Registries Stakeholder Group Statement

Issue: **Statistical Analysis of DNS Abuse in gTLDs - Final Report**

Date statement submitted: **19 September , 2017**

Reference URL: https://www.icann.org/public-comments/sadag-final-2017-08-09-en

Background

Study commissioned by the Competition, Consumer Trust, and Consumer Choice Review Team (CCTRT) to measure rates of common forms of abusive activities in the DNS.
Contractor: Delft University of Technology and SIDN Labs.

Registries Stakeholder Group (RySG) comment:

The Registries Stakeholder Group (RySG) welcomes the opportunity to comment on the final report[1] of the Statistical Analysis of DNS Abuse in gTLDs.

Foremost, we appreciate the work undertaken by researchers from Delft University of Technology and the Foundation for Internet Domain Registration to apply quantitative research methodologies to better understand trends in the occurrence of abuse in the DNS. We applaud ICANN for commissioning and funding the study and encourage the overall reliance on empirical research to understand trends in the DNS and support the development of policies that improve the provision of domain services for users and service providers alike.

Allow further breakdowns of data to better-target abuse research.

The RySG is not surprised to learn that most of the abuse in gTLDs can be localised and attributed to a limited number of TLDs and that 'approximately one third of the new gTLDs available for registration did not experience a single incident in the last quarter of 2016'. This finding refutes the sometimes-heard general statements that abuse is widely spread throughout all gTLDs. We would like to see future studies include further cross-segmentation of its findings (e.g. breakdowns by registry backend, registry operator, or registrar family) to better understand how practices by registries or registrars correlate with abuse.

Identify more effective mechanisms for handling abuse rather than ineffective TLD-level mechanisms.

The RySG notes the study's key observation: the new gTLD program and corresponding increase in the number of registries has NOT resulted in a net increase in total abuse across all gTLDs. The fact that there is NOT more total abuse to date amplifies the inherent weakness in an abuse mitigation model that relies strictly on registries to combat online abuse, as was endeavored through the new gTLD safeguards. Registries should not be a target for combating online abuse. More nuanced forms

[1] While we understand that the report is in its final iteration and the research methodology adopted generally sound, we would like to add some minor methodological recommendations, to be taken into account if the study is repeated or similar studies are conducted in the future. We have included these recommendations as an addendum to the comment.

of enforcement and involvement of additional parties is imperative if the goal is to impact the degree to which abuse occurs.

Balance conclusions from the report about the impact of registry services or models against other, positive, impacts to registrants.

Despite the fact that the researchers did not conduct any cross-segment analysis on most of these factors, the conclusion suggests correlations between abuse and some of the additional services and practices by registry operators or registrars stating:

'*Competitive domain registration prices, unrestrictive registration practices, a variety of other registration options such as available payment options, free services such as DNS or WHOIS privacy, and finally the increased availability of domain names decrease barriers to abuse and may make some new gTLDs targets for cybercriminals*.'

However, previously, the study itself says '…the usage of Privacy and Proxy services for abusive domains is not that high.' Figure 27 shows that only 5 to 15 percent of newly registered abusive domain names use privacy services, far lower than the overall share of domain registrations using privacy or proxy services. The study also notes that even though other models suggest that registry differentiators can predict abuse, its 'results indicate that none of the registry operators have statistically significant effect on the abuse counts.' Furthermore, these services often answer a concrete demand and/or provide tangible benefits to legitimate registrants and Internet users, for example:

- The provision of free privacy services empowers registrants to protect their privacy when registering a domain name and protects them from abuses of the WHOIS database like harvesting registration data for spam purposes.
- Offering domains at low prices can help bring more registrants online, particularly in developing areas, and provide increased competition in the marketplace for domain registrations (one of the stated goals of the new gTLD program). Attempts to curb abuse by artificially raising prices for domain names should be avoided due to the likelihood of distortive effects on competition in the marketplace for domain names.

Therefore, we urge the CCTRT and the ICANN community to also account for the benefits such services present to registrants when considering whether and how to address the potential impacts on abuse.

Conclusion

Given the report's critical finding that the introduction of gTLDs did not increase the aggregate amount of abuse in the DNS and that none of the required safeguards appears to have impacted the behavior of bad actors in either legacy or new gTLDs, we believe the report underscores the inherent weakness of addressing abuse at the registry level. We urge the CCTRT, Board, and community to reconsider the expensive and ineffective safeguards and take these findings into account as it reviews abuse related practices in the 2012 round and going forward, as well as to avoid overactive conclusions that could have distorting effects on the marketplace for gTLDs or negative impacts on registrants.

Addendum: Methodological Recommendations

While we welcome empirical research of the kind found in the Statistical Analysis of DNS Abuse in gTLDs, and believe the methodology adopted by the researchers was generally sound we would like to call attention to the following methodological shortcomings of the report. We encourage the consideration of these comments with respect to research approach in the event the study is revised, or if this or a similar study is repeated in the future:

- **Encourage independent validation of findings:** The RySG observes the authors' reliance on statistical information from Spamhaus and SURBL in compiling data for their report. Some previous data supplied to the industry by these organizations was later found to include significant errors. While we applaud the use of data from multiple sources, we strongly encourage independent validation of these data sources, where possible.
- **Avoid assumptions and focus on empirical findings:** The study inserts opinion in several places. For example, the study refers to "malicious spam domains" when referring to domain names flagged for spam, which may or may not be malicious. In another place the survey says x% of domains were "abused by cybercriminals and blacklisted by Spamhaus." However, the researchers can only be sure that the domains were blacklisted by Spamhaus. Whether or not they were abused by cybercriminals is a legal determination.
- **Properly cite past recommendations:** The researchers use language like "regression analysis has been used before" and a "commonly observed trend", which implies third party corroboration. However, the footnotes supporting such statements refer to recent articles published by at least a subset of the researchers. If no other sources are available, it's more transparent to state "our previous work found."