ISPCP

The Internet Service Provider and Connectivity Provider Constituency
ICANN
27 September 2017

ISPCP Comments on ICANN Statistical Analysis of DNS Abuse in gTLDs

The Internet Service Provider and Connectivity Providers Constituency (ISPCP) welcomes the opportunity to submit comments on the ICANN Statistical Analysis of DNS Abuse in gTLDs (SADAG) Report. (See: https://www.icann.org/public-comments/sadag-final-2017-08-09-en.)

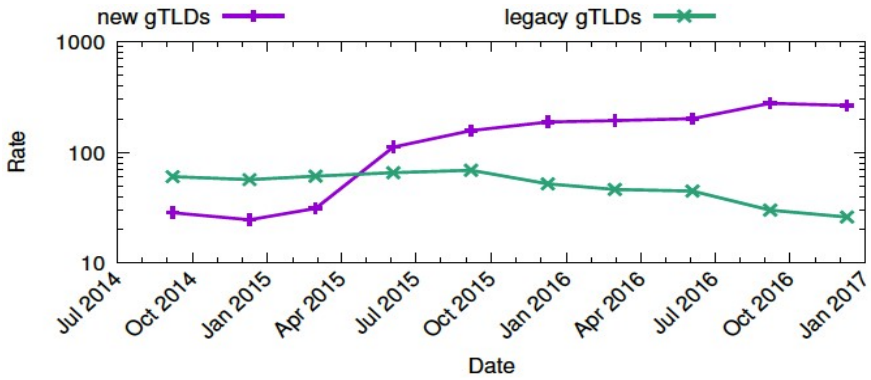
The purpose of this analysis is to explore how abuse of the DNS system affects the stability and reliability of the Internet. As the frontline to governments, consumers, and businesses, the ISPCP has an investment in both the stability of the DNS and a proper understanding of the roots of any instabilities. Given its role, the ISPCP's comments and concerns about the findings of the SADAG Report a) originate from observations about the SADAG methodology; and b) raise concerns about the implications of the SADAG's findings.

ISPCP Comments and Concerns About ICANN Enforcement Actions

The ISPCP is concerned that the SADAG fails to demonstrate that ICANN enforcement actions are having the impact one would expect for effective measures combatting abuse.

This concern arises from two observations:

- Overall, we believe the paper fails to deliver on its promise to discuss the effectiveness of the safeguards introduced by the new gTLD program. If those safeguards were effective, there would be an evident lower level of malicious registrations in new gTLDs than in legacy gTLDs. Instead, the opposite is true, rates of abuse among the new gTLDs are almost 10 times greater than legacy gTLDs (57 per 10,000 registrations in legacy TLDs vs. 527 per 10,000 in new gTLDs), suggesting that those safeguards are not effective.
- The results for one or two registrars, in particular, are the cause for major concern within our Constituency. Despite the report concluding that enforcement action by ICANN had an 'immediate and dramatic effect' in reducing DNS abuse, the evidence offered does not support that fact. For example, there are 15 gTLDS where at least 10% of all the registered domains are blacklisted by Spamhaus. Registrations by at least two registrars were skewed toward abusive registrations. This suggests that more enforcement action by ICANN, including better distribution of these enforcement actions and more transparency about registrar reputation levels of abuse, would be helpful.



- The SADAG indicates throughout that criminals now prefer just to register malicious domains rather than going to the trouble of compromising third party domains. This suggests that the safeguards surrounding registration of domains are failing to address stability, security and resilience issues, as suggested in the figure above.

ISPCP Comments and Concerns About SADAG Methodology

The ISPCP is concerned that the SADAG's analysis is skewed in ways which lead to inappropriately interpreted results.

- While the SADAG methodology is robust and explained fully to the audience, it carefully states that only a sample of legacy gTLD data was used in comparison to scan the whole zone of the new gTLDs. This would suggest the possibility of a skewed sample and misinterpreted, inaccurate results. In addition, this makes it impossible to compare results in future years where the analysis is repeated.
- The ISPCP notes that primary sources for abuse data have comparatively low levels of overlap when measuring for the same abuse method (i.e. phishing, spam, malware). This suggests that the lists themselves do not represent the full picture of abuse occurring in the DNS space, or within the sources. In turn, this would tend to under-report the levels of DNS abuse when taken through into the zone file analysis. Given the possibility that abuse has been inaccurately reported, the ISPCP recommends further exploration of these shortcomings and sources.

The concern about methodology extends to a needed consideration for the special concerns of new gTLDs. Three areas of note are:

a) The report notes the four categories of new gTLDs (standard/community/geographic/brand) and their differences in terms of registration policies as background, yet the potential differences between these new gTLDs in terms of abuse is poorly reflected in the conclusions. For example: in its background section, the study "excludes the great majority of brand TLDs" for which SLDs cannot be registered by Internet users or alludes to more stringent conditions which may apply to registrants for Geographic TLDs. That "caveat", however, may not be reflected in the conclusions. Or, the SADAG report's finding that the amount of "maliciously registered" appear higher in new gTLDs would seem to apply to all new TLDs - irrespective of their nature and indiscriminately if not equally to standard, community, geographic and brand TLDs. It would be unfortunate both in terms of methodology and interpretation of the findings.

b) Further, in terms of methodology, very little is said about the selection of samples (and the criteria used for this selection) and both whether and why those are believed to be representative of the whole 'population' of TLDs or data. An estimation of the error to be expected between different samples would have made it possible to ascertain the findings. And,
c) Regarding regression models, it is said that one fits the data and samples, but it is not said whether there might be other, potentially better, regressions which could have provided a better fit. This requires further exploration.

Final Matters of Support, Clarification, or Concern

While the SADAG report is a robust and ambitious analysis of abuse within the DNS, and the constituents of the ISPCP appreciate the time and effort put into the study, it is evident that the study requires either a second phase, additional source material, or a revised analysis, specifically:

- It is mentioned only in passing that abuse and price are correlated, for example. Prices from 50 cents to 1 dollar (U.S.) are tied to abusive registrations. However, this ignores mentioning that the .top gTLD is offered at 10 cents per domain for multiple registrars. Given the evidence that price and abuse are tied together, this would require further exploration.
- As speculation and defensive registrations dominate the growth of registrations in the DNS and there are new gTLDs and registrars where there are greater than 50% abusive registrations, including one registrar where 90% of the domains are reported as abusive, then an analysis of this registrar's attraction is required. Is this something that any member of the ISPCP might encounter? Or is this a deliberate business strategy?

Again, the ISPCP is thankful for the opportunity to submit these comments, concerns, and questions of clarification. The ISPCP thanks members, volunteers and the all involved in the creation of the SADAG for their work on this process and stands ready to assist.