ALAC Response to the GNSO Letter on DNS Abuse

DRAFT: 28 March 2022

1. Can you please provide further details on what specific problem(s) policy development, in particular, would be expected to address and why you believe policy development is the right mechanism to solve those problems?

There is evidence that domain names are registered, often in large quantities, to specifically use for malicious activities such as botnet command & control and spam used for distribution of malware. These domain names are typically used for short periods of time, so once the malicious activity is detected, they can be taken down, but by then they have served their purpose. Prior to GDPR, WHOIS information could sometimes be used to detect registrations that had not yet been used and thus taken down before they cause additional problems. With GDPR, that is no longer possible. So it is increasingly crucial to detect such registrations prior to their use, or to prohibit such registrations.

Currently there are no tools to do this.

One area of potential policy development is to minimize the number of bulk registrations made with malicious intent. Clearly there are bulk registrations done for valid and legal reasons, but the challenge will be to reduce or eliminate those bulk registrations done with malicious intent. A previous example with some similarity to this was the case of Domain Tasting. In that case, the Add Grace Period was used to register domains for short periods of time at no cost to the registrant. By increasing the cost of such registrations as to make the practice financially unviable. Bulk registrations may be more complex, but the intent is to investigate methodology to detect abusive behavior and either prohibit it or make it financially unattractive. A possible key component is Know Your Customer (KYC). There are well established processes (and regulations) with regard to financial transactions. The technique can also be applied to registrants who do not do bulk registrations but do a large number of registrations over time. KYC may arguably not be practical for small-scale domain registrations, but that is not the case if large numbers of registrations are involved.

Bulk registrations are an example of where policy development may address an issue related to domain abuse. There may well be other areas This is not the only area that may be identified as an opportunity to to address registrations made with malicious intent. As another example, there has been a lot of research and operational deployment of predictive algorithms that identify potentially abusive domains at registration time (examples: Predator and Premadoma). To date they have been used for ccTLDs with

good success (and minimal false positives). Such tools could be developed and deployed by ICANN at minimal cost to registrars and registries, either as distributed software or through a cloud-based system.

For avoidance of doubt, the preceding are examples of possible areas of policy development and not meant to be the definitive list.

The ALAC also believes that the issue of accuracy (in its varied meanings) is relevant to domain name abuse. This could be addressed through incremental improvements to ensure accuracy, or a large scale change which would change how registrations are managed. However, this is all under consideration by the Accuracy Scoping Team and is not the subject of this current submission.

2. What do you believe are the expected outcomes if policy development would be undertaken, taking into account the remit of ICANN and more specifically GNSO policy development, in this context?

The expected outcome is to significantly reduce the number of domains registered with malicious intent, thus reducing the opportunities for phishing, botnet control and spam distribution of malicious software.

3. Does the ALAC have any expectations with regards to possible next steps the GNSO Council could or should undertake in the context of policy development?

The ALAC and At-Large are not experts related to maliciously registered domains, but such experts exist. As a first step, the GNSO should appoint a small team of such experts to more fully develop a catalog of activity that should be targeted - The SSAC, GAC PSWG and others should be able to readily identify such a team.The output of this small team would then feed into an Issue Report leading to a PDP.

When a PDP is initiated on one or more of these subjects, it must have strong representation from the groups directly involved with cyber-security, and must have ACTIVE involvement from ICANN Contractual Compliance to ensure that the resultant policy is one that can be properly enforced.

BACKGROUND (not part of submission)

Essentially all three questions are asking whether we believe that the GNSO should initiate a PDP related to Domain Abuse. Should the answer be yes, they would have to start by requesting an Issue Report. Addressing their three questions may be facilitated by looking at what a Request for an Issue report requires. I have extracted the salient questions from the PDP Manual and started addressing the points to be covered.

Request for Issue Report	
Please provide rationale for policy development:	We know that some aspects of what we call domain abuse involves the registration of domain names explicitly to facilitate some forms of malicious action. The vast majority of spam and botnet command-and-control domain names are maliciously registered. Although studies have shown that many of these registrations are concentrated on particular TLDs and sponsored by specific registrars, Contractual Compliance does not appear to have any tools to take action. Nor are there any penalties or disincentives for contracted parties encouraging them to stop such activities. Policy development may be able to provide tools (actionable compliance interventions and/or financial disincentives).
Suggestions on specific items to be addressed in the Issue Report (if any):	Domain Tasting virtually eliminated by identifying methodology for identifying those abusing the policy and levying financial penalties. Potential for limiting use of bulk registration without appropriate certification of the registrant and of planned use. The same can be applied to registrants who do not do bulk registrations but cumulatively do a large number of registrations.
Please provide a concise definition of the issue presented and the problems raised by the issue, including quantification to the extent feasible:	Extract of reports (see EU Study on DNS Abuse and its references. NEED SPECIFIC REFERENCES
What is the economic impact or effect on	Consumer trust in the Internet is damaged by

competition, consumer trust, privacy and other rights:	abuses associated with domain registrations associated with cyber-criminal activities.
Please provide supporting evidence (if any):	Extract of reports (see EU Study on DNS Abuse and its references. There are studies that have estimated the financial losses associated with cyber crime, much of which is facilitated by domain name abuse (CITATIONS)
How does this issue relate to the provisions of the ICANN Bylaws, and/or ICANN's Articles of Incorporation:	Consumer Trust is mentioned several times in the bylaws. The use of domains for malicious intent also goes against stability and security of the DNS. Moreover, as custodian of the domain name system and gTLDs which constitute a large part of the DNS, ICANN has an obligation to ensure that it is not used for criminal activities.