19 August 2019

Open Letter to the ICANN Community from the Registries Stakeholder Group

Over the past several months, members of the RySG have participated in a number of ICANN Org facilitated community discussions about DNS Abuse: in Washington DC in January; the ICANN GDD Summit in May; and most recently in London in July.

This letter addresses some of the questions that ICANN Org posed during those community discussions and the content of the letter is consistent with responses that our members contributed during the meetings identified above. The RySG and several other Constituencies have proposed community sessions in Montreal to further a community discussion on the issue of DNS Abuse and security threats and we hope that this letter will be regarded as a constructive contribution to those community discussions. We look forward to participating with ICANN Org and the Community in open conversation about DNS abuse and security threats at ICANN 66 in Montreal.

Use of the term "DNS Abuse" requires greater precision and must fit within ICANN's Bylaws

The term 'DNS Abuse' means many different things to many people and often elicits calls from the community and others for contracted parties to address a problem that, as yet, has not been quantified or articulated in any meaningful or standardized way. In our review of recent community discussions, it is clear that the concepts of DNS Abuse and Content Abuse are largely conflated. More should be done to distinguish and clearly define the terms.

As we all know, Content Abuse is not within ICANN's remit, as is clearly expressed in ICANN's Bylaws (Article 1, Section 1.1(c), "ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide . . . " https://www.icann.org/resources/pages/governance/bylaws-en). That said, we are aware that registry operators may choose to address Content Abuse by establishing and enforcing anti-abuse or acceptable use policies.

Various ICANN sources use the word "abuse" broadly and such use could be interpreted to mean anything that violates a registry's terms of use (which often include an anti-abuse policy) or Content Abuse. In the RySG we strongly prefer to use the term "security threats" to refer to threats within scope of our Registry Agreements, as this is consistent with Specification 11, 3(b) of the New gTLD Registry Agreement.[1] That provision identifies security threats as "…phishing, pharming, malware, and botnets", and requires registries to monitor their zones for such threats.

[1] 2017 gTLD Registry Agreement, Specification 11, 3(b). https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html#specification11.b

It is important to distinguish between the security threats that registry operators can monitor for, and potentially mitigate, as defined by Specification 11, 3(b) of our Registry Agreements, and unlawful activity that is more properly handled by relevant law enforcement or by other actors in the Internet ecosystem, such as content hosting providers. We note that the Office of the Chief Technology Officer (OCTO) at ICANN Org has also recently reverted to using the term "security threats" as opposed to DNS Abuse. We believe that the much-needed definition of DNS Abuse should, consistent with ICANN's Bylaws, focus on whether the overall use of a domain name itself affects or impacts the security and stability of the Internet, and not encompass particular content on a website or service.

Registry Operators and the PSWG have already developed a Framework

We urge the community to rely on past work in the area as discussions move forward. The RySG and the Public Safety Working Group jointly developed and mutually agreed to a Framework for Registry Operators to Respond to Security Threats (the Framework). We encourage the community to review this framework to better understand the potential security threat response options available to registry operators. Incorrect assumptions about what a registry operator can do in response to security threat reports frustrate many community discussions of DNS Abuse.

As detailed in the Framework, registry operators generally only have two options for the actions they can take:

a) refer the complaint to the registrar or hosting provider; or
b) take down the entire domain name.

Unless a domain name's primary use is for a security threat, the risk of collateral damage associated with taking down a domain name can be significant, as it may have an adverse impact to other users that far exceeds the harm being done. A registrar or hosting provider is in the best position to facilitate security threat mitigation because they usually have the most direct relationship with the registrant. Hosting providers, in particular, are best positioned when a domain's primary purpose is not abusive, as they can remove specific content hosted on the domain without affecting non-abusive content.

We need to learn more about DNS Abuse and Security Threats

The RySG is aware that the community is concerned about unaddressed DNS Abuse or security threats and we welcome opportunities to discuss those concerns so that we might better understand the nature of the concerns and share with the community information about how and when we respond to security threats.

We are aware that some members of the community may rely on data provided in ICANN's Domain Abuse Activity Reporting - or DAAR - to support claims of systemic or widespread DNS Abuse. However, it is our opinion that the tool has significant limitations, cannot be relied upon to accurately and reliably report evidence of security threats, and does not yet achieve its objectives. The feeds DAAR relies upon may include abuses that do not correspond to the definitions set forth in registries' RAs with ICANN and security threats where the registry operator is poorly positioned to take action, or may include feeds that have higher false positive rates than are appropriate given the high risk of collateral damage associated with domain-level takedowns. The RySG has had several meaningful and constructive interactions with OCTO about these limitations and we recently formed a working group to analyze DAAR with a view to recommending enhancements to OCTO to ensure DAAR better serves its intended purpose and provides the ICANN community with a valuable resource. We've shared examples with OCTO and they are already working on improvements.

Going Forward

The RySG understands that the community is concerned about DNS Abuse. Registries are similarly focused and we want to engage and work constructively with the community and ICANN Org to address and respond to issues that we can mitigate. As registry operators, the success of our businesses depends on our ability to offer a reputable product that our users can trust. To this end, many registry operators go above and beyond the security threat monitoring requirements of our Registry Agreements.

We believe that ICANN 66 in Montreal provides the community with a timely opportunity for cross community engagement on this topic that we hope will result in a common understanding of what is within ICANN's remit to address, options available to contracted parties to respond, and a better understanding of the community concerns. We understand that the Meeting Planning Committee is in the process of discussing topics for plenary discussion at ICANN 66. We support the topic of DNS Abuse being a priority given its importance to every Constituency, the considerable interest generated prior to and during ICANN 65 in Marrakech, and the continuing community discussions led by ICANN Org.

We look forward to engaging with other community groups about this topic at ICANN 66 in Montreal.

Yours sincerely

D. Austin

Donna Austin
Chair, RySG