ALAC Response to the GNSO Letter on DNS Abuse

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?

The following are examples of possible areas of policy development and not meant to be a definitive list.

There is evidence that domain names are registered, often in large quantities, for specific use in malicious activities such as botnet command & control and spam (often used for distribution of malware and other malicious activities). These domain names are typically used for short periods of time, so although once the malicious activity is detected they can be taken down, by then they have served their purpose. Prior to GDPR and the resultant Interim Specification/EPDP, 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 without significant Registry/Registrar investigation. So it is increasingly crucial to detect such registrations prior to their use, or to prohibit such registrations.

Currently there are no known tools in use to do this for gTLDs.

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 is 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. Increasing the cost of such bulk registrations made the practice financially unviable. Bulk registrations may be more complex, but the intent is to investigate methodologies to detect abusive behaviour and identify ways to either prohibit/reduce 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. Based on knowledge of the customer, certain behaviours or actions may be allowed, disallowed, or subject to specific constraints. KYC may arguably not be practical for small-scale domain registrations, but that is not the case if large numbers of registrations are involved. These techniques can also be applied to registrants who do not do bulk registrations but do a large number of registrations over time.

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 are well known examples). To date they have been used for ccTLDs with good success (and minimal false positives). Such tools could be developed and kept current (due to changing threat models) by ICANN (or a sub-contractor) and deployed at no or minimal cost to registrars and registries, either as distributed software or through a cloud-based system.

A third area for consideration is where there are already contractual conditions (Registry and Registrar) that should address certain types of abuse (such as those referenced in the Base Registry Agreement Specification 11, section 3b) but do not seem to truly allow effective compliance actions.

For avoidance of doubt, the preceding are examples of possible areas of policy development and not meant to be a 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, although it might contribute to mitigating DNS abuse, 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 and various attacks.

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 Community have a strong interest and have gained significant understanding, but we are not experts on the subject of maliciously registered domains. However, such experts exist. As a first step, the GNSO should appoint a small team of such experts, augmented with knowledgeable ICANN participants, to more fully develop a catalog of activities 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 (or multiple PDPs).

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.

At-Large is of course willing to contribute to all phases of such work going forward.

References

Abusive domain recognition (Premadoma, Predator, etc.):
https://lirias.kuleuven.be/retrieve/549721/,
https://www.icir.org/vern/papers/predator-ccs16.pdf,
http://essay.utwente.nl/84073/1/proactive_recognition_of_domain_abuse_erratum_final.pdf,

Criminal Abuse of Domain Names:
https://interisle.net/sub/CriminalDomainAbuse.pdf

ICANN DAAR Reports: https://www.icann.org/octo-ssr/daar

Bulk Registration:
https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns

04 April 2022