigation: Recent Developments

Recent developments underscore the need for improved contracts

- ICANN released the results of its **Audit of Registrars' Compliance with DNS Abuse Obligations** (24 August 2021)
  - ICANN Compliance selected registrars with at least five domains listed as DNS security threats by the 2019 Registry Operator Compliance Audit program and/or the November 2020 ICANN Office of the Chief Technology Officer (OCTO) Abuse Report.
  - Findings:
    - 126 registrars audited (managing over 90% of all registered domains in gTLDs)
    - 111 registrars required follow-up for potential noncompliance (deficiencies)
    - 92 registrars took actions to become fully compliant, 19 currently implementing changes
  - Common reasons for noncompliance were listed in the report as:
    - Registrar websites were missing abuse tracking procedures;
    - Abuse phone lines not being made available to the public (or not responsive);
    - Abuse phone lines for Law Enforcement use not being responsive;
    - or Websites missing abuse handling procedures entirely.

DNS Abuse Mitigation: Recent Developments

Recent developments in the DNS Abuse Conversation

- Board Responds to the **Stability, Security, & Resiliency Report (SSR2)** Recommendations
  - The ICANN Board in July 2021 responded (scorecard / blog) to the SSR2 Review Team's 63 Final Recommendations (25 Jan. 2021).
  - Recommendation Groups 8-15 had particular relevance to DNS Abuse issues
    - 8.1: " *ICANN org should commission a negotiating team that includes abuse and security experts...*"
      - ***Rejected:*** *" **The Board notes that ICANN org negotiates in the broader interest of ICANN, including the public interest"***
    - 9.4: "*ICANN org should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts."*
      - ***Rejected***: "*The Board accepts in principle the idea of improving the tools that the ICANN org Contractual Compliance team has available to it in order to enforce policies that have been adopted by the community. However,* ***the Board cannot approve the part of the recommendation that contemplates "measures that would require changes to the contracts"*** *as such changes cannot be undertaken by either the Board or ICANN org unilaterally."*
        - The Board appears unwilling to "contemplate" informing Org's negotiation team of contractual tools to address security threats in the DNS.

DNS Abuse Mitigation: Recent Developments

Recent Developments in the DNS Abuse Conversation

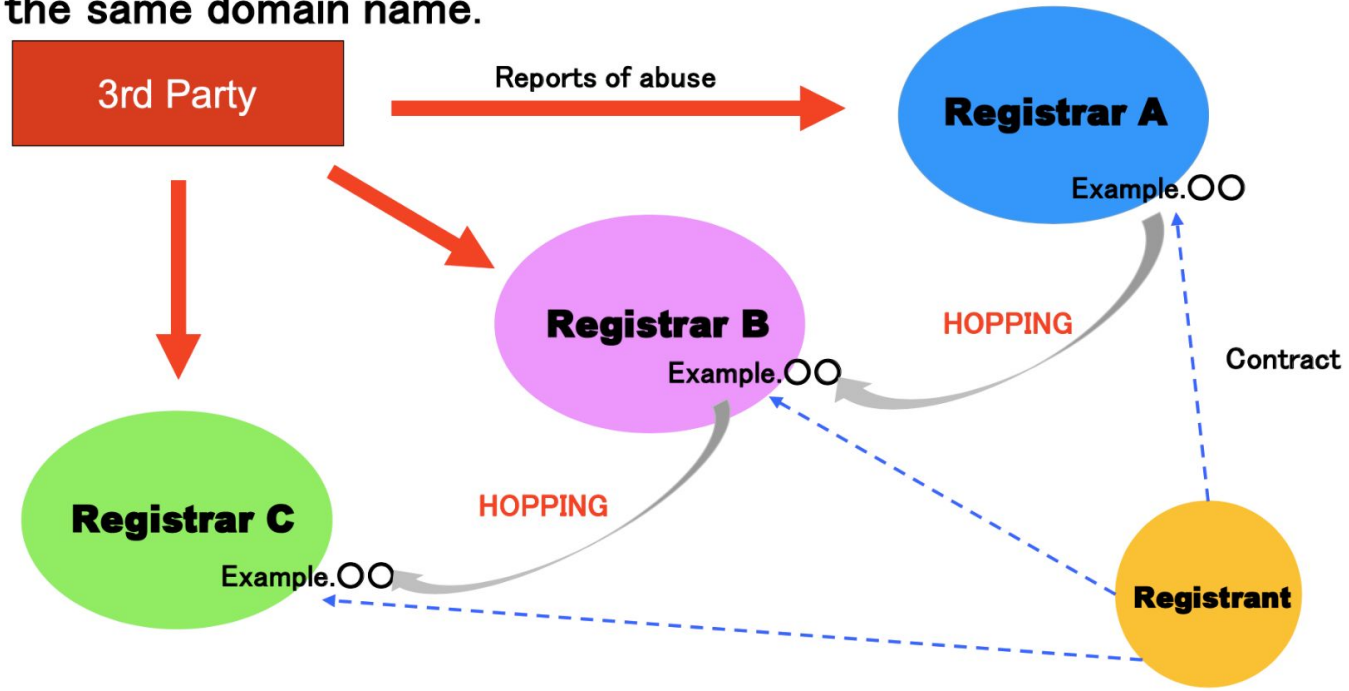
- Publications:
  - Phishing Landscape 2021, An Annual Study of the Scope and Distribution of Phishing
    - Interisle Consulting Group, 2021 September 22, link
  - Domain Name System Security Facilitation Initiative Technical Study Group (DSFI-TSG)
    - Commissioned by ICANN CEO *"in response to significant attacks on the Domain Name System (DNS), such as the Sea Turtle hijacking and the DNSpionage"*, 2021 October 15, link
- Conversations:
  - Board Informational Session on DNS Abuse (Link to recording not yet available)
  - GNSO's Registration Data Accuracy Scoping Team
    - Accuracy of registrant information is a key component in combating DNS abuse
      - Identification of Subjects
      - Victim Notification
      - Dissuading abuse before it happens
  - Common Abuse Reporting Platform
    - SSAC 115 suggested similar w their Common Abuse Facilitator

Presentation by Japan

1. Overview of Registrar Hopping

0

- **Registrar Hopping** is a case that a domain name is transferred to another registrar every time a third party reports the domain name for abuse.
- We think the purpose of **Registrar Hopping** is to prevent registrars from identifying the identity of registrants and suspending them from using domain name, etc.
- **"Hopping"**, without any regulations, allows registrants to continue abuse while using **the same domain name.**



Presentation by Japan

2. Challenges of Registrar Hopping and Our Proposal

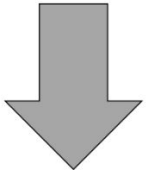
1

Challenges

- Even if a third party makes a report to a registrar, the third party has to keep repeating the same procedure due to registrar hopping.

  * In Japan, there are some cases where registrants doing abuse hop between registrars and we can't identify the identity of the registrant.

- According to RAA 3.18, when registrar receive reports of addressing abuse, registrar shall prompt steps to investigate. But, we don't know whether a registrar can investigate a registrant who has transferred.



Proposal

GAC begin to discuss the issue of "Registrar Hopping" and the need for action in terms of strengthening contractual compliance between ICANN and registrars.

DNS Abuse Mitigation: Recent GAC Communiqués

GAC ICANN68 Communiqué (27 June 2020)

- In the context of COVID-19**,** the GAC commended efforts of registries, registrars, SSAC and OCTO and shared the belief that capacity building and training should be prioritized by ICANN org for countries most affected
- The GAC noted "*that **new efforts to tackle DNS abuse should not replace, but rather complement, existing initiatives** to improve accuracy of registration data, such as the Accuracy Reporting System, and to implement policy on privacy and proxy services, which are currently on hold despite having been recommended by a number of review teams and endorsed by previous GAC advice"*.
- The GAC called on the ICANN Board "*to **implement existing advice** and on the ICANN community to **seize this opportunity and commit to its different work streams on DNS Abuse** [...]"*

GAC ICANN69 Communiqué (23 October 2020)

- The GAC took "*note of the GNSO Subsequent Procedures PDP Working Group determination that **DNS Abuse issues should be addressed in a holistic manner**, **such that any proposed approach/methodology** for addressing DNS abuse **would be applicable to both existing and new gTLDs***"
- The GAC noted that is belief that "*[b]eginning with the recommendations from the CCT-RT and the SSR2 RT and continuing through several cross-community sessions and more recent work on a DNS Abuse Framework", "**there is now a solid expression of broad support for concrete steps to be taken** to address the core components of effective DNS abuse mitigation".*
- The GAC indicated that it "*stands **ready to work with the ICANN Board and the Community** to advance this shared goal, including **through proposals to improve policies and/or improve contract provisions and enforcement**, in relation to curbing DNS Abuse.*"

DNS Abuse Mitigation: Recent GAC Communiqués

GAC ICANN70 Communiqué (25 March 2021)

- The GAC stated that "***DNS Abuse should be addressed in collaboration with the ICANN community and ICANN org prior to the launch of a second round of New gTLDs****. The GAC supports the development of proposed contract provisions applicable to all gTLDs to improve responses to DNS Abuse.*"
- The GAC emphasized "*the i**mportance of taking measures to ensure that Registries, Registrars and Privacy/Proxy Services providers comply with the provisions in the contracts** with ICANN, including audits.*"
- The GAC welcomed "*the recently-launched **DNS Abuse Institute** and encouraged community efforts to **cooperatively tackle DNS Abuse in a holistic manner***"

GAC ICANN71 Communiqué (21 June 2021)

- The GAC recognized "*the **collaborative efforts taking place within the ICANN community to develop voluntary mechanisms to address DNS Abuse**, such as the Framework on Domain Generating Algorithms Associated with Malware and Botnets, and appreciates the **efforts from all parties within the multistakeholder community to identify opportunities for advancement on the topic** of DNS Abuse when and where possible*".
- The GAC acknowledged "*the **importance of ensuring that registries and registrars comply with ICANN contractual obligations***" noting that *"At the same time, **the GAC continues to emphasize the need to develop and implement improved contract provisions**, with clear and enforceable obligations, to better address DNS Abuse before further expanding the root through any subsequent application round for new gTLDs*."
- The GAC indicated "*it will continue to closely follow developments within the community*" related to "***Improvements to the measurement, attribution, and reporting of abuse***" which it stressed were "*much needed*"

DNS Abuse Mitigation: ICANN72

ICANN72 Objectives (Leadership Proposal For GAC Action in GAC Session Briefing)

1. **Consider the ICANN Board's** Resolution and Scorecard (22 July 2021) **on the Recommendations of the Security Stability and Resiliency Review (SSR2)** on which the GAC had submitted Comments (8 April 2021).

2. **Consider the results of ICANN's Audit on Registrars' compliance with DNS Abuse obligations** as reported in a announcement and report (24 August 2021).

3. **Consider the SSAC proposal for an** Interoperable Approach to Addressing Abuse Handling in the DNS (19 March 2021) including the proposed creation of a "Common Abuse Response Facilitator" as an independent non-governmental, not-for-profit organization that would act as a facilitator for the entire DNS ecosystem to streamline abuse reporting and minimize abuse victimization

4. **Consider Noting ICANN's ability to negotiate agreements, including Public Interest Commitments**, with any party (which includes Registries and Registrars) in service of its Mission. In its role as a public benefit corporation tasked with ensuring the stability and security of the Internet's unique identifier systems, ICANN is particularly well placed to receive public policy input and negotiate updates to the standard Registry and Registrar agreements to ensure these contracts promote the public interest by including clear and enforceable obligations to detect and respond to security threats and DNS Abuse.

Review our Expected Standards of Behavior when participating in ICANN Meetings.

Go to:
http://go.icann.org/expected-standards

Review the ICANN Community Anti-Harassment Policy when participating in ICANN Meetings.

Go to:
http://go.icann.org/anti-harassment

Do you have a question or concern for the ICANN Ombudsman?

Email ombudsman@icann.org to set up a meeting.

ICANN