APAC Space web conference

DNS Abuse

13 February 2020

Agenda

- **Welcome Remarks** (5 mins)
  by Jia-Rong Low (ICANN)
- **Introduction to DNS Abuse** (30 mins)
  by Donna Austin (RySG) and Holly Raiche (ALAC)
- **Q&A / Community Discussion** (20 mins)
  facilitated by Satish Babu (APAC Space Community Facilitator)
- **AOB** (5 mins)
  - APAC Space @ ICANN67 Cancún

APAC Space

- “Space for APAC community members
- Community-led bi-monthly Sessions — web conference, or face-to-face at ICANN Meetings
- ”Practice ground” to facilitate community discussion for ICANN participation
  - DNS industry topics
  - ICANN Policy Development Processes, and
  - ICANN Reviews

Subscribe to our mailing list : subscribe@apacspace.asia
Community discussions: discuss@apacspace.asia
Find out more: www.apacspace.asia

DNS Abuse

Donna Austin
Chair, gTLD Registries Stakeholder Group (RySG)

APAC Space Web Conference—DNS Abuse

Donna Austin, Chair RySG
Raymond Zylstra, Director – Policy and Compliance, Neustar

What is DNS Abuse?

There is no one singular agreed definition of DNS Abuse within the ICANN community.

However, the ICANN community does agree that DNS Abuse is an important topic for the community to discuss and better understand.

This includes the RySG.

Within the RySG we prefer the use of the term "security threats" to refer to threats within the scope of the Registry Agreement.

References

- RySG Open Letter to the Community
- GAC Statement on Abuse
- Business Constituency Statement on Abuse
- ALAC advice on DNS Abuse
- Plenary Session conducted at ICANN 66 in Montreal
- ICANN Compliance Audit Report

Registry Agreement Specification 11(3)(b)

"Registry Operator will 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. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request."

Requirements

- Technical analysis to identify potential security threats
- Maintain records of threats identified and actions taken

ICANN Advisory re: R A Spec 11 (3)(b)

- “[O]ffers one voluntary approach registry operators may adopt to perform such technical analyses to assess security threats and produce statistical reports as required by Spec 11 (3)(b).”
- Technical analysis: (1) reviewing data feeds; and/or (2) automated analyses that provide data equal to “Domain Reputation Service Providers” (RBLs).
- Analysis should be not less than monthly basis.
- Technical Analysis:
  - Consider use of one or more domain reputation service providers (RBLs) for a leading indication of potential problems.
  - Consider review of RR/RY transaction summaries (EPP and DNS) to identify potential problems.

Security Framework

Aim is to deliver on the ICANN Board's GAC:

"regarding ICANN soliciting community participation to develop a framework for how a Registry Operator (RO) may respond to identified security threats."

- Voluntary framework developed over 2 years ago between PSWG and Registries
- Presents a registry response to Security Threats
- Notes a hierarchy of the severity of security threats, noting difference in quality in a report
  - Who is the reporter? (higher priority LEA/public safety agencies)
- ROs should provide prompt response and should within 24 hours communicate contemplated steps
- Notes that "ROs are not necessarily the best parties to address certain security threats"

Proportionality / Collateral Damage

- Because of limited options, acting at the DNS level can have huge impact
- Acting on a domain for a piece of website content renders every other piece of content, subpage, information, email accounts for the whole domain inaccessible
- Example: Craigslist post

What can a Registry do?

Existing Registrations

1. Refer to registrar
2. Suspend the domain (e.g. apply serverHold status)
3. Lock the domain so it can't be changed
4. Redirect* the domain
5. Transfer* the domain
6. Delete

Unregistered Domains*

1. Create and typically redirect (Domain Generation Algorithms)
2. Block/reserve

* Typically for DGAs

DNS Abuse

ALAC Position

Holly Raiche
ALAC Member

DNS Abuse

Background:

- Impact of GDPR on collection of RDS data
- Competition, Consumer Trust, Consumer Choice Review Final Report 2018
  See https://www.icann.org/public-comments/cct-final-recs-2018-10-08-en
- Discussions on DNS Abuse:
  - DNS Abuse – End User Concerns Panel at ICANN 66
    See https://66.schedule.icann.org/meetings/1116759
  - ALAC Consolidated Policy Working Group discussions Oct 2019
- ALAC Statement to the Board 24 December 2019
  See <https://atlarge.icann.org/advice_statements/13747>

DNS Abuse

Competition, Consumer Trust, Consumer Choice

Chapter 9: Recommendations 14 – 24

Themes

- Incentives on registries/registrars for anti-abuse measures
- Use of Domain Abuse Activity Report (DAAR)reports to identify systemic abuse/miscreants
- Compliance Reporting

DNS Abuse

DNS Abuse – End User Concerns Panel at ICANN 66

- Definitions of DNS Abuse
- DNS Abuse Reporting: Domain Abuse Activity Report (DAAR)
- Requirements already on Registries/Registrars
- PIR – some ‘best practice’

DNS Abuse

ALAC Views

- DNS Abuse is one of the biggest challenges faced by individual Internet end users and remains a key factor eroding confidence in a single, trusted, interoperable Internet. Systemic abuse is a persistent problem; bulk registrations are a problem.
- Good actors don't obviate the need for intervention with bad actors. No new round of TLD applications should without a thorough reform effort to mitigate DNS Abuse.
- A good start in mitigating DNS Abuse is the implementation of Community recommendations, including PIR-Led Best Practices, and even they could go further to deal with systemic abuse.
- Suggesting ICANN does not have a role to play is factually incorrect, and counter-productive. ICANN has the ability to take action on this issue and delaying any action will perpetuate DNS Abuse. The status quo is insufficient, and ALAC Advice (described in the following section) provides constructive recommendations to the ICANN Board on mitigating DNS Abuse.

DNS Abuse

ALAC Recommendations to the Board:

- Establish a clear definition of DNS Abuse. The GNSO has already produced consensus definitions of “abuse” and “malicious use of domain names” that are more expansive. According to that definition, “abuse” is an action that: 1) Causes actual and substantial harm, or is a material predicate of such harm; and 2) Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such a purpose is disclosed. The GNSO also recognized that “malicious use of domain names” include, but are not limited to: 1) spam, 2) malware distribution, 3) online child sexual exploitation and imagery abuse, 4) phishing, 5) botnet command-and-control. ICANN should clarify the purposes and applications of “abuse” before further work is done to define DNS abuse. Once those purposes are identified, ICANN should determine whether abuse definitions used by outside sources can serve as references for the ICANN community, or whether a new, outcomes-based nomenclature could be useful (including impersonation, fraud, or other types of abuse) to accurately describe problems being addressed.

● Cease rate limiting WHOIS (eventually RDAP) or simplify the process of whitelisting, so that it can report on the registration ecosystem. Adopt a uniform and timely access framework for publicly available registrant data.

● Direct ICANN Org to establish low thresholds for identifying bad actors. Direct ICANN Org to publish more actionable Domain Abuse Activity Reporting (DAAR) data: identifying the operators with high concentrations of abuse against whom onward action ought to be contemplated

DNS Abuse

ALAC Recommendations (continued)

● Provide an explicit mandate to ICANN Contractual Compliance to regularly use the audit function to root out “systemic” abuse; not to regulate content, but to proactively exercise enforceability .

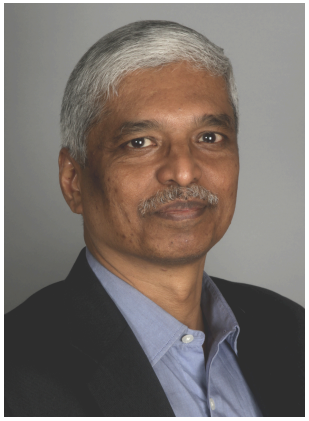
● Do not process registrations with “third party” payments, unless they have been approved prior to the request.

● Adopt an “anti-crime, anti-abuse” Acceptable Use Policy (AUP) and include enforcement.

● Compel industry-wide good behaviour: for eg. by increasing per domain transaction fees for registrars that continually demonstrate high abuse rates.

● Implement the above in agreements/contracts, with clear enforcement language for ICANN Contractual Compliance to adopt. Convene a discussion between the Contracted Parties and ICANN Compliance to finally resolve what additional tools might be needed by Compliance.

Q&A / Community Discussion



Satish Babu
APAC Space Community Facilitator

AOB

APAC Space
Wednesday, 11 March 2020
10:30AM – 12:00PM (local time)

APAC Social
Wednesday, 11 March 2020
6:30PM – 7:30PM (local time)
Refreshments provided

ICANN 67
COMMUNITY FORUM
CANCÚN
7–12 March 2020

Engage with ICANN

Thank You

Visit us at **icann.org**

subscribe@apacspace.asia

discuss@apacspace.asia

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg