18 May 2020

Mr. Seun Ojedeji
Chair, AFRALO

RE: ICANN 67 – AFRALO/AFRICANN Statement “Call on the ICANN Org and Community to intensify their efforts in curbing DNS Abuse”

Dear Mr. Ojedeji,

Thank you for your letter regarding DNS Abuse discussions at ICANN 67. We acknowledge AFRALO/AFRICANN’s concern regarding DNS Abuse and agree that it is a significant and growing problem.

Your letter called for the following:

1. Set aside adequate resources to increase DNS Abuse awareness and mitigation:

   “We call upon the ICANN Org to set aside adequate resources as the Steward of the Global Domain Name System, geared towards creating more awareness on DNS Abuse in its global multistakeholder community and how the same can be mitigated.”

   Given ICANN org resources are limited, community input on how those resources should be distributed to best meet community requirements is always appreciated. However, pragmatically speaking, the definition of “adequate” in this context will tend to be subjective – what is seen as insufficient to some will be seen as over-generous to others.

   ICANN org has dedicated resources for creating awareness about general DNS ecosystem security challenges, including DNS Abuse. The Office of the Chief Technology Office (OCTO) Technical Engagement and Security Stability and Resilience teams and the Global Stakeholder Engagement (GSE) team have been providing regional webinars on related topics. The regional webinars are publicized by our Communications and GSE teams and may be of interest to the AFRALO community. In addition, we have been updating and creating new capacity development offerings made available through the ICANN Learn platform. DNS Abuse is a key topic in these learning modules, which include practical guidance for registrants and the wider community and share good practices to protect against malicious schemes and attacks.

   To further support these outreach and capacity development activities, we have recently added two new OCTO Technical Engagement Specialists to support the GSE team in Africa.

We will continue to work to improve awareness of DNS Abuse globally and would encourage AFRALO to continue to provide input on how ICANN org can best deploy resources on this task in the context of the other activities performed by ICANN org for the benefit of the community.

2. Ensure that ICANN org stays within its remit and does not act as a content regulator by virtue of efforts against DNS Abuse.

   "Fighting the DNS Abuse shouldn't turn in a content regulation which is out of the ICANN remit. In fact, what is considered as content abuse in a country may be a freedom of expression in another. AFRALO would not accept any effort to fight DNS Abuse that becomes a content regulation. In view of this, we call upon the ICANN organization to facilitate more discussions on DNS Abuse at Regional Level through the coordination of Policy, GSE and ICANN Learn teams with African community leadership to ensure effective deliberation."

   ICANN org's response to DNS Abuse is multifaceted, reflecting the need to address abuse of the DNS within the constraints of ICANN's Bylaws and policies as defined by the ICANN community, and by obeying local law and regulatory requirements. As part of that response, we are careful to ensure content issues are not conflated with DNS security threat-related obligations included in the Registry Agreement (RA) and the Registrar Accreditation Agreement (RAA).

   With respect to organizing and facilitating more discussions on DNS Abuse at Regional levels, ICANN org's engagement plans for Africa are described in the ICANN Africa Regional Plan for 2021-2025, currently open for public comment at https://www.icann.org/public-comments/africa-regional-plan-fy21-25-2020-04-15-en. The facilitation of discussions on DNS Abuse is envisioned across all ICANN's regions, and particularly in Africa.

3. Ensure DNS Abuse reporting is simplified for Internet end users to understand:

   "We call upon the ICANN org through the office of the Chief Technical Officer to embrace reporting on DNS abuse in clear and simple language geared towards end users who are major consumers of DNS Products and services."

   Generally speaking, the OCTO team always endeavors to provide reports, briefings, and related information in a way that will allow the audience of those documents to understand and make use of them in policy discussions and elsewhere. However, this can sometimes be challenging when discussing DNS Abuse, particularly when there is a desire to avoid oversimplifying for a technical audience.

   For example, in the case of ICANN's Domain Abuse Activity Reporting (DAAR) reports, the only public report on DNS Abuse that ICANN currently publishes, the target audience is those involved in efforts to understand and mitigate abuse. As you may be aware, DAAR is a system for studying and reporting on domain name registration abuses and

security threats (i.e., phishing, malware distribution, botnet command and control, and spam) across top-level domain (TLD) registries. The DAAR system provides a replicable methodology for analyzing security threat activity and their trends that is intended to be used by the ICANN Community to facilitate informed policy decisions. End users are not directly the target audience of the DAAR reports, however per your request, ICANN org is working on publishing a complementary document 'Understanding the DAAR Report for Non-Technical Purposes" in the near future. It is worth highlighting the fact that DAAR reports are not intended to present immediately actionable abuse notifications, or to be an education tool for end-users, but rather to provide input to the ICANN community on DNS Abuse-related matters.

Additionally, we encourage you read and share with AFRALO members recent blogs intended to share direct ICANN org-related activities which also aim to inform and educate the community about DNS Abuse:

- ICANN Org's Multifaceted Response to DNS Abuse provides more information about ICANN org's increased efforts in identifying DNS abuse that leverages the COVID-19 pandemic.

- Identifying Phishing Scams, DNSSEC-Signing, and Other Tips to Protect Your Domain Name provides domain name owners and registrants with information on how to protect both their domain name and personal information related to their domain name registration.

- Reporting Potential Pandemic-Related Domains provides more details regarding a specific effort by OCTO aimed at helping to mitigate some forms of DNS Abuse, specifically phishing and malware distribution, associated with the COVID-19 pandemic.

- Introducing the DNS Security Facilitation Initiative Technical Study Group will explore ideas around what ICANN can and should be doing to increase the level of collaboration and engagement with DNS ecosystem stakeholders to improve the security profile for the DNS.

Thank you for following up on the discussions held during ICANN 67, as well as sharing your concerns and suggestions. I hope you find this response to be useful and I look forward to further engagement with your community as the ICANN community, Board, and org work towards a more secure, resilient, and reliable DNS ecosystem. Your continuous input in the DNS Abuse discussions is appreciated and welcome.

Sincerely,

David Conrad,
Chief Technology Officer, ICANN

cc:
Adiel Akplogan, Vice President for Technical Engagement
Silvia Vivanco, Senior Manager, At-Large Regional Affairs, ICANN