Messaging, Malware and Mobile Anti-Abuse Working Group

M3AAWG Companion Document:
M3AAWG Comments on the Initial Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process

Version: .0

March 2020

The direct URL to this paper is: www.m3aawg.org/dns-crypto-recipes

This document is intended to accompany and complement the companion document, "M3 AAWG Tutorial on Third Party Recursive Resolvers and Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic" (www.m3aawg.org/dns-crypto-tutorial).

This document was produced by the M3 AAWG Data and Identity Protection Committee.

Table of Contents

Messaging, Malware and Mobile Anti-Abuse Working Group

781 Beach Street, Suite 302
San Francisco
California 94109
United States of America

www.m3aawg.org

Foreword

M3AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group, appreciates this opportunity to comment on the Initial Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process (https://gnso.icann.org/en/issues/epdp-phase-2-initial-07feb20-en.pdf). We make these comments in our capacities as cybersecurity professionals and researchers committed to ensuring the security and stability of the internet, including the domain name ecosystem.

This issue is very important to M3AAWG members. **Our 2018 Joint Survey published jointly with the Anti-Phishing Working Group** found that changes to WHOIS access following ICANN's implementation of the Temporary Specification is significantly impeding cyber applications and forensic investigations and allowing more harm to victims. M3AAWG appreciates the hard work of the EPDP Phase 2 team and the progress they have made to date. The successful completion of this policy and the ultimate implementation of a workable System for Standardized Access/Disclosure (SSAD) of Registration Data is key to organizations and individuals, including many of our members, that require access to registration data in order to detect threats, investigate new attack vectors and to understand trends aimed at protecting users and the Internet as a whole. This includes law enforcement authorities, both civil and criminal, who rely on the analysis and coloration of Registration Data obtained by private sector researchers and security. Failure to allow these professionals to access this data will threaten the security, stability and resiliency of the Internet as a whole and result in higher abuse rates, more harm inflicted on users and result in more criminal impunity on a global scale.

Given that context, M3AAWG has identified the following preliminary recommendations that represent the greatest concern to our members.

1. Preliminary Recommendation #12. Query Policy

In the course of investigations, especially those of a global nature, it is often necessary to request many thousands of requests for Registration data from the SSAD system. While we appreciate the need for any system to protect itself from abuse of all kinds, we are concerned that the definition of "abusive use" of the SSAD, specifically point #4, may inadvertently interfere with some investigations. E.g

> 4. Storing/delaying and sending high-volume requests causing the SSAD or other parties to fail SLA performance. When investigating abuse based on this specific behavior, the concept of proportionality should be considered.

Query policy limits enforced by the SSAD must not impede the access required by accredited investigators to detect, attribute and mitigate abuse on a global scale. The receipt of requests at this scale must not result in throttling or result in a situation where legitimate requests are rejected.

2. Preliminary Recommendation #9. Determining Variable SLAs for response times for SSAD

The definition and enforcement of SLA associated with response times is of high importance to ensuring a workable and effective SSAD system. We note that the ability of accredited cyber-security investigators to tag their requests as "Urgent Requests" is currently not possible given the current definition. At best it is unclear:

> "The criteria to determine whether it concerns an urgent request are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation."

Given most campaigns to attack internet users [consumers] are short lived by design, a maximum response time of 5 business days is neither acceptable nor sufficient. By then the damage will have been done. As such the definition of "Urgent Requests" must be updated to include the important work of cybersecurity investigators.

We suggest adding the following language to make it clear that accredited cybersecurity researchers can submit requests that have been tagged as Urgent.

> "For the avoidance of doubt, this includes issues related to malware, Botnets [and their command and control systems], phishing, pharming and abuse related to consumer fraud."

Finally, we note that the SLAs defined in Recommendation #9 focus on response times only. In order to ensure transparency of the system in addition to allowing accountability to the community there must exist a mechanism to measure the rate of disclosure of RDS data across all disclosers. As such an SLA that measures and tracks disclosure rates must be added to this recommendation. The data associated with this SLA must be routinely audited and reported publicly.

3. Preliminary Recommendation #7. Authorization for automated disclosure requests

In order to be effective, the SSAD system (as defined in the initial report) must support additional use cases that can be fully automated above and beyond the two currently specified (in Jurisdiction LEA and URS/UDRP due process). These must include use cases related to the needs of properly Accredited cybersecurity and anti-abuse investigators.

We note that additional use case review will be the subject of further discussion by the EPDP Phase 2 working group. In our review of the "Working Draft Use Case Candidates for Possible Automation"[1], we are encouraged that Use Case #7 "Identify infrastructure involved in botnets, malware, phishing, and consumer fraud" will be considered and believe strongly that an SSAD system that did not include this (or a similar) use cases would not address the needs of accredited cybersecurity and antiabuse investigators.

[1] https://community.icann.org/display/EOTSFGRD/Working+Draft+Use+Case+Candidates+for+Possible+Automation

4. Preliminary Recommendation #19. Mechanism for the continuous evolution of the SSAD

The need for a mechanism that ensures the SSAD system can evolve at Internet speed is a very important concept and policy must exist to support it. It is equally important that transparency, accountability and full participation by all stakeholders be assured and as such we insist that any mechanism involved in defining how the SSAD will evolve include stakeholders outside of the GNSO, including the SSAC, GAC and ALAC. In addition, decisions that result from this mechanism must not be subject to a vote from the GNSO Council that does not include the Advisory Committees.

5. Preliminary Recommendation #15. Financial Sustainability

M3AAWG is very concerned that the use of the SSAD may involve per transaction/requests charges. While we do not object to reasonable fees to ensure proper accreditation of members of the cybersecurity community, we would object to any financial sustainability model that may impose any per-transaction fees related to requests required during the course of a legitimate investigations.

Thank you in advance for your consideration of these comments.

As with all M3AAWG documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates to this paper.