ICANN | RrSG
Registrar Stakeholder Group

13 March 2023

Dear Mr. Ducos:

Thank you for your 6 January 2023 communication on the topic of Bulk Domain Registration. The Registrar Stakeholder Group (RrSG) is pleased to have the opportunity to respond to Council with our perspective and expertise on the subject and is happy to be a resource now and in the future.

The RrSG would like to first recognize that t “bulk registrations" is not a defined term, nor is it definable. The reason for this is that the registrar space is exceedingly diverse in terms of both business models and customer base, so choosing an arbitrary number or percentage to indicate “bulk” is not feasible. In many cases, even attempting to define “bulk registrations" is an invitation to abuse—telling someone that they’re not allowed to register X domains would simply result in registration of X-1 domains across different accounts in order to avoid scrutiny while achieving the same result; in addition, putting into place such a refusal of sale may have liability consequences for some registrars.

In the past, some criminals made use of algorithmically-generated domains (including Conficker in 2008 and Avalanche in 2016) and registered malicious domains using the same registrants details at distinct registrars in batches. However, in the years since then, registrars have noticed that malicious actors have evolved their tactics to blend in with typical orders, scattering their registrations by using multiple registrant information sets and registrering across many registrars and TLDs, thus keeping their activity hard to identify.

Registrars routinely support legitimate purchases of multiple domains at the same time—both similar domains and domains that are not related to each other. A trademark owner, for example may purchase the same string in multiple TLDs; a marketing firm might purchase a batch of domains to track the success of different marketing campaigns; sunrise in a new TLD frequently prompts a flood of new registrations; protected marks lists (such as DPML) also function as aggregated registration.

Taking into account that “bulk registrations" cannot be adequately defined, we offer the following in response to your questions:

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

> Registrars do not consider “bulk registrations" to be a trackable statistic for measuring or otherwise addressing DNS Abuse. Since the early 2010s, the landscape of malicious activity has changed, making it an obsolete term and tactic. In our experience, criminals are using more elaborate tactics including using different registrars, TLDs, and sets of registrant details. We have focused on other means to address DNS Abuse.

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.

> The RrSG’s DNS Abuse Sub Group is not aware of any work that might be beneficial in this regard and would instead advise to focus on other means to address DNS Abuse more efficiently, such as those raised in the other letters from the Small Group.

ICANN | RrSG
Registrar Stakeholder Group

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?

> In addition to the verification obligations imposed by the 2013 RAA, registrars have more effective ways of combating malicious registration and note that fraudulent banking transactions are often a significant flag for malicious registration. Some registrars restrict payment types; others use credit card processing companies to identify valid (or invalid) payment information. Registrars may also use IP address tracking, restrict their customers to certain local geographic areas, or establish personal relationships with their customers in order to screen out malicious registrations. However, it is important to note that these steps are not used to prevent "bulk registrations", but rather, *any* malicious registrations, and confining them to an undefined term ("bulk registrations") could have negative consequences.
>
> Restricting domain purchases to a certain threshold or hampering a new account to keep it from purchasing multiple domains are not considered by the RrSG DNS Abuse Sub Group to be *de facto* effective methods of constraining malicious actors and it is difficult to foresee any value or benefit in promoting such restrictions at the ICANN level. Some registrars may use similar restrictions, based on their business model, but neither voluntary adoption nor policy development in this area should be considered evidence that a registrar is employing these methods exclusively to mitigate DNS Abuse since these types of registrations are not considered to be *de facto* DNS Abuse and there are other technical reasons for limiting registrations, such as ensuring the number of registrations does not exceed a registrar's technical capacity.
>
> It is important to note that there is the potential for actual harm in adopting such measures because they do not take into account the diversity of business models and instead attempt to apply an arbitrary definition to all.

We greatly appreciate the opportunity to respond to the GNSO Council's questions with regard to bulk registrations and hope that the above is helpful. We are happy to answer any future questions you may have.

Sincerely,

Ashley Heineman
Chair, Registrar Stakeholder Group