DNS Abuse Mitigation (1/2)

Laureen Kapin (US Federal Trade Commission, Co-Chair GAC PSWG)
Chris Lewis-Evans (UK National Crime Agency, Co-Chair GAC PSWG)
Gabriel Andrews (US Federal Bureau of Investigation)

ICANN70

23 March 2020

ICANN | GAC

Governmental Advisory Committee

Agenda

1. **Introduction: ICANN70 Discussions of DNS Abuse**

2. **Review of the Recommendations Given by the Second Security, Stability, and Resiliency (SSR2) Final Report**

3. **Japan's proposals on DNS Abuse**

4. **Next Steps for the GAC on DNS Abuse Mitigation**
   - Current State of ICANN Community Work and Discussions
   - Considered Priorities for the GAC
   - Possible concrete proposals

Introduction

GAC Discussions of DNS Abuse during ICANN70

- Agenda Item 8 - DNS Abuse Mitigation Discussions (1/2) — Tue. 23 March 1400 UTC
  - SSR2 Review Recommendations
  - Next Steps
- Agenda Item 12 - GAC Meeting with the ICANN Board — Tue. 23 March 1800 UTC
  - SSR2 Review Recommendations
  - Access to and Accuracy of gTLD Registration Data
- Agenda Item 14 - GAC Meeting with the GNSO — Wed. 24 March 1400 UTC
  - SSR2 Review Recommendations
  - Accuracy of gTLD Registration Data
- Agenda Item 16 - DNS Abuse Mitigation Discussion (2/2) — Wed. 24 March 1615 UTC
  - Panel Discussion of DNS over HTTPS (DoH)

Other Relevant Sessions during ICANN70

- Contracted Parties DNS Abuse WG Community Outreach — Mon. 22 March 1530 UTC
- ICANN Board Meeting with SSAC — Wed. 24 March 1930 UTC
- ICANN OCTO on DNS and Naming Security — Thu. 25 March 1400 UTC
- SSAC Public Meeting — Thu. 25 March 1530 UTC

Review of the SSR2 Recommendations

Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

- Purpose
  - ICANN By-Laws Section 4.6(c)
    - *"The Board shall cause a periodic review of ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the system and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates ("SSR Review")."*
      - *"...the SSR2 Review Team shall also assess the extent to which ICANN org has successfully implemented its security efforts…"*

- SSR2 Team included GAC nominees:
  - Kerry-Ann Barrett (OAS) and Noorul Ameen (India)

- The SSR2 Review Team delivered a Draft Report (24 January 2020)
  - The GAC Comment (3 April 2020) endorsed many of the recommendations and in particular those pertaining to improving Domain Abuse Activity Reporting (DAAR) and the strengthening of compliance mechanisms.

Review of the SSR2 Recommendations

Background

- The SSR2 Review Final Report (25 January 2021) is now open for Public Comments
  - (Deadline for comments: **8 April 2021**).

- Summary
  - 57 pages (96 pages w Appendixes)
  - 24 Recommendation Groups, containing **63 Recommendations** in total
    - Full Consensus of SSR2 team was achieved for all 63 recommendations

Review of the SSR2 Recommendations

Review of Recommendations (for GAC Consideration)

- Recommendation 1:
  - Further Review of SSR1
    - *"implementation plans for those recommendations were … insufficiently measurable"*
- Recommendation 2:
  - Creation of a "C-Suite" (Chief Security Officer or Chief Information Security Officer) Position Responsible for both Strategic and Tactical Security & Risk Management
    - consolidates existing security-specific duties/roles currently addressed by two existing ICANN teams lead by the Office of Chief Technology Officer & Chief Information Officer.
- Recommendations 3-7 give this proposed CSO/CISO specific duties
  - Recommendation 3:
    - SSR-related Budget Transparency
  - Recommendation 4:
    - Risk Management Processes and Procedures
  - Recommendation 5:
    - Industry standard "Security Management Systems" Compliance & Certifications
  - Recommendation 6:
    - SSR Vulnerability Disclosure & Transparency
  - Recommendation 7:
    - Business Continuity & Disaster Recovery Process/Procedure Improvements

Review of the SSR2 Recommendations

Review of Recommendations (for GAC Consideration)

- Recommendations 8-15 have direct DNS Abuse implications

- Recommendation 8
  - **Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties**
  - 8.1 - ICANN org should commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the DNS for end-users, businesses, and governments.
    - "This recommendation can be considered implemented when ICANN org has included abuse and security specialists in these (contract) negotiations…"

Review of the SSR2 Recommendations

Review of Recommendations (for GAC Consideration)

- Recommendations 8-15 have direct DNS Abuse implications

"During an April 2018 dialogue with the SSR2 Review Team, ICANN Contractual Compliance asserted that the current contracts with registries and registrars do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names and are thus ineffective in allowing them to pursue those engaged in systemic DNS abuse." - SSR2 page 34

- Recommendation 9
  - **Monitor and Enforce Compliance**
    - 9.1 ICANN Board to direct the ICANN Compliance Team to "strictly enforce" SSR obligations
    - 9.2 Monitor and enforce registration data accuracy
    - 9.3 External audits be conducted against ICANN Org's Compliance Team
    - 9.4 Task Compliance with publishing regular reports "tools" needed for its mission

    - These recommendations can be considered
      - implemented *"when audits are happening regularly, and summaries published."*
      - effective *"when ICANN org has completed an audit successfully and reported out to the community."*

Review of the SSR2 Recommendations

Review of Recommendations (for GAC Consideration)

- Recommendations 8-15 have direct DNS Abuse implications

- Recommendation 10
  - **Provide Clarity on Definitions of Abuse-related Terms**
    - 10.1 Post a web page of such terms
      - clearly define which DNS abuse categories ICANN org sees as within its remit
    - 10.2 Establish a working group (CCWG) to update the terms over time
    - 10.3 Make consistent use of the terms in ICANN's public documents, contracts, plans, etc

    - These recommendations can be considered
      - implemented *"when ICANN org publishes the web page that includes the first output of the CCWG..."*
      - effective *"when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions … thus enabling other stakeholders to define codes of conduct around DNS abuse"*

Review of the SSR2 Recommendations

Review of Recommendations (for GAC Consideration)

- Recommendations 8-15 have direct DNS Abuse implications

- Recommendation 11
  - **Resolve Centralized Zone Data Access (CZDS) Data Access Problems**
    - 11.1 Ensure access to CZDS data is available, in a timely manner, w/o unnecessary hurdles

- Recommendation 12
  - **Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review**
    - 12.1 ICANN Org should create a DNS Abuse Analysis team of experts (no $ interest) to "overhaul" DNS Abuse reporting prioritizing: actionable data, validation, transparency, and independent reproducibility of analyses.
    - 12.2 Seek to improve contracts w such reporting data providers to allow sharing/reproducibility of data for non-commercial use.
      - publish contracts; terminate contracts which don't enable data-sharing
    - 12.3 ICANN org should publish reports that identify registries and registrars whose domains most contribute to abuse.
    - 12.4 ICANN org should publish reports of actions taken by registries/registrars in response to complaints of illegal/malicious conduct connected to the use of the DNS.

Review of the SSR2 Recommendations

Review of Recommendations (for GAC Consideration)

- Recommendations 8-15 have direct DNS Abuse implications

- Recommendation 13
  - **Increase Transparency and Accountability of Abuse Complaint Reporting**
    - 13.1 Establish a centralized "DNS abuse complaint portal" to automatically refer complaints
      - ICANN org would collect only summary (complaint category) / metadata
      - mandatory for gTLDs, voluntary for ccTLDs
    - 13.2 ICANN org should publish the number of complaints made, and allow third parties to analyze the types of complaints on the DNS.

    - These recommendations can be considered
      - implemented *"when ICANN org simplifies the process of submitting and receiving abuse complaints and offers insight into the number of complaints and some metadata (e.g., type of abuse reported, dates, time to resolution) for researchers and community members."*
      - complete "*when the portal is up and running.*"
      - effective *"when contracted parties have to spend less time on misdirected complaints, and the research community as well as the broader ICANN community can see and study the associated data about those complaints"*

Review of the SSR2 Recommendations

Review of Recommendations (for GAC Consideration)

- Recommendations 8-15 have direct DNS Abuse implications
- Recommendation 14 & 15
  - **14. Create a Temporary Specification for Evidence-based Security Improvements**
    - 14.1 ICANN org should create a TempSpec requiring contracted parties to keep their X% of abusive domains below a published “reasonable” threshold.
    - 14.2 ICANN org should provide to contracted parties a list of domains in their portfolios identified as abusive.
    - 14.3 ICANN org should verify if/when abusive domains hit the X% threshold, and issue a notice to the relevant party
    - 14.4 ICANN org should allow 30 days to rectify or demonstrate flawed data
    - 14.5 ICANN org should consider $ incentives to portfolios of less Y% abuse
  - **15. Launch an EPDP for Evidence-based Security Improvements**
    - 15.1 After creating the TempSpec, ICANN org should establish a staff-supported Expedited Policy Development Process (EPDP) to create an anti-abuse policy
    - 15.2 The EPDP should define countermeasures/remediation actions vs types of abuse, define time frames for actions by contracted parties in response to abuse reporting, and define ICANN contractual compliance enforcement actions. ICANN org to insist on power to terminate contracts in face “pattern and practice” of harboring abuse.

Review of the SSR2 Recommendations

Review of Recommendations (for GAC Consideration)

- Recommendations 16-24 are engineering / standards focused.

- Recommendation 16:
  - Privacy Requirements and Registration Directory Service (RDS)
- Recommendation 17:
  - Measuring Name Collisions
- Recommendation 18:
  - Informing Policy Debates
- Recommendation 19:
  - Complete Development of the DNS Regression Test Suite
- Recommendation 20:
  - Formal Procedures for Key Rollovers
- Recommendation 21:
  - Improve the Security of Communications with the TLD Operators
- Recommendation 22:
  - Service Measurements
- Recommendation 23:
  - Algorithm Rollover
- Recommendation 24:
  - Improve Transparency and End-to-End Testing for the Emergency Backend Registry Operator (EBERO) Process

Review of the SSR2 Recommendations

Discussion of other Stakeholders' Comments (thus far) on SSR2 Final Report

- To date, comments were submitted by the Registry Stakeholder Group (RySG), PIR and Verisign
  - Both the RySG and PIR have objected to
    - Recommendations 8 (Abuse & security experts participating in contract negotiations)
    - Recommendation 14 (TempSpec for Evidence Based Security Improvements)
- The RySG further does not support Recommendation 2's Creation of a central Chief Security Officer
  - but supports the "*recommendations insofar as they represent strategic requirements for ICANN Org risk management.*"
- Verisign published comments encouraging further consideration of various potential Post-Quantum DNSSec cryptographic algorithms (No corresponding SSR2 Recommendation)

- **Questions & Answers with the SSR2 Authors**

- **Reminder:** Comments for SSR2 are due by April 08

Japan Presentation

DNS Abuse Mitigation - Next Steps

Current State of ICANN Community Work and Discussions

- **ICANN Board/Org**
  - The ICANN Board directed ICANN org (1 March 2019) to facilitate community efforts to develop a definition of "abuse" to inform further action on CCT Review Recommendation 14 & 15
  - ICANN Compliance has been auditing Registries and Registrars regarding DNS Abuse-related obligations
  - ICANN OCTO reported on its activities and trends (incl. DAAR and DNSTICR for COVID-related names)
  - ICANN agreed with Verisign on an Amendment to the .COM Registry Agreement incorporating language consistent with Specification 11 3a/b of the Base Registry Agreement, as well as a Letter of Intent
- **GNSO**
  - GAC and GNSO Leadership previously discussed a possible framework to make progress on DNS Abuse
  - The Sub Pro PDP WG called for DNS Abuse to be addressed holistically and did not consider recommendations
  - This matter is identified as "Unplanned" in the GNSO Council planning documentation (as of 18 February 2021), with the GNSO Council "*to determine next steps, if any, on DNS Abuse*".
- **Contracted Parties**
  - Argue that they have limited, and not always appropriate tools to respond to DNS Abuse
  - Reluctant to consider policy development, unless precisely scoped
  - Think that there is potential to make ICANN Compliance enforcement of current contracts more effective
  - Report growing activity in their dedicated and joint DNS Abuse Working Groups
  - Participate in voluntary initiatives such as the DNS Abuse Framework and DNS Abuse Institute
- **SSAC** will propose strategies and processes to address DNS Abuse identification and mitigation in upcoming paper
- **ALAC** has been discussing the definition of DNS Abuse, looking for ways to address the disconnect in the community regarding contract enforceability and effectiveness of enforcement, and working on education campaigns.

DNS Abuse Mitigation - Next Steps

ICANN69 GAC Action Point:

- **GAC PSWG** to consider developing a concrete proposal regarding DNS Abuse Mitigation steps to prepare GAC for further discussions at ICANN70 (per GAC Wrap up Session discussion)

Considered Priorities for the GAC (to inform Concrete Proposals)

- Focus on the impact of DNS Abuse. Disagreement on statistics related to volumes of abusive domains; also data does always reflect significant impact on victims
- Prioritize action on types of DNS Abuse that are known to enable cybercrime
- Ensure timely action when abuse is detected, especially if it's systemic abuse (repeat bad actors)
- Tackle specific, clearly identified and known issues in responding to DNS Abuse
- Prioritize actions that address behavior of the core of DNS abuse (without burdening compliant actors)
- Foster better information sharing between parties
- Streamline and standardize Abuse Reporting to Registries, Registrars and other relevant parties
- Ensure Access to accurate gTLD Registration Data
- Education of end-users

DNS Abuse Mitigation - Next Steps

Possible Concrete Proposals

- ICANN Community Work
  - Possible cross-community work to identify specific issues with certain levels of consensus and discuss available opportunities to address these, including via policy development if appropriate
  - Financial incentive programs to reward effective prevention and mitigation (CCT Review, SSR2 Review, discussions with CPs)
  - A single trusted notifiers program similar to those operated by some Registries and Registrars
- Seek closure of discussion on DNS Abuse definitions
- Improvements to Existing Contracts, Tools and Measures
  - Clarification of contractual provisions for their effective enforcement
  - Making DAAR Reporting more actionable, including information regarding Registrars and actions taken by Registries
  - Adoption of ccTLD Best Practices in the gTLD space
- Continue efforts to study DNS Abuse to ensure currency and relevance of tools and mechanisms in place at ICANN

Concrete Proposal: Improvement of Contracts

Enforceability of ICANN contract provisions

- GAC had advised that all commitments set forth in new gTLD applications should be transformed into binding contract obligation subject to compliance oversight by ICANN
- GAC Beijing Communiqué (11 April 2013): provided safeguard advice with mandatory proposals specific to all new gTLDs, regulated gTLDs, and highly-regulated gTLDs (subsequently modified by ICANN Board)
- ---> led to Public Interest Commitments (Specification 11 of Registry Contract for new gTLDs)
- Registry Agreement Specification 11:

  Section 3.a. include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision:

  - prohibiting Registered Name Holders 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,
  - providing consequences for such activities (including suspension of domain name)

Concrete Proposal: Improvement of Contracts

Enforceability of ICANN contract provisions

- Registry Agreement Specification 11 Section 3.b.:
  - periodically conduct a technical analysis (assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets
  - maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks.
  - provide to ICANN upon request

- Gaps:
  - Does not specify what type of actions need to be taken to respond to security threats
  - ICANN Compliance experienced challenges in obtaining detailed info from certain Registries on this topic during the Registry Operator Audit for Addressing DNS Security Threats (17 September 2019)

- PSWG and Registries have worked together on voluntary guidelines in the Framework for Registry Operator to Respond to Security Threats (20 October 2017)

Concrete Proposal: Improvement of Contracts

Enforceability of ICANN contract provisions

- ICANN Board has signaled in correspondence to IPC (12 February 2020) that ICANN Compliance can't enforce certain contract provisions:
  - *does not grant ICANN org an enforcement right against registrars who fail to include the required language in their agreements with RNHs or authority over how, or to determine whether, registrars "do impose these consequences"*
    - *Instead, RA Specification 11 3(a) provides registry operators and registrars a mechanism to take action against the prohibited activities. In that regard, ICANN org expects registry operators to enforce their Registry-Registrar Agreements (RRAs) with registrars and registrars to in turn enforce their registration agreements with RNHs.*
  - Re: Rgr. Agreement: *the RAA does not prescribe the specific consequences that registrars must impose on domain names that are the subject of abuse reports. ICANN org has no contractual authority to instruct registrars to delete or suspend domain names.*
- Next round of gTLDs could provide example of improved contract provisions on DNS Abuse

Concrete Proposal: Definition of DNS Abuse

Seek closure of discussion on DNS Abuse definitions

GAC Statement on DNS Abuse (18 September 2019) notes range of definitions:

- **CCT Review Team**:
  - "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" refers to 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
- **ICANN contracts**:
  - Required prohibition on registrants: 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, and providing consequences for such activities including suspension of the domain name.
  - **Registry Operators of new gTLDs** 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." (list is illustrative rather than exhaustive)
  - **Registrars of new gTLDs** must promptly "investigate and respond appropriately to any reports of abuse."

→ **These sources, developed within the ICANN multistakeholder community comprise a common foundational understanding of what comprises DNS Abuse**.