AL-ALAC-ST-1219-03-00-EN
ORIGINAL: English
DATE: 24 December 2019
STATUS: Ratified

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

Observations

It has become increasingly imperative that the ICANN Community step up to address the challenge of DNS Abuse in its many forms. The implementation of the European Union's General Data Protection Regulation (GDPR) has driven an increase in the incidences of DNS abuse, as it has become severely problematic to leverage WHOIS and/or other parts of the DNS for the purpose of identifying bad actors and mitigating abusive behavior. Increases in abuse are well documented, and DNS Abuse has not gone without community notice.

ICANN Org has facilitated at least three separate discussions on DNS Abuse in 2019, and a major cross-community discussion on the topic took place during ICANN66 in Montreal. As the Governmental Advisory Committee (GAC) recently said about the importance of addressing DNS abuse, "Protecting the public from security threats and DNS Abuse is an important public policy issue."

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 continue 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. An explicit mandate for ICANN Compliance is needed not to regulate content, but to exercise enforceability against DNS Abuse.

On 24 October 2019, the At-Large Consolidated Policy Working Group (CPWG), Co-Chaired by Jonathan Zuck and Olivier Crépin-Leblond, discussed recent DNS Abuse research and how DNS Abuse impacts the Internet end user community, including the erosion of trust and security. The At-Large Community reached consensus that 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 Internet end user protection against DNS

Abuse. Graeme discussed the PIR led framework for DNS Abuse[1] as a set of “best practices” and a kind of floor to which ICANN 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. Systemic abuse is a persistent problem; bulk registrations are a problem.
- Good actors don’t obviate the need for intervention with bad actors[2]. No new round of TLD applications should begin without a thorough reform effort to mitigate DNS Abuse.
- A good start in mitigating DNS Abuse is the implementation of Community recommendations, Including PIR-Led Best Practices, and even they could go further to deal with systemic abuse.
- Suggesting ICANN does not have a role to play is factually incorrect, and counter-productive. ICANN has the ability to take action on this issue and delaying any action will perpetuate DNS Abuse. The status quo is insufficient, and ALAC Advice (described in the following section) provides constructive recommendations to the ICANN Board on mitigating DNS Abuse.

[1] https://thenew.org/pir-fighting-abuse-join-us/

[2] ALAC recommends defining bad actors based on quartiles: Identify the registrars that fall outside of the pattern of the rest of the registrars, perhaps by using a fraction like #ofabusedomains/#ofdomainssponsored. See https://www.thoughtco.com/what-is-the-interquartile-range-rule-3126244. To do this, the ALAC: 1) objects to any attempt by ICANN org or community members to stop collecting registrar data, and 2) recommends that the ICANN DAAR project be whitelisted from all registrar and registry WHOIS / RDAP rate limiting.

Recommendations

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:

- **Establish a clear definition of DNS Abuse.** The GNSO has already produced consensus definitions of "abuse" and "malicious use of domain names" that are 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 publicly available registrant data.
- **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 against whom onward action ought to be contemplated.[3]
- **Provide an explicit mandate to ICANN Contractual Compliance** to regularly use the audit function to root out "systemic" abuse; *not to regulate content, but to proactively exercise enforceability*.
- **Do not process registrations with "third party" payments**, unless they have been approved prior to the request.[4]
- **Adopt an "anti-crime, anti-abuse" Acceptable Use Policy** (AUP) and include enforcement.
- **Compel industry-wide good behaviour:** for eg. by increasing per domain transaction fees for registrars that continually demonstrate high abuse rates.
- **Implement the above in agreements/contracts**, with clear enforcement language for ICANN Contractual Compliance to adopt.[5] Convene a discussion between the Contracted Parties and ICANN Compliance to finally resolve what additional tools might be needed by Compliance.

Community dialogue cannot delay or defer ICANN's commitments or operations related to DNS Abuse. The above recommendations speak to the insufficiency of the status quo, and stress that no new round will be approved without substantial changes in the area of DNS Abuse.

---

[3] There are a number of metrics that DAAR already offers. One is "cumulative count of abuse domains over 365 days". Data is available showing which registries and registrars exhibit "register, use, discard, repeat" - which is the same behavior that criminals use with burner mobile phones. The phone is used once and then it is abandoned. The domain is used for a single campaign or attack, and then it is abandoned. Basically, all the data counted per registry, per registrar, can be used to formulate many metrics.

[4] Much of the POC data regarding mainly "persons" and fewer "organizations" was falsely composed. Organizations (any registrar that is not a natural person), should only accept payment methods authorized by the registrant organization. Organizations would benefit by having the ability to impose a single payment method and a focused anti-fraud measures program.

[5] ICANN has definitions of DNS Abuse, either in its contracts (from GNSO PDP work already done) or from International Treaties like the Council of Europe's Convention on Cybercrime. The ACs (including ALAC) must push for change and pursue ICANN Board members who understand the need to balance public interest against competition/commerce, in order to impact DNS Abuse.