ICANN Specific Reviews – Competition, Consumer Trust and Consumer Choice Review (CCT)
Recommendation 16 - Implementation Documentation

Published on 30 September 2022

CCT Final Report https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf

Board resolution on CCT Final Report https://www.icann.org/resources/board-material/resolutions-2019-03-01-en#1.a

October 2020 resolution on a set of pending CCT Recommendations: https://www.icann.org/en/board-activities-and-meetings/materials/approved-resolutions-regular-meeting-of-the-icann-board-22-10-2020-en#2.a.rationale

Board resolution on a set of CCT Pending Recommendations https://www.icann.org/resources/board-material/resolutions-2020-10-22-en#2.a.rationale

- Recommendation submitted: September 2018
- Recommendation approved: March 2019
- Implementation completed: N/A

See https://community.icann.org/display/CCT/Implementation for more information on CCT implementation.

CCT Recommendation 16

Further study the relationship between specific registry operators, registrars, and DNS Security Abuse by commissioning ongoing data collection, including but not limited to, ICANN Domain Abuse Activity Reporting (DAAR) initiatives. For transparency purposes, this information should be regularly published, ideally quarterly and no less than annually, in order to be able to identify registries and registrars that need to come under greater scrutiny, investigation, and potential enforcement action by ICANN organization. (Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remedy problems identified,**)** and define future ongoing data collection.

* Per the 1 March 2019 Board action on the CCT-RT Final Report, the portion of the recommendation in brackets was passed through to the community groups the CCT-RT identified.

Board Action on CCT Recommendation 16

The Board notes that ICANN org will continue to collect data and generate monthly reports on an ongoing basis. DAAR itself is not and cannot be a compliance/enforcement tool. Rather, it is a tool that monitors third party reputation lists to indicate possible concentration of DNS security threats.

Final Implementation Report

ICANN's Domain Abuse Activity Reporting (DAAR) project is a system for studying and reporting on domain name registration and security threats (domain abuse) across top-level domain (TLD) registries. The overarching purpose of DAAR is to develop a robust, reliable,

verifiable, and reproducible methodology for analyzing security threat activity, which the ICANN community may use to make informed consensus policy decisions. It is up to the ICANN community to determine whether or how to use the reports derived from DAAR-collected data in policy deliberations.

ICANN org has been operating the Domain Abuse Activity Reporting (DAAR) for more than three years as well as publishing the results. ICANN org has established a group within the Office of the CTO (OCTO) dedicated to researching SSR related issues, including a focus on DNS security threats. Efforts within this group include the Domain Name Security Threat Information Collection and Reporting (DNSTICR) project (see the blog post).

Data collected out of the DAAR system is currently being used to generate monthly reports on an ongoing basis. These reports are made public at https://www.icann.org/octo-ssr/daar. In alignment with the CCT Recommendation 16, DAAR currently uses a documented set of reputation list providers to identify and track reported domain names associated with a specific set of security threats and abuse behavior across all generic and some country code top-level domain registries.

It should be noted that data collected by DAAR related to security threats and abusive behavior are derived from information collected by third-party reputation blocklist (RBL) providers. While these data are publicly available (potentially at some cost), they invariably come with licensing terms that may or do prohibit ICANN org's reproduction of those data. ICANN org continues to investigate ways in which it can publish more detailed DAAR reports. However, in the interim, the DAAR system and output was specifically designed to be reproducible by interested parties, so those interested in more specifics than that which is available in the public reports have avenues in which they can explore DAAR data. The DAAR reports do not (yet) associate names with specific registrars due to an inability to obtain data on the sponsoring registrar at the same granularity of registry level security threat metrics in DAAR, that is on a daily basis. The identification of a sponsoring registrar for a given domain name is only publicly available via the WHOIS system, however querying the registry WHOIS servers is rate-limited by most, if not all, registry operators. ICANN org continues to try to identify ways in which sponsoring registrar data can be obtained in bulk to enable reporting on registrars as is done for registries.

Internally, when clear outliers in terms of security threats or abusive behaviors become apparent within the DAAR data, ICANN org's OCTO staff notify ICANN org's Contractual Compliance. While the data DAAR collects is not, in and of itself, indicative of a security threat or abusive behavior, it does provide an indicator that additional scrutiny of the registry may be warranted.

ICANN org, through OCTO, continues to refine and evolve the DAAR system and is in discussions with the community on ways in which DAAR can be improved. It has begun to incorporate ccTLDs who volunteer to participate in DAAR and is looking at modifying the DAAR reports to provide additional and/or different statistical measures.

ICANN org continues its commitment to research and is actively working with the community to gain acceptance of naming registries and registrars that contribute to DNS security threats. The ability to expose more detailed data is dependent on community consensus. The ability to identify and report on specific registrars is dependent on registries granting access to *Bulk Registration Data Access* (BRDA) data for full research purposes,

In parallel, ICANN org, through OCTO, has initiated a project that uses similar reputation data, albeit limited to phishing and malware distribution threats, to identify potentially malicious

domain names that match a set of keywords related to COVID-19. Currently called DNSTICR - Domain Name Security Threat Information Collection and Reporting, when a potentially malicious domain name is identified, it is reported to bodies, e.g., the registry and/or registrar, that can take appropriate action. While this project is initially focused on COVID-19-related abusive names, it can be reused anytime a high profile event results in a surge in domain name registrations. Should there be events with a similar profile to the COVID-19 pandemic in terms of domain name registrations, ICANN org will be able to identify and report potentially abusive names with high confidence and in a timely fashion in the future.

Rationale

ICANN org will be continuously evaluating the security threat landscape and making adjustments to data analysis as the landscape changes. This recommendation is complete at the time of evaluation and implementation, as it is ICANN org's intent to not leave this in a static state. Therefore, ICANN org wishes to recognize the evolutionary nature of data collection and reporting and that any new CCT Review Team take that into consideration when evaluating the success of this recommendation's implementation.

In relation to CCT's measure of success; "Comprehensive, up-to-date technical DNS Security Abuse data is readily available to the ICANN Community to promptly identify problems, craft data-driven policy solutions, and measure the efficacy of implemented safeguards and ongoing initiatives. Furthermore, the next CCT Review Team will have a rich dataset on DNS abuse from which to measure safeguard efficacy.", at this time, ICANN does not publish the raw data to the community with the exception of providing each registry with their own abuse counts on a daily basis so they can compare their own data over time. Currently, the publicly available reports are aggregated analytics and visuals without reference to the underlying details. There is ongoing discussion within ICANN org and with the wider community as to whether ICANN org can and should publish this data at a more granular level.

Likewise, the above comment applies to the CCT's measure of success: "The review team also envisioned regular publication of such data, "enabling the community and the ICANN organization in particular to identify registries and registrars that need to come under greater compliance scrutiny and thereby have such behavior eradicated.".

Timeline

Expected implementation date: N/A
Final implementation date: N/A

Milestones

- DAAR - Regular reports [ongoing effort started in January 2019]
  Data collected out of the DAAR system is currently being used to generate monthly reports for gTLD registries on an ongoing basis. These reports are made public at https://www.icann.org/octo-ssr/daar. In addition, gTLD registries can access their own security threat scores via MoSAPI on a daily basis.
- DNSTICR - Relevant reporting [ongoing effort]