



EN

AL-ALAC-ST-1119-01-00-EN
ORIGINAL: English
DATE: 25 November 2019
STATUS: Pending Ratification

AT-LARGE ADVISORY COMMITTEE ALAC Advice to ICANN Board on DNS Abuse

Introduction

It has become increasingly imperative that the ICANN Community step up to address the challenge of DNS Abuse in its many forms.

According to the review of the last round of new TLDs by the Consumer Competition, Choice and Trust Review Team (CCT-RT), the safeguards put in place during the last round were not effective, and the compliance operation within ICANN does not have the necessary mandate nor probably the ideal tools to combat DNS Abuse effectively. Discussions are ongoing about how to define DNS Abuse, but there are also settled consensus definitions that could be employed for immediate reform. Once tools are in place, a change in definition will only change the scope of how these tools are used.

On [24 October 2019](#), the At-Large Consolidated Policy Working Group (CPWG), Co-Chaired by Jonathan Zuck and Olivier Crepin-Leblond, received a presentation regarding recent DNS Abuse research, in a report published by the [Interisle Consulting Group on 18 October](#). This report dealt with bulk registrations in particular and the risks they represent. While there are some legitimate uses for bulk registrations, some sort of accreditation for bulk registration could help prevent the abuse intended and facilitated by the majority of such registrations.

During the ICANN66 Annual General Meeting (AGM) in Montreal, Canada, the At-Large Community organized a policy session on "[DNS Abuse – End User Concerns](#)", with a panel presentation by Drew Bagley, Secure Domain Foundation / CrowdStrike and [Graeme Bunton](#), Chair, Registrar Stakeholder Group. Jonathan Zuck and Joanna Kulesza, Co-Chair of the At-Large Capacity Building Working Group (CBWG) and EURALO ALAC Member, moderated the session and summarized how At-Large can enhance end user protection against DNS Abuse. Graeme discussed the PIR led framework for DNS Abuse as a set of "best practices" and a kind of floor to which we should bring all contracted parties. Unfortunately, the PIR report also attempts to separate this from ICANN jurisdiction which would make it difficult to bring the other parties in line to stop bad actors. Finally, even the good actors could do more with a more proactive, account-based audit instead of only a domain-by-domain takedown. The machine learning in use by EURID and Nominet show a great deal of promise, with nearly 80% accurate predictions of potential abusive registrants.

Specifically, the At-Large believe:

- 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.
- No new round of TLD applications should begin without a thorough reform effort to mitigate DNS Abuse.
- A good start is the implementation of the recommendations from the CCT-RT, the Interisle Consulting Group Report, and Business Constituency (BC).

ALAC Advice to ICANN Board on DNS Abuse

The BC recommendations are robust and constructive, and coupled with the findings of the CCT-RT and the Interisle Consulting Group Report, the At-Large Advisory Committee (ALAC) on behalf of the At-Large Community recommend to the ICANN Board the following actions to mitigate DNS Abuse:

- Provide an explicit mandate to ICANN Contractual Compliance to regularly audit and take action against registries for “systemic” abuse. Thresholds should be determined by the community.
- Improve validation.
- Do not process registrations with “third party” payments, unless they have been approved prior to the request (i.e., if John Smith is registering domains and the credit card says “Mary McCall”, don’t allow).
- Adopt an “anti-crime, anti-abuse” Acceptable Use Policy (AUP) and include enforcement (see the Interisle Report).
- Incentivize industry-wide action: for eg. reduce per domain transaction fees for registrars that continually demonstrate low abuse rates.
- Publish more actionable Domain Abuse Activity Reporting (DAAR) data.
- Cease rate limiting WHOIS or simplify the process of whitelisting.
- Adopt a uniform and timely access framework for public WHOIS.
- Implement the above in agreements/contracts, with clear enforcement language for ICANN Contractual Compliance to adopt.