4 June 2019

RE: Comments Pertaining to the Domain Abuse Activity Reporting (DAAR) System

Jerry Upton
Executive Director
Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG)

Dear Mr. Upton:

Thank you for providing your comments on the Domain Abuse Activity Reporting (DAAR) project. This project is a work in progress and we always welcome suggestions for improvement.

The DAAR project aims to provide the community with abuse information to inform ongoing discussions regarding DNS abuse. Now that we have developed security threat metrics as discussed in the DAAR monthly reports[1], one of the first priorities is to provide registry operators with the ability to see their own abuse scores relative to the published anonymous averages.

We acknowledge your request to publish aggregate abuse metrics for each registry and registrar. While publishing this information would be in keeping with our commitment to transparency and thus, among the main purpose of DAAR, before taking any actions, we need to work with the various community stakeholders to determine the best way in which

this information should be published. In particular, given the tendency for the DAAR information to be misinterpreted, we need to ensure there is a clear understanding as to what the DAAR data is and isn't in the context of informing policy discussions. We encourage your ongoing participation in those discussions.

With regards to registrar-related abuse statistics, as you may be aware, rate-limiting of queries for the registrar identifier which is included in WHOIS data remains a challenge. We continue to research ways in which the registrar that is sponsoring a domain name can be obtained in a scalable fashion. As a result, the registrar level abuse metric is still under development.

Finally, please note that it is and has been a core requirement that the data behind DAAR originates from publicly available sources. The methodology behind DAAR was carefully designed to be replicable and reproducible by others in industry and academia. Therefore, in theory, any stakeholder should be able to replicate the methodology and obtain the same

---

[1] https://www.icann.org/octo-ssr/daar

results generated by DAAR. Accordingly, while we are working in publishing the abuse metrics, we would be interested to understand whether the reproducibility requirement is allowing the community members to successfully generate their own abuse metrics based on DAAR.

Again, thank you for providing your comments on DAAR and we look forward to M3AAWG's continued involvement in the evolution of the DAAR project.

Sincerely,

David Conrad
Chief Technology Officer, ICANN