The ICANN GNSO "Business Constituency"

Comment on report of Statistical Analysis of DNS Abuse in gTLDs

Status: FINAL

Version: 8

27-Sep-2017

Business Constituency Submission

GNSO//CSG//BC

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants, as defined in our Charter:

> The mission of the Business Constituency is to ensure that ICANN policy positions are consistent with the development of an Internet that:
>
> 1. promotes end-user confidence because it is a safe place to conduct business
> 2. is competitive in the supply of registry and registrar and related services
> 3. is technically stable, secure and reliable.

This document builds upon earlier comments by the BC on related issues and topics:

> BC Comment on new gTLD Program Safeguards to Mitigate DNS Abuse[1]
> BC comment on Framework for Registry Operators to Respond to Security Threats[2]
> BC Comment on Proposed Amendments to Base New gTLD Registry Agreement[3]
> BC Comment on the Review of Competition, Trust, and Choice from new gTLDs[4]
> BC Comment on the Phase II Assessment of Competitive Effects of New gTLDs[5]

SUMMARY: STATISTICAL ANALYSIS OF DNS ABUSE IN GTLDS

The Statistical Analysis of DNS Abuse in gTLDs Report ("SADAG Report") was requested by the Competition, Consumer Trust and Consumer Choice Review Team (CCTRT) and undertaken by a joint team comprised of researchers from Delft University of Technology (TU Delft) and the Foundation for Internet Domain Registration in the Netherlands (SIDN). The objective of the study was to analyze levels of technical abuse in legacy and new gTLDs with the intention of ascertaining how the introduction of new gTLDs has impacted DNS abuse.

The BC notes several key findings and observations from the Report:

1. Although the Report contains important statistics and data, it did not make conclusions regarding the effectiveness of the safeguards introduced by the New gTLD Program. If those

---

[1] http://www.bizconst.org/assets/docs/positions-statements/2016/2016_05may_bc-comment-on-safeguards-to-mitigate-dns-abuse.pdf (May 2016)

[2] http://www.bizconst.org/assets/docs/positions-statements/2017/2017_07July_31%20BC%20comment%20on%20Framework%20for%20Registries%20to%20respond%20to%20Security%20Threats.pdf (July 2017)

[3] http://www.bizconst.org/assets/docs/positions-statements/2016/2016_07july_20%20bc%20comment%20on%20proposed%20gtld%20base%20registry%20agreement%20final.pdf (July 2017)

[4] http://www.bizconst.org/assets/docs/positions-statements/2017/2017_05May_19%20BC%20Comment%20on%20CCTRT%20recommendations.pdf (May 2017)

[5] http://www.bizconst.org/assets/docs/positions-statements/2016/2016_12december_5%20bc%20comment%20on%20phase%20ii%20assessment.pdf (Dec. 2016)

safeguards had been effective, there would have been an observable reduction in the level of malicious registrations in new gTLDs as compared to legacy gTLDs.

2. While the introduction of new gTLDs does not appear to have increased the aggregate amount of abuse in the DNS, there was an observed decrease in the number of malicious registrations in legacy gTLDs.
3. New gTLDs experienced a rate of abuse that was almost 10 times higher than the rate experienced in legacy gTLDs.
4. Since the inception of the new gTLD program there is a discernable shift in the distribution of new gTLD abuse away from legacy gTLDs and toward new gTLDs for types of abuse that depend on low-cost, high-volume registrations.
5. Other types of abuse that depend more heavily on the reputation of the domain name in question (e.g., compromised domains, phishing, trademarks) have not seen a comparable shift away from legacy gTLDs and toward new gTLDs.
6. The level of abuse in a particular TLD appears to be influenced by both price and registry policies and enforcement:
    a. Lists of TLDs with the highest concentrations of abuse are dominated by TLDs with extremely low-cost pricing structures or promotions.
    b. Steps taken by certain registries appear to have a significant impact on reducing abuse in that TLD, despite low cost.
7. Some registrars and new gTLD operators appear to operate their businesses in ways that are overly permissive of domain abuse, with references made to registrars and gTLD registries with concentrations of abuse above 50 percent, including one with 90 percent concentration.

OVERALL STATEMENT FROM THE BC

In general the BC welcomes this report and its conclusions. The BC is an ardent advocate for increased and improved empirical research about the DNS, particularly with respect to abuse[6].

Pursuant to our mission to promote end user confidence, a safe business environment, and technical stability, security and reliability, the BC looks forward to addressing issues identified by the SADAG Report. We suggest that the CCTRT use these findings to propose targeted improvements to the New gTLD program that will be more effective in reducing DNS abuse.

The BC is particularly hopeful that these new insights, empirical information, and statistical analysis are used in determining direction and nature of any future expansion of the gTLD space.

[6] The BC notes that the SADAG Report relies heavily on data provided by Spamhaus, a third party organization. There are additional sources for published abuse analysis, such as the DomainTools study at https://blog.domaintools.com/2017/05/the-domaintools-report-spring-2017/

On the basis of key findings, listed above, the BC makes the following recommendations in response to the SADAG Report. We urge ICANN, the CCTRT, and the community at large to consider the findings of these studies and these recommendations as it works to curb abuse in the DNS.

BC RECOMMENDATIONS

Increased Compliance Scrutiny on Registries with High Abuse Rates

The higher reported rates of abuse in new gTLDs, as compared to legacy gTLDs, supports the need to review and revise the effectiveness of safeguards and registration policies and apply empirical findings to make them more impactful.

These findings should also be used to make ICANN compliance's operations more targeted, efficient, and effective by placing greater compliance scrutiny on those contracted parties that are experiencing excessively high abuse rates. These should also lead to, inter alia, requiring those registries to submit and adhere to detailed mitigation plans designed to reduce the rates of abuse.

Future Abuse Studies Should be Conducted and Expanded to Include Additional Breakdowns of Abuse by TLD and Registry

The BC recommends that ICANN commits to publicly posting relevant abuse data on an ongoing basis as part of its "Open Data Initiative," and to conducting a DNS Abuse Study every two years, to include practical suggestions for improvement. The design of future reports should be improved with additional information, to inform future policy work. For example, Table VIII and Table IX show that 37.09 and 49.44 percent of all domains appearing in StopBadware and SURBL Blacklists, respectively, were registered using a registrar located in Gibraltar. Subsequent analysis of the surprising findings pinpoint a single registrar, Alpnames Limited, which features tools that allow for random generation and registration of thousands of domain names in a single command, as the single source of the high concentration of abuse.

This suggests that while behavior by registries and registrars with respect to abuse handling is highly varied, some registrars and potentially registries operate their businesses in ways that encourage or facilitate abusive registrations.

Further cross-segmentation of the results by registry or registrar family would help to distinguish negligent actors from good actors, as well as help determine practices and policies, whether they be pricing and promotion structures, acceptable use policies and enforcement techniques, or technical tools for abuse monitoring and handling, which are most effective for limiting abuse.

Consider Linking Incentives to Good Practices for Abuse Handling

Findings about the linkage between domain name price and abuse data offers guidance for further study:

> "The registry operators of the most abused new gTLDs compete on price. We found that their retail registration prices were occasionally below US $1 or even US $0.50, which was lower than the registration fee for .com domains." (SADAG Report, p. 25)

We do not advocate regulation to artificially raise the price of domains as a method to curb abuse, given the potential for distorting effects on the market. But as we noted in our Jul-2017 comment on the new Base Registry Agreement:

> While it is not ICANN's role to set and regulate prices, it may be useful for ICANN to collect data on a range of registry (and registrar) activities, including pricing at the wholesale and retail level (and domain name abuse). This data might establish a correlation between free/ low prices without abuse safeguards and abusive domain name practices. This proposal is consistent with previous BC input on the development of a new gTLD Health Index.

A more nuanced scheme of incentives could be used to reward registries that act as good stewards of the DNS ecosystem, while excluding bad actors. One example could be linking the level of registry fees to registry practices or policies to curb abuse, or providing credits toward these fees for registries that demonstrated low levels of abuse. We believe that differentiation of fees based upon abuse levels and practices could be justified given the greater costs imposed on ICANN and the community at large by registries and registrars that operate their businesses in ways that are overly permissive of abuse.

The data could also be used to make ICANN compliance's operations more targeted, efficient, and effective by placing greater compliance scrutiny on those contracted parties that are experiencing excessively high abuse rates.

Endeavor to Address Abuse Effectively

The BC has previously expressed concern that businesses are driven to register domain names as " defensive" against potential abuse. We ask the CCTRT to consider recommendations that would reduce the perceived need for "defensive" registrations that businesses feel forced to make to guard against abuse that directly undermines consumer trust and results in consumer detriment.

Lastly, the report shows a tendency of abuse to leapfrog between TLDs on the basis of price and abuse policies and procedures, even where overall level of abuse in the ecosystem remain unchanged. This brings up some of the limitations of addressing domain abuse at the TLD level, since a domain that is suspended by one registry or registrar can easily be re-registered elsewhere.

This suggests the need for additional GNSO policy work to curb abuse so that efforts don't simply result in redistribution of abuse that leaves the overall impact on the ecosystem unchanged.

--

This comment was drafted by Waudo Siganga, Stephanie Duchesneau, Margie Milam, Marie Pattullo, Chris Wilson, and Marilyn Cade.

It was approved in accord with the BC Charter.