M³AAWG Messaging Malware Mobile Anti-Abuse Working Group

To: Goran Marby, CEO, ICANN; Cherine Chalaby, COB, ICANN;
Rod Rasmussen, Chairman, ICANN SSAC
From: Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)
Date: October 18, 2018
Subject: Joint APWG/M³AAWG GDPR and WHOIS User Survey Results

Dear Sirs:

The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) is an industry association that comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation. We are the largest global anti-abuse industry association, with more than 200 member companies worldwide, bringing together all the stakeholders in the online community in a confidential, open forum. We develop cooperative approaches for fighting online abuse.

M³AAWG membership continues to follow the ICANN community's efforts to define an interim plan to ensure that the existing public display (disclosure) of domain name registration data complies with the European Union's General Data Protection Regulation (GDPR). To assist the ICANN community in this effort, M³AAWG has collaborated with the Anti-Phishing Working Group (APWG) in conducting a survey of cyber investigators to understand how ICANN's *Temporary Specification for gTLD Registration Data* has affected their access and usage of domain name registration information and their ability to mitigate abuse.

From our analysis of over 300 survey responses, we find that the changes to WHOIS access following ICANN's implementation of the EU GDPR, the Temporary Specification for gTLD Registration Data[1] ("Temp Spec," adopted in May 2018), is significantly impeding cyber applications and forensic investigations and allowing more harm to victims.

The policy has introduced delays to investigations and the reduced utility of public WHOIS data is a dire problem. Delays favor the attacker and criminal, who can claim victims or profit over longer windows of opportunity while investigators struggle to identify perpetrators or strip them of their assets (i.e., domain names) with limited or no access to the data that had previously been obtained or derived from WHOIS data. The loss of timely and repeatable access to complete WHOIS data is impeding investigations of all kinds, from cybercrime activities such as phishing and ransomware, to the distribution of fake news and subversive political influence campaigns.

In their responses, cybercrime investigators and anti-abuse service providers overwhelming report that the implementation of ICANN's Temp Spec introduces the following impediments to cyber security investigations:

Cyber-investigations and mitigations are impeded because investigators are unable to access complete domain name registration data through public WHOIS services in (near) real-time, as they had before the implementation of the Temp Spec. The partial data that are available through the public WHOIS services after redaction are insufficient to investigate or to respond to incidents.

The mitigation or triage of cyber incidents cannot be accomplished in a timely manner. Specifically, the need to request access to the non-public data elements introduces, at a minimum, delays of days in circumstances where mitigation prior to the adoption of the Temp Spec was often accomplished in hours or one day. Such delays allow attacks to remain active longer. Extended windows of operation put more Internet users in harm's way.

[1]Temporary Specification for gTLD Registration Data, https://www.icann.org/resources/pages/gtld-registration-data-specs-en

WHOIS has become an unreliable or less meaningful source of threat intelligence. The WHOIS contact data that is most relevant to investigators and has evidentiary value to law enforcement and prosecutors is generally not available through public WHOIS services since the implementation of the Temp Spec. (Note: even fraudulently composed, pseudonymous, incomplete, or inaccurate data is useful for assigning reputations or creating correlations; for instance, in tracing known perpetrators' latest criminal excursions in establishing spoof domain names.) Investigators have been using alternative data sources with mixed success.

Requests to access non-public WHOIS by legitimate investigators for legitimate purposes are routinely refused. Investigators indicate that the implementation of "WHOIS reveal" is largely not working. The Temp Spec is unspecific, implementation is not uniform, and the processes are poorly understood by investigators, domain name registrars, and domain name registries. The majority of survey responders report that investigators do not know how to request access to non-public WHOIS data. Registrars and registries disclose redacted WHOIS data at their individual discretion, often without reasonable justification.

Those who protect internet resources are also making more coarse blocking or mitigation decisions in the absence of what was formerly reliable data. Network operators and protective service providers, in fact, are blocking entire Top-level Domains. Investigators report that in circumstances where they are unable to use non-public WHOIS data to make blocking decisions about individual domains, and where they cannot establish associations across (very large) sets of suspicious domain names, they are exercising an abundance of caution and blocking more aggressively.

The utility of WHOIS has been severely damaged. Four months after the Temp Spec implementation, an alarming 17% of responders claim that public WHOIS service is no longer useful or reliable, and 13% have ceased using WHOIS entirely.

The redaction of WHOIS data is excessive. Investigators do not believe that it is necessary to redact legal entity point of contact data or point of contact data for data subjects outside the EU to comply with the EU GDPR.

Based on these findings, we encourage the ICANN organization and community to consider these recommendations during their ongoing deliberation of WHOIS policy:

1. **There must be an accredited access mechanism, providing tiered or gated access to qualified security actors.** A unified access program is necessary to restore predictable, automatable, swift access that balances privacy with legitimate use under GDPR. The technical mechanism would be RDAP (Registration Data Access Protocol).
2. **ICANN should *not* allow redaction of the contact data of legal entities**. Other WHOIS operators, such as the Regional Internet Registries and some European ccTLDs (Country Code Top Level Domains), do not redact data as aggressively as the Temp Spec allows.
3. **ICANN should adopt a contact data access request specification that will ensure consistency across all accredited registrars and gTLD registries.** The policy should be specific regarding the legitimate uses for which a timely completion of response is appropriate. These should align with the legitimate uses as described in the GDPR. A clear definition of "timely" should be included in the policy. Approved access requests should accommodate repeated access. Further, the specification should be specific with respect to:
    A. Format of request (for both forms of WHOIS services);
    B. Identification of the information required to be set forth in the request;
    C. Email addresses where requests can be sent;
    D. Specification of the documentation required for authenticating request; and
    E. Time limitation for a response to requests. We recommend that responses be processed in 24 hours or less.

4. **ICANN should ensure that the accredited access to redacted WHOIS data does not introduce delays in collecting or processing WHOIS data, and further, that the access not be encumbered by per request authorizations:** these simply do not scale for the volumes and purposes that investigators identified in their responses. We further ask that ICANN consider a framework wherein an accredited party be granted timely access and persistent access to complete WHOIS data.
5. **Recommendation 5: ICANN should reconsider the current redaction policy.** In the interest of serving data protection *and* legitimate needs to access complete WHOIS data, we urge ICANN to consider using secure hashes rather than redacting data. We call your attention to the proposal, *Public WHOIS Attributes, Securely Hashed (WhASH): Hashing Point of Contact Details in Public Domain Name WHOIS*, submitted 4 June 2018, by APWG's Board of Directors to ICANN CEO and Chairman of the Board[2].
6. **We ask that ICANN publish point of contact email addresses to provide investigators with an effective means of identifying domains associated with a victim or person of interest in an investigation**. Some European ccTLDs and the RIRs (Regional Internet Registries) are publishing email addresses in their public WHOIS. Consistency across WHOIS services will facilitate investigations across identifier systems.

We respectfully request that the ICANN organization, community and Board consider the attached survey report. The report is also published on the M³AAWG website under our Public Policy Comments and available directly at http://www.m3aawg.org/WhoisSurvey2018-10.

Thank you in advance for your consideration.

Sincerely,
[SIGNATURE]
/s/
Jerry Upton, Executive Director

Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)
781 Beach Street, Suite 302
San Francisco, California 94109
https://www.m3aawg.org

[2] https://www.icann.org/en/system/files/correspondence/jevans-to-marby-et-al-04jun18-en.pdf