At-Large Workspace: Statistical Analysis of DNS Abuse in gTLDs (SADAG) Report

Public Comment Close	Statement Name	Status	Assignee (s)	Call for Comments Open	Call for Comments Close	Vote Open	Vote Close	Date of Submission	Staff Contact and Email	Statement Number
27 September 2017	Statistical Analysis of DNS Abuse in gTLDs (SADAG) Report	No Statement	TBC						Brian Aitchison brian.aitchison@icann.org	TBC

Hide the information below, please click here >>

- Comments Forum

Brief Overview

Purpose: Public comment is sought on the data, methodology, and results of this report.

Current Status: The report is under review by the Competition, Consumer Choice, and Trust Review Team (CCTRT) during the public comment proceeding.

Next Steps: Findings from the SADAG study, as well as any relevant public comments, will be incorporated into the CCTRT's Final Report as the CCTRT deems appropriate.

Section I: Description and Explanation

The CCTRT has sought to measure the effectiveness of a number of technical safeguards developed for the New gTLD Program in mitigating various forms of DNS abuse. As part of this process, the CCTRT requested a comprehensive DNS abuse study to analyze levels of abuse in legacy and new gTLDs, which would produce a baseline set of data for future analyses.

The SADAG study serves to inform the CCTRT's analysis of potential factors explaining abuse rates in a given gTLD. The study analyzes rates of spam, phishing, and malware distribution in the global gTLD DNS from 2014 to 2016, distinguishing between legacy and new gTLDs.

The study provides measures and analysis of:

- Absolute counts of abusive domains per gTLD and registrar from 1 January 2014 until 31 December 2016
- Abuse rates, based on an "abused domains per 10,000" ratio (as a normalization factor to account for different TLD sizes), per gTLD and registrar from 1 January 2014 until 31 December 2016
- Abuse associated with privacy and proxy services
- Geographic locations associated with abusive activities
- Abuse levels distinguished by "maliciously registered" versus "compromised" domains
- Effects of DNSSEC, domain parking, and registration restrictions on abuse levels

The aim of this study is to enable the CCTRT to determine abuse level correlations between registries and registrars, gTLD zones, and, to the extent possible, corresponding safeguards. This research will also serve as a baseline for future CCTRTs and other review teams, including the Security, Stability and Resiliency Review Team, which began its work in March 2017.

Section II: Background

In preparation for the CCTRT's review of "safeguards put in place to mitigate issues involved in…the expansion" of the gTLD space as mandated by its Affirmation of Commitments, ICANNissued the report "New gTLD Program Safeguards to Mitigate DNS Abuse." This report analyzed the history of DNS abuse safeguards tied to the New gTLD Program. In doing so—and with the input of the community via two webinars held in January 2016 and a public comment process in March 2016—the report assessed a number of means to define and measure DNS abuse.

However, challenges arose in definition and measurement of abusive activities, as some are considered abusive in some jurisdictions but not others. Some of these activities, such as those focused on intellectual property violations, are interpreted differently not only in terms of substance but also in terms of available remedies depending upon the jurisdiction. Another challenge is the lack of data available regarding certain types of abuse. Nonetheless, some common activities are widely regarded as abusive and also generate useful data for analysis; these include spam, phishing, and malware distribution.

The CCTRT recognized the absence of a comprehensive comparative study of DNS abuse in new and legacy gTLDs that would allow them to assess the effectiveness of New gTLD Program safeguards. The SADAG study aims to fill this absence, and serve as a baseline for future studies focused on explaining the variation in abuse rates in different gTLDs.

Section III: Relevant Resources

- Statistical Analysis of DNS Abuse in gTLDs (SADAG) Final Report [PDF, 2.23 MB]

Section IV: Additional Information

- New gTLD Program Safeguards Against DNS Abuse
- Request for Proposal Announcement – DNS Abuse Study

Section V: Reports

Staff Contact

Brian Aitchison
brian.aitchison@icann.org

FINAL VERSION TO BE SUBMITTED IF RATIFIED

The final version to be submitted, if the draft is ratified, will be placed here by upon completion of the vote.

FINAL DRAFT VERSION TO BE VOTED UPON BY THE ALAC

The final draft version to be voted upon by the ALAC will be placed here before the vote is to begin.

FIRST DRAFT SUBMITTED

The first draft submitted will be placed here before the call for comments begins.