Draft Report: New gTLD Program Safeguards to Mitigate DNS Abuse

The gTLD Registries Stakeholder Group (RySG) thanks the experts including the Abuse Policies Working Group APWG), Registry Internet Safety Group (RISG) , Computer Emergency Response Teams (CERTs) and participant members from the banking, financial and Internet security communities for the draft report on New gTLD Program Safeguards to Mitigate Abuse. Our comments are organized according to the document posted for public comments.

2. DNS ABUSE: KEY TERMINOLOGY

The Registration Abuse Policies Working Group

Potential forms of Registration Abuse

Under potential forms of registration abuse on Page 6, the fact that Name Spinning could lead to suggestions which are trademarked names is offset by the fact that the registrar intimates/informs the fact of the domain name being a trademark as a compliance measure to the registrant and even then, if the registrant registers such a domain name, the abuse would be covered under cybersquatting.

The Nine Safeguards

1. Question: How do we ensure that bad actors do not run Registries?

Safeguard: Vet Registry Operators
Defining Effectiveness and Possible Data Collection and Measurement
The possibility of an additional background screening of the registry operator after a specific period of time after delegation of the TLD might be an additional way to measure the effectiveness of the safeguard on an ongoing basis.

2. Question: How do we ensure integrity and utility of registry information?

Safeguard: Require Demonstrated Plan for DNSSEC Deployment
Possible Data Collection and Measurement
In addition to the number of issues reported on registry compliance with DNSSEC requirements, the average time period within which the DNSSEC compliance issues are solved could gauge the execution and implementation of DNSSEC.

3. Question: How do we ensure more focused efforts on combating identified abuse?

Safeguard: Centralization of Zone-File Access
Defining "Effectiveness"
There could be a system of 2 factor-authenticated automatic access to zone-file based on a set of questions needed for cursory verification by the registry operator to grant access which could eliminate the need for manual verification removing chances of errors.

Safeguard: Documented Registry Level Abuse Contacts and Procedures
Defining "Effectiveness"
A Central Repository of all the accredited gTLDs along-with their single abuse point of contact could be maintained and updated regularly which makes it easier for users to access and communicate in case of any abuse-related incidents.

4. Question: How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?

Safeguard: Create a Draft Framework for a High Security Zone Verification Program
The framework could be tested on the TLDs with maximum proportion of abuse identified in a specific period to implement the High Security Zone verification process identified for the banking and pharmaceutical TLDs.