Comment on:
Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations

Involved parties

The **Brazilian Association of Software Companies (ABES)** represents around 2 thousand companies, which total approximately 85% of the billing of the software and services sector in Brazil.

AR-TARC was one of the first certification authorities in Brazil and has been advancing the interests of Small and Medium Enterprises (SMEs) internationally for the past decades.

Governance Primer is a consultancy acting in the Internet Governance space, specializing in increasing Global South participation and in the usage of diverse language writing systems online.

Preamble

The Brazilian Association of Software Companies (ABES), AR-TARC, and Governance Primer, would like to signal support to the amendments being carried out by ICANN org. and the ICANN Contracted Parties. We understand these amendments to consist of targeted and reasonable modifications that will provide additional clarity on how abuse is to be dealt with moving forward. This is a strong first step towards making the Internet safer and adequately fulfilling our role as stewards of the DNS.

SMEs often have a difficult time making the investment necessary to defend against the myriad of online threats that emerge at an increasing pace, so clearer and more effective rules to deal with malicious action are greatly appreciated. It is our hope that further conversations will follow the successful voting of this proposal, so that the community continues to advance proposals which ensure that the DNS is progressively less viable as a vector for security threats, data breaches, scams, and other ills that affect companies and individuals from around the world.

Specific comments

DNS Abuse Definition

The establishment of a clear base definition of what constitutes technical DNS Abuse is essential, and we welcome the adoption of the widely accepted base criteria initially outlined by I&JPN and subsequently adopted by many actors in debates around this theme.

We would like to reinforce that the methodologies employed by malicious actors are in constant evolution, in such a way that it is vital for these definitions to be reviewed periodically (every 1 or 2 years) with an eye towards flagging and being able to take subsequent action to combat new forms of technical abuse of the DNS.

Prompt mitigation action

We appreciate the difficulty in setting in stone a timeframe for action, as each situation has specificities and needs. With that said, it would be desirable for a ceiling to be established, so that ICANN Compliance and the reporters themselves can set appropriate expectations.

A timeframe that we have heard from multiple actors would be reasonable is “3 business days”, so this would be worthy of discussion within the current negotiation. This would definitely need to be framed as a ceiling, however, as malicious actors need much less time than that to cause severe harm.

Obligation of action (3.18.2)

This additional clause is key, and speaks directly to the necessity of more accountability among DNS actors. We reinforce that these new obligations absolutely need to be kept in the final version of these amendments, as they are the backbone of the proposal.

We also suggest that the parties involved in the negotiation give a second look at the overly restrictive definition that makes it so that it is necessary that a domain name is “being used for DNS Abuse.” While practical, this language does not account for abuse carried out over time, which is a commonly observed phenomenon. Having broader language such as “was used” in this section would allow for greater ability to stop systematic abuse, without many undesirable consequences.

Inclusion of webforms

This is a helpful development that should pave the way for better abuse management. The standardization of these forms is something that should be sought with priority in order to help the DNS community in the tracking of malicious actors and aggregate data associated with that. We signal towards CleanDNS/DNS Abuse Institute's Netbeacon as a template from which best practices can be derived for wide adoption within the industry.

ICANN Compliance's role

We would like to indicate a strong desire for greater enforcement powers to be given to ICANN Compliance in order to ensure that CPs that are truly out of line and prove to be unaccountable in the long run can be appropriately actioned upon. In case no reasonable path of action is found after the establishment of a proven history of laxness towards DNS Abuse, ICANN Compliance should have the power to have their contracts terminated.

COI disclosure

The lead drafter of this comment was co-Chair of the GNSO Council's DNS Abuse Small Team, which played part in achieving the current outcome of this process.

18 June, 2023