M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

APWG

To: Göran Marby, CEO, ICANN; Maarten Botterman, COB, ICANN; Rod Rasmussen, ICANN SSAC

From: Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and
Anti-Phishing Working Group (APWG)

Date: June 8, 2021

Subject: 2021 ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later.

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, DDoS attacks and other online exploitation. We are the largest global anti-abuse industry association, with more than 250 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.

APWG is the international coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors and NGO communities. APWG's membership of more than 2200 institutions worldwide is as global as its outlook, with its directors, managers and research fellows advising: national governments; global governance bodies like the Commonwealth Parliamentary Association, Organisation for Economic Co-operation and Development, International Telecommunications Union and ICANN; hemispheric and global trade groups; and multilateral treaty organizations such as the European Commission, the G8 High Technology Crime Subgroup, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe, Europol EC3 and the Organization of American States. APWG is a member of the steering group of the Commonwealth Cybercrime Initiative at the Commonwealth of Nations.

In 2018 M3AAWG and APWG conducted a survey of cyber investigators and anti-abuse service providers to determine the impact of ICANN's implementation of the EU GDPR, the Temporary Specification for gTLD Registration Data (Temporary Specification, adopted in May 2018) and shared our findings along with recommendations to you for your consideration. M3AAWG and APWG recently conducted a follow up survey to determine the current state of those impacts.

From our analysis of 277 survey responses, we find that respondents report that changes to WHOIS access continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyber attacks.

Specifically, the survey responses indicate that the Temporary Specification has reduced the utility of public WHOIS data due to wide-ranging redactions, beyond what is legally required. It also introduces considerable delays, as investigators have to request access to redacted data on a case-by-case basis; often with unactionable results. Furthermore, with limited or no access to the data that had previously been obtained or derived from WHOIS data, some investigators struggle to identify perpetrators and put an end to criminal campaigns. The resulting delays and roadblocks are a boon to attackers and criminals, prolonging their windows of opportunity to cause harm during cybercrime activities such as phishing and ransomware distribution, or the dissemination of fake news and subversive political influence campaigns.

M3AAWG and APWG observe that there are four issues that ICANN needs to address:

1. **Access to some relevant data like contact data of legal persons needs to be readily available while protecting natural persons' privacy.**
2. **Both sporadic WHOIS users who make relatively few requests, as well as bulk users who use data-driven approaches for blocklisting should be accommodated by ICANN.**
3. **ICANN should establish a functional system of registrant data access for accredited parties; such a system needs to be workable for cybersecurity professionals and law enforcement in terms of time delays and administrative burden, and should include strict privacy and security controls.**
4. **The survey responses indicate that the solutions currently discussed at ICANN would not meet the timeline requirements of law enforcement and cybersecurity actors.**

We respectfully requests 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 https://www.m3aawg.org/for-the-industry/published-comments

Thank you in advance for your consideration.

Sincerely,

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

Foy Shiver
Deputy Secretary-General
Anti-Phishing Working Group