AFNIC Public Consultation -
Fight against abuse: Common system for verifying holders' data

Submission by: The ICANN Business Constituency
24-Nov-2023

Introduction

Thank you for the opportunity to reply to AFNIC's consultation on industry's efforts to combat domain name system (DNS) abuse; specifically, a proposed system for verifying domain name holders' data. We are very appreciative that the DNS is a subject of this AFNIC proposal and call for comment. As correctly stated, domain names -- the worldwide fulcrum of internet navigation -- too often are maliciously used to commit a growing number of crimes. It therefore is crucial that all necessary measures are taken to investigate, prevent and mitigate online harms, and that domain name registries are equipped with the tools for doing so.

Accordingly, our input focuses on the criticality of the integrity of domain name registration data (known historically as "WHOIS"), which is a central element of healthy DNS functionality.

About the ICANN Business Constituency

The Business Constituency (BC) is the voice of commercial internet users within ICANN (the Internet Corporation for Assigned Names and Numbers – the coordinating body of DNS policy). ICANN is a global body with responsibility for policies related to the DNS. Domain names are the names consumers and businesses rely upon to find websites for legitimate products and services on the Internet. The mission of the BC is to ensure that ICANN policies support an internet that promotes end-user confidence, because it is a safe place to conduct business.

The important role of domain name registration data

The BC applauds consultations regarding the contention of DNS abuse and, in particular, the instrumentalities of combating abuse through the appropriate deployment of WHOIS policy. Not only must experts and authorities have the ability to prevent threats from arising and to mitigate threats through remediation, but also, importantly, the ability to thoroughly investigate the party or parties, at scale, responsible for offending domain names once registered. This requires access to complete and accurate domain name registration data. Such records can identify domain name registrants and can be used to quickly trace the activity of ill-intended actors -- activity which often extends far beyond the immediately visible -- and potentially prevent further harm.

Unfortunately, over-implementation of the European Union's (EU) General Data Protection Regulation (GDPR) by domain name registrars and registries prompted the virtual elimination of publicly available WHOIS data. This has significantly impaired investigatory efforts related to online harms.

WHOIS and investigatory capability

Mindful of the appropriate latitude in GDPR law prescribing the availability of certain types of data, the restoration of an accurate and verified WHOIS database (in accordance with Article 28 of the European Union's Network and Information Security (2) Directive (NIS2)) would tremendously assist investigations

by law enforcement, cybersecurity authorities, intellectual property rights holders and others with legitimate interests in uncovering registration data for nefariously used domain names. Often, quick and timely access to this data can help uncover the source of online crimes and offenses, even without employing the blunt instrument of domain name takedowns.

It is important to state that these investigations must be able to access the final, underlying documentation of the registrant. Frequently, registrars employ privacy and proxy services to further mask the identities of registrants; while privacy and proxy services may provide utility to the registrant, they must not be cited or presented as the authoritative WHOIS record for a given domain name. Only the registrant-specific data underlying any masking service is appropriate for investigatory needs.

To work with registries and registrars to address DNS abuse with appropriate tools, the BC supports AFNIC's proposed common system for verifying holders' data. We recognize that there currently exists no common form of registration data validation and, accordingly, endorse such a system as a method for ensuring the data necessary for investigatory capability is well-formed and accurate.

Points arising from AFNIC survey

As AFNIC points out in its request for consultation:

> *While reachability is established in general terms, in most cases at the time the domain name is created, post-creation verification is limited (-20% of respondents) and fewer than half of respondents subsequently check reachability at least once a year.*

Such a response rate is insufficient to address DNS abuse. Any registry – including a ccTLD registry – interested in significantly combating abuse through the DNS must redouble its efforts to ensure that registration data is complete and accurate.

BC support for development of a common system

Because of the above, the BC lends its support to AFNIC's development of a "common system" for verification of registration data, including, as outlined in AFNIC's consultation, verification of holder data and the uploading of data to a registrant database or centralized query service with a status update tag.

Use of digital identities

To AFNIC's question regarding the use of digital identities as a means of verifying domain name holders' data in parallel with its usual means of checking, the BC fully supports measures (such as thus proposed) that will enhance verification methodology.

We note that such procedures – while in their developmental stage (e.g., trusted notifiers) – have had a positive impact on the health of gTLD registry databases, where employed. We therefore encourage their use in a more formalized way going forward.

The BC thanks AFNIC for the opportunity to comment on this proposal and encourages authorities to contact the BC with questions or follow-up actions.

This comment was drafted by Mason Cole, and approved in accord with the BC Charter.