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: September 30, 2021

Subject: Recommendations pertaining to findings from the M3AAWG and APWG WHOIS Survey Report presented to ICANN in June, 2021

This statement is based on materials available on or before September 21st, 2021

In 2018 and recently in 2021, M3AAWG and APWG conducted surveys of cyber investigators and anti-abuse service providers to determine the impact of the ICANN implementation of the EU GDPR, the Temporary Specification for gTLD Registration Data (Temporary Specification, adopted in May 2018).

On June 8, 2021 M3AAWG and APWG published a report containing the results of the 2021 survey.[1] Our survey results indicate that changes to WHOIS access continue to significantly impede cyber applications and forensic investigations and thus cause harm to victims of phishing, malware or other cyber attacks.

WHOIS records are an essential resource used by cybersecurity experts, law enforcement agents, blocklist providers and others to attribute criminal activity, understand malware campaigns, flag malicious domains, and more. While users of the WHOIS tend to use the system for different reasons, two use cases seem worth highlighting:

1) Investigators use the WHOIS to find information on specific domain names, for example when they identify a counterfeit shopfront, after receiving an abuse report, or to better understand or categorize traffic patterns.

2) Investigators also use large numbers of WHOIS data to detect patterns of abuse, and to associate malicious domains with each other, as well as malware, phishing, or spam campaigns.

The WHOIS system is crucial for Law Enforcement and Cybersecurity experts. For example, criminals regularly register large numbers of domains in bulk, often in batches of hundreds or thousands of names at the same time. The purpose of bulk registrations is to make attacks resilient from discovery or to complicate mitigation: criminals will distribute attacks across many domains, or they will swiftly switch to new, already-registered names from their earlier bulk orders when criminal domains are identified. While not all cybercrimes and attacks require large numbers of quickly replaceable names, this approach is common.

[1] https://www.m3aawg.org/WhoisSurvey2021-06

To respond  to cybercriminals that leverage bulk buying and bulk resource use, investigators query WHOIS data constantly and at all times to detect patterns. Registrant as well as technical data can be used to identify sets of likely malicious domains based on their association with already known bad domains or known records: names, email addresses, telephone numbers are likely to be the same for domains used by the same criminal group or same campaign, while bulk orders might also present extremely similar time stamps. When matches are found, domains can be analyzed or added to watchlists. If other criteria indicating abuse are satisfied, these defenders and blocklist providers might also add these names to a blocklist.

Specifically, the survey responses indicate that ICANN's Temporary Specification, in itself an interpretation of the GDPR, combined with the varying implementations by the contracted parties, have significantly reduced the utility of registrant information, i.e. the data traditionally served with the WHOIS protocol. Redactions are inconsistent, error-prone, and beyond what is legally required.[2] In combination, these factors cause considerable problems for cybersecurity and public safety actors: two-thirds of the 2021 M3AAWG and APWG survey[3] [the survey] respondents indicate that their ability to detect malicious domains has decreased. The Temporary Specification and its implementation by Contracted Parties also introduces considerable delays, as investigators have to request access to redacted data on a case-by-case basis but even more so because contracted parties often take a long time to respond. Over 60% of the survey respondents see average wait times of more than a week. Following these long waits, investigators' efforts are usually in vain: our respondents report that requests are being ignored, denied, or answered with fake data. With limited or no access to WHOIS data, investigators struggle to identify perpetrators and are unable to put an end to those criminal campaigns: a perturbing 70% of our 2021 respondents see their investigations negatively affected and that threats cannot be addressed in a timely manner.

The resulting delays and roadblocks simplify the activities of attackers and criminals, prolonging their windows of opportunity to cause harm during cybercrime activities such as phishing and ransomware distribution. Essentially, every criminal activity that in some way relies on the DNS is made easier because key parties cannot access relevant information quickly enough, if at all. Continuing lack of access for key parties, including cybersecurity professionals and public safety and security, will cause harm to the public good and the internet as a whole. The ICANN organization, board, and community have a responsibility to resolve this issue.

Our report indicates there are three issues that ICANN must address:

1. ICANN must require that access to relevant data like contact data of legal persons is readily available while protecting natural persons' privacy.

2. ICANN must establish a functional system of registrant data access for trusted or 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.

---

[2] Lu, Chaoyi, et al. "From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR." (2021), p.14.
[3] https://www.m3aawg.org/WhoisSurvey2021-06

3. ICANN policy must provide workable solutions for both, sporadic WHOIS users who make relatively few requests, as well as bulk users who use data-driven approaches for blocklisting.

The public interest for privacy as well as the public interest in investigating abuse both exist but are currently out of balance, as the needs of security researchers and law enforcement are not being addressed. In order to address this imbalance, M3AAWG and APWG have identified the requirement of a trusted access mechanism[4] for qualified stakeholders to this irreplaceable resource while maintaining and improving the quality of data accessed via public WHOIS.

## Trusted Access

1. ***Recommendation:*** 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.

    ***Consideration:*** The European Data Protection Board (EDPB) specifically states in a letter to ICANN that "data can be made available to third parties who have a legitimate interest in having access" given that safeguards are in place.[5]

    ***Consideration:*** The system needs to be workable for all stakeholders, including cybersecurity professionals and law enforcement.

    ***Consideration:*** Trusted access must significantly reduce time delays and administrative burden; most cybercriminal schemes are profitable and do most harm during the first few hours, sometimes days.

    ***Consideration:*** Trusted access should be global and uninterrupted. The process of individually requesting data is not workable for cybersecurity professionals, many of whom support the public good of a safe and secure internet.

    ***Consideration:*** Trusted access should also provide unrestricted access to all publicly available data.

# Public Access

2. ***Recommendation:*** All contact data of legal persons must be publicly readily available.

    ***Consideration:*** Natural persons' privacy is protected but there are no blanket protections for legal persons.

---

[4] As outlined by the ALAC minority statement on the EPDP Phase 2A report, ICANN received guidance from the European Data Protection Board that such a system would be "reasonable", yet that "this advice was ignored by the EPDP". (https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2a-updated-final-report-03sep21-en.pdf)

[5] https://edpb.europa.eu/sites/default/files/files/news/icann_letter_en.pdf

3. ***Recommendation:*** ICANN should require the creation of functional and workable solutions for contacting registrants that are easily accessible and automatable.

    ***Consideration:*** The use of pseudonym email addresses is a tried and tested solution, while online forms are less accessible and sometimes unworkable in practice.

    ***Consideration:*** Legitimate resources are sometimes compromised and abused. Mitigation may require timely and functional correspondence with the resource owner. It is not always necessary to learn who they are.

4. ***Recommendation:*** All non-personal data should be readily available and publicly visible.

    ***Consideration:*** A notice procedure should be established, informing registrants in advance which data fields would be visible. Notices to keep these data up to date are already being sent out.

5. ***Recommendation:*** Provide measures for correlation so that individuals without access to the trusted access scheme can perform basic analysis of registrant data without impacting on individuals' privacy.

    ***Consideration:*** While not suitable for cybersecurity and law enforcement, hashing[6] and reverse search provides anonymous, basic functionality for researchers, allowing comparison and identification of identical data across records.

    ***Consideration:*** Pseudonymization or hashing can be used when this satisfies operational needs, but these technologies will not be suitable for many use cases and hence cybersecurity researchers and law enforcement must also be able to access the raw data.

## Enforcement of Rules

6. ***Recommendation:*** ICANN needs to enforce rules on registrant data access to protect individuals, public safety and security.

    ***Consideration:*** In the past, registrant data was often harvested in breach of the Terms of Service (ToS) for purposes including advertising, spam, and fraud. ICANN must act quickly to deal with any breaches of the ToS not only for trusted access but also for public access to WHOIS data. Only the use of significant and well-publicized penalties will engender trust in the data access control regime.

[6] Hashing allows researchers to correlate data fields, which is useful in identifying domains that are registered in bulk. For example, see proposal to ICANN: https://www.icann.org/en/system/files/correspondence/jevans-to-marby-et-al-04jun18-en.pdf

Thank you in advance for your consideration.

Sincerely,

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

Peter Cassidy
Secretary General,
Member of APWG BoD
Anti-Phishing Working Group