Mar 3, 2023
To: Sebastian Ducos (by email only via gnso-secs@icann.org)
Subject: RE: Subject: Bulk Registrations

Dear Mr. Ducos,

Thank you for your 6 January letter on the topic of Bulk Registrations. The Registries Stakeholder Group (RySG) has reviewed the letter in collaboration with the RySG's DNS Abuse Working Group and is pleased to have the opportunity to provide the following input based on the questions posed.

What information, evidence, or complaint statistics can you share that can shed further light on the potential role of bulk registrations in DNS Abuse?

The RySG would need additional detail to usefully answer the queries. Whilst we appreciate the nature of the request, we are unclear as to what the GNSO Small Team defines as 'Bulk Registrations' and therefore it is exceedingly difficult for us to pass comment on the 'potential role' of such. DNS Abuse management is a resource-heavy endeavor for any Registry Operator, and in the absence of clear and focused presentation and review of evidence of the probative value in the identification of patterns alone, evidenced based escalation of DNS Abuse remains the preferred avenue for DNS abuse management and escalation processes at the registry level.

Are you of the view that further work may be beneficial to address potential issues with bulk registrations in the context of DNS Abuse? If yes, please provide further details.

Again noting the difficulty of providing specific comment in the absence of more detail, the RySG remains committed to addressing any established vector for DNS Abuse, where the registry is the appropriate party in the circumstances to mitigate or take disrupting action.

What measures, if any, do registrars and/or registries have in place in relation to bulk registrations (examples might include, but are not limited to, additional checks adopted where registrations go above a certain threshold, and restrictions on bulk registrations from new accounts)? Are these found to be effective in constraining malicious actors? Would there be value in promoting the adoption of such measures on a voluntary basis,

or should adoption through policy development be considered? Is there potential harm in the adoption of such measures?

One area where the RySG has observed correlation of registrations as a factor, is in the case of domain generation algorithms (DGAs). The use of a DGA in such a manner is rarely carried out in 'bulk'; DGAs sometimes result in large numbers of registrations, but they typically do so over a prolonged period of time, across various registrars, and multiple registrant accounts. This is an important distinction, as we are ordinarily reliant on third party expertise in identifying such registrations, and rarely would registrant or registrar information, held by us, be of any correlative value or benefit. Regardless, we would like to note that there are numerous examples of effective responses to such DGAs, all of which have been based on existing and established anti-abuse escalation paths. The RySG notes that the success of such actions have hinged on highly responsive and effective involvement of targeted victim registries as part of quite substantial international coordinated law enforcement actions (e.g., Conficker, Avalanche, GameOver Zeus and Cryptolocker). Although past actions have been largely successful, the RySG does continue to seek out ways to further improve our industry response to such incidents. Specifically we would like to remind the Small Team and the Council of the existing work done in this area, for example the joint effort of the RySG and the GAC's Public Safety Woring Group, in defining a prudent and effective framework in handling such DGA type situations, which can be found here:
https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf .
There has been additional work on the subject on DGA's from the Internet and Jurisdiction Policy Network, through its Framing Brief - Improving the Workflow of Fighting Botnets: Handling Algorithmically Generated Domains .

The above being noted, beyond ongoing efforts on DGAs, the RySG will always welcome discussion and focus on distinct areas of improvement. We remain unsure as to the expectation of the Small Team with regards to this matter, however, generally speaking, from the point of view of a registry operator, mitigation efforts based on an evidence based approach, remains the most effective means of DNS Abuse management. In principle where actionable evidence of abuse exists, it should be escalated as appropriate. This remains true, regardless of the presence of a bulk registration.

We greatly appreciate the opportunity to respond to the GNSO Council's questions and hope that the above is helpful.

Sincerely,

Alan Woods
Vice-Chair (Admin), Registries Stakeholder Group; Co-Chair RySG DNS Abuse Working Group