M3AAWG

Messaging Malware Mobile
Anti-Abuse Working Group

From: Messaging, Malware and Mobile Anti-Abuse Working Group

Date: January 6, 2022

Subject: EPDP Phase 2A Policy Recommendations for ICANN Board Consideration

**Overall Comments:**

It is in the public interest for anti-abuse actors to be able to contact, and obtain information about, the registrant of a public resource such as a domain name, in order to address cybercrime, hacking, botnets, phishing, and other abuse. For bona fide actors with a legitimate interest, access to WHOIS must be effective, functional, timely, and efficient to ensure appropriate cybercrime and abuse response. Thus, we would like to voice our agreement with the recommendations made in SAC118, as released by SSAC on July 15th 2021.

The WHOIS plays a role in more or less any mitigation or response strategy that addresses DNS abuse and cybercrime within the DNS infrastructure. As there is no other avenue to tying a registration to a responsible party, the WHOIS is required to ensure the future safe and secure operation of the global identifier system and the internet as a whole. Thus, a robust WHOIS system and the security, stability, and resiliency (SSR) of the DNS are deeply linked.

The ICANN Board and Community should keep in mind that uniformity is extremely important for cybersecurity specialists and law enforcement but also individual data subjects. WHOIS policies, procedures and guidelines must be clear, straightforward and uniformly applied and enforced. Therefore, policies should use clear, prescriptive language and avoid voluntary clauses.

Without clear policy language, confusion will arise as to what rules and procedures are to be followed and actually implemented by different parties. Furthermore, some players may not comply with voluntary rules. Uniformity is required to ensure timely response to incidents. The current uncertainty (requests, time lines, etc.) is a major challenge for anti-abuse specialists.

Before embarking on the creation of a future access system, it would be useful to liaise with security communities that rely on the DNS to better understand what they need and require, some of which has been outlined above, in the M3AAWG and APWG WHOIS Study[1], and prior communications. SAC118 further illustrates how a workable system could be achieved.

[1] https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

As we have stated in our September 30, 2021 letter[2], “ICANN needs to enforce rules on registrant data access to protect individuals, public safety and security.” Only by setting standards and making them requirements, end users, cybersecurity specialists, and contracted parties have clarity on what happens to data and how it can be accessed.

**Specific Comments:**

**EPDP Recommendation #1**

> *The EPDP Team recommends that a field or fields MUST be created to facilitate differentiation between legal and natural person registration data and/or if that registration data contains personal or non-personal data. ICANN org MUST coordinate with the technical community, for example the RDAP WG, to develop any necessary standards associated with using this field or fields within EPP and the RDDS.*

It makes sense to differentiate between legal and natural persons, as different rules apply to these groups. However, to be workable, the field must be required for every registration, and used consistently with globally valid identifiers by all contracted parties.

As we stated in our September 30, 2021 letter[3], “ICANN must establish a functional system of access to all now redacted fields for trusted parties, accommodating both bulk users and those putting in manual requests.” And further: “All non-personal data should be readily available and publicly visible.”

Without consistent, global use and application of a field that clarifies what data can be accessed or displayed, there is little use in differentiation as we have outlined above. Timeliness, predictability, and cohesiveness are key requirements for a workable WHOIS system and for that, uniformity is required. Not making uniformity a requirement will increase the burden on contracted parties who take steps to resolve these challenges vis a vis those who remain inactive, while some, unfortunately, will leverage resulting inconsistencies to provide domain name registration services to abusive registrants.

**EPDP Recommendation #2**

> *The EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance below and clearly document all data processing steps. However, it is not the role or responsibility of the EPDP Team to make a final determination with regard to the legal risks, as that responsibility ultimately belongs to the data controller(s).*

As above, uniformity is required to ensure the WHOIS is functional and predictable for registrants, contracted parties, and cybersecurity specialists. Therefore, following relevant guidance and creating documentation should be mandatory. Making this voluntary will also burden those contracted parties who comply, while enabling those who choose to ignore the recommendation.

[2] https://www.m3aawg.org/sites/default/files/icann_recommendations_whois_survey_report-sept302021.pdf

[3] https://www.m3aawg.org/sites/default/files/icann_recommendations_whois_survey_report-sept302021.pdf

**EPDP Recommendation #3**

> *The EPDP Team recommends, in line with GDPR Article 40 requirements for Codes of Conduct, that the above developed guidance concerning legal/natural differentiation should be considered by any possible future work within ICANN by the relevant controllers and processors in relation to the development of a GDPR Code of Conduct. For the avoidance of doubt, this Code of Conduct is separate and distinct from the Code of Conduct referenced in the RAA and/or Registry Agreements. Consistent with GDPR recital 99, "When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations".*

While the creation of a code of conduct (CoC) is useful, a baseline CoC that applies to all registrars and registries is necessary to establish a functional and uniform system. As stated above, it is in the interest of end users, cybersecurity specialists, and contracted parties who care about security to establish systems and rules that are predictable and apply to everyone.

**EPDP Recommendation #4**

> *The EPDP Team recommends that Contracted Parties who choose to publish an intended to be pseudonymized registrant-based or registration-based email address in the publicly accessible RDDS should evaluate the legal guidance obtained by the EPDP Team on this topic (see Annex F), as well as any other relevant guidance provided by applicable data protection authorities.*

As we stated in our September 30, 2021 letter[4], "ICANN should require the creation of functional and workable solutions for contacting registrants that are easily accessible and automatable."

Therefore, the ICANN community should establish clear rules and requirements that apply to all registrars and registries. Providing a pseudonymized point of contact directly available to trusted parties via RDDP/SSAD should be a requirement for all registrations to enable registrants to be contacted.

The M3AAWG and APWG WHOIS Survey data[5] indicate that anti-abuse actors struggle with website-based contact forms, which is why we recommend the addition of privacy-preserving email contact addresses to the WHOIS.

Furthermore, pseudonymised registrant identifiers (this could be contact addresses or other data points) can be used for correlation and data analysis. These tasks are critical for incident investigations, while the use of pseudonymised identifiers would not expose PII and other protected data. Attempts to make such pseudonymised data available within or better across multiple registrars' portfolios are laudable and should be supported.

[4] https://www.m3aawg.org/sites/default/files/icann_recommendations_whois_survey_report-sept302021.pdf

[5] https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

Thank you in advance for your consideration of these comments.

Sincerely,

Amy Cadagin, Executive Director
Messaging, Malware and Mobile Anti-Abuse Working Group