22 January 2016

Subject: SAC077: SSAC Comment on gTLD Marketplace Health Index Proposal

The Security and Stability Advisory Committee (SSAC) welcomes the opportunity to comment on the gTLD Marketplace Health Index Proposal in the Public Comment Forum that opened on 17 November 2015 and is scheduled to close on 22 January 2016.[1] The SSAC notes that SSAC member Greg Aaron, in his personal capacity, submitted his own thoughtful comments to the forum on 18 November 2015, and we as a committee strongly agree with all of his comments.[2] We expand on some of his comments and offer others.

First, and most importantly, Greg observes that:

> *...some of the proposed KPIs are crafted around data that is currently available. That makes them cost-effective to collect, but it does not mean that the data is always fit for the designated purpose. In some cases ICANN may need to develop new sources of data.*

The SSAC strongly supports this view, and further emphasizes that ICANN is approaching the problem backwards by starting with data that is already easily available. Developing a Key Performance Indicator (KPI) must first start with the insight into the ecosystem that the KPI is intended to convey, then drill down on what metrics best convey that insight, which actors have access to data or measurement capability to contribute to those metrics, and how to incentivize those actors to provide that data and measurement. The SSAC warns that, at least for metrics related to security, including consumer trust, and stability of the marketplace, relevant KPIs will require access to data that is not currently being shared (or perhaps not even being collected) by registrars or registries. For metrics related to economics and marketplace health, an ICANN-commissioned economics analysis in 2010 of the then-proposed new generic Top Level Domain (gTLD) program concluded that:

> *...in order to derive the greatest informational benefits from the next round of gTLD introductions, ICANN should adopt practices that will facilitate the assessment of the net benefits from the initial rollout of additional gTLDs. Specifically, ICANN should require registries, registrars, and domain names registrants to provide information sufficient to allow the estimation of the costs and benefits of new gTLDs.*[3]

[1] See https://www.icann.org/public-comments/gtld-marketplace-health-2015-11-17-en.
[2] See http://forum.icann.org/lists/comments-gtld-marketplace-health-17nov15/msg00000.html.
[3] See https://www.icann.org/en/topics/new-gtlds/economic-analysis-of-new-gtlds-16jun10-en.pdf June 2010.

The SSAC's recent investigation that led to the publication *of SAC074: SSAC Advisory on Registrant Protection – Best Practices for Preserving Security and Stability in the Credential Management Lifecycle* [4] provided additional evidence for this conclusion. In that study, the SSAC found that the lack of consistently available information about data breaches at registrars and registries, and the nature and impact of attacks that may use credential management vulnerabilities as a vector, leaves the SSAC without some useful data that would help it analyze those problems,[5] and which is related to the objectives of the Marketplace Health Index.

The SSAC notes that to develop and maintain effective metrics of security and stability of the gTLD ecosystem, ICANN will have to undertake auditing activity, including mandating future disclosure of aspects of registry and registrar operations and behavior, in a form that emphasizes consumer protection over industry norms.

Second, the SSAC notes that recommendation III. (b) suggests that ICANN reference the "Total number of unique phishing reports, as measured by Anti-Phishing Working Group reports." There are additional categories of domain registrations that are reported for abusive, fraudulent, or malicious purposes. Some of these include spam and malware campaigns, as well as domains used in botnet control operations. These present greater security problems for Internet users, are obtained via registration systems, and affect user perceptions of Internet security and usability. ICANN should collect and disseminate information about known categories of how domain registrations are used for abusive and fraudulent purposes. Note that it is important to distinguish between domains that were actually registered for fraudulent/abusive purposes versus domains compromised subsequent to registration via a hacking attack or account compromise. Such activities are partially reflected in the following metrics, which we suggest as additional KPIs that should be tracked in aggregate across the entire breadth of the gTLD marketplace as well as at the registry and registrar level as appropriate:

- Total number of abuse complaints involving malicious or abusive registrations (data will likely need to be normalized to account for repetitive and/or invalid complaints);
- Total number of unique domains that had complaints filed against them;
- Total number of domains suspended for abuse;
- Total number of domains suspended for fraudulent payment;
- Total number of domains suspended by registry due to inaction by registrars (domain suspension requests sent by registries to registrars);
- Total number of complaints against resellers; and
- Total number suspensions of reseller credentials.

To the extent that data to create these KPIs is not currently available because the relevant actors are not collecting or sharing it, ICANN should require the contractual disclosure of such data as soon as possible.

---

[4] See Recommendation 1 of SAC 074, available at https://www.icann.org/en/system/files/files/sac-074-en.pdf.
[5] See https://www.icann.org/groups/ssac/charter. The second item is: "2. To engage in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and to advise the ICANN community accordingly. The Committee shall recommend any necessary audit activity to assess the current status of DNS and address allocation security in relation to identified risks and threats."

Third, the SSAC supports ICANN's proposal to report the number of data security breaches reported by registrars, as required by the 2013 RAA. Such a proposal is in line with SSAC's recommendations in SAC074. However, the SSAC disagrees with the hypothesis (in section III.a) that "A smaller number of security breach reports could correlate to a stronger perception of marketplace stability among consumers." The number of reported breaches does not correlate to the perception of stability of the marketplace. Rather it reflects what is currently an ineffective and incentive-misaligned reporting mechanism. The SSAC also emphasizes that measuring perceptions of stability, or consumer trust, is different from measuring the actual stability and the actual security of the Domain Name System (DNS) infrastructure. ICANN should first focus on metrics that will objectively measure actual security and stability, informing consumers as to what they should trust in the first place. KPIs that include the type of breach, the number of similar breaches reported, and the number of affected users, are more reflective of actual security, which may also be reflected in consumer perceptions once consumers have access to such KPIs. The SSAC suggests these KPIs be incorporated into Section II, Trusted gTLD Marketplace. This section should also include a measurement of the number of registrars accepting Delegation Signer (DS) records.[6] ICANN should consider integrating external sources of information on DNSSEC in new gTLDs, showing signed domains per TLD, and by registrar, to illustrate adoption and availability of DNS Security Extensions (DNSSEC).[7]

Fourth, only one of the three metrics in Section III reflects registry stability, the other two reflect security. Other stability concerns that merit metrics include the frequency and impact of TLD registries and/or registrars going out of business or merging with other businesses.[8] Of further concern are impacts from a TLD being withdrawn completely if the registry of last resort process[9] does not complete with a new registry operator for an abandoned TLD. ICANN should prepare metrics and tie them to KPIs to reflect the impact of market dynamics on DNS stability.[10]

[6] ICANN currently collects this data at https://www.icann.org/resources/pages/deployment-2012-02-25-en, but these figures may not be current. The deployment graph at https://www.icann.org/resources/pages/deployment-graph-2012-02-25-en is also an available data point.
[7] See https://ntldstats.com/dnssec.
[8] See https://www.icann.org/resources/pages/gtld-registry-agreement-termination-2015-10-09-en#notice.
[9] See gTLD registry Transition process, https://archive.icann.org/en/topics/new-gtlds/registry-transition-processes-clean-30may11-en.pdf.
[10] By some accounts, almost half of new gTLDs are currently operating at a fiscal loss. http://www.circleid.com/posts/20160104_infographic_2015_new_gtld_year_in_review/. We do not know the method for computing this figure, and acknowledge the opacity of the financial health of the ecosystem is another systemic risk to robustness, consumer trust, and market stability.

Finally, we draw attention to a publication in Association for Computing Machinery (ACM) SIGCOMM's Internet Measurement Conference 2015, "From .academy to .zone: An Analysis of the New TLD Land Rush,"[11] which includes:

> *We take a comprehensive approach to understanding how registrants use domain names in ICANNs new TLD program. We used data from many sources, including zone file data available to researchers, extensive crawls of Web and DNS information, and public data from ICANN, registries and registrars. We determined that only 15% of domains purchased by a registrant show behavior consistent with primary registrations and that domain parking drives over 30% of registrations in the new gTLD zone files. We use domain pricing information to estimate that only half of all registries have recouped their application fee in wholesale revenue. Similarly, we conservatively estimate that registrants have spent roughly $89 million USD on domain registrations in the new TLDs. Finally, we validate the expectation that users visit fewer new domains in new gTLDs than those in old, and that new domains are more than twice as likely to appear on a commonly available blacklist within the first month of registration. Taken together, our findings suggest that new gTLDs, while accruing significant revenue for registrars, have yet to provide value to the Internet community in the same way as legacy TLDs.*

The authors emphasize that their data does not reveal why new gTLDs consistently contribute to higher rates of abusive behavior. ICANN should develop metrics that would identify which TLDs are hosting domains engaged in abusive behavior.

We encourage ICANN to take a step back from what existing data is available and consider how best to inform the larger community, especially consumers, with respect to the security and stability of the DNS marketplace.

Patrik Fältström
Chair, ICANN Security and Stability Advisory Committee (SSAC)

[11] From .academy to .zone: An Analysis of the New TLD Land Rush. http://conferences2.sigcomm.org/imc/2015/papers/p381.pdf. (Related papers by same authors: XXXtortion? Inferring Registration Intent in the .XXX TLD, http://cseweb.ucsd.edu/~voelker/pubs/xxxtld-www14.pdf The BIZ Top-Level Domain: Ten Years Later, http://www.sysnet.ucsd.edu/sysnet/miscpapers/dot-biz.pam12.pdf.