DNS Abuse
Recommendations

Jonathan Zuck and All

At-Large Consolidated Policy Working Group (CPWG) Call

Wednesday, 11 December 2019
13:00 UTC

ICANN

Recommendations

- Encourage a definition of abuse that is not artificially restricted to the functioning of the DNS infrastructure. The GNSO has already produced consensus definitions of "abuse" and "malicious use of domain names" that are appropriately 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 public WHOIS.

- 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.

Recommendations, continued

- Provide an explicit mandate to ICANN Contractual Compliance to regularly use the audit function and root out "systemic" abuse.

- Validate the insufficiency of the status quo and suggest that no new round will be approved without substantial changes in the area of DNS Abuse.

- 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.

- Incentivize industry-wide action: for eg. reduce per domain transaction fees for registrars that continually demonstrate low abuse rates.

- Implement the above in agreements/contracts, with clear enforcement language for ICANN Contractual Compliance to adopt. Community dialogue cannot delay or defer ICANN's commitments or operations related to DNS Abuse.