M3AAWG | Messaging Malware Mobile Anti-Abuse Working Group

Legal Disclaimer

This document is not legal advice. M3AAWG strongly suggests that readers work with their company's legal counsel or avail themselves of independent legal advice regarding their rights, responsibilities and obligations relevant to prevailing legal jurisdictions.

M^{3}AAWG Supports EPDP Phase 2A Policy Recommendations for ICANN

On Jan. 6, 2022, The Messaging, Malware and Mobile Anti-abuse Working Group (M^{3}AAWG) announced and notified the ICANN Board of its support for recommendations made by ICANN's Security and Stability Advisory Committee (SSAC) in SAC118 SSAC Comments on Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team - PHASE 2A.

This continues M3AAWG's efforts to highlight and help remove barriers that prevent critical access to WHOIS data by accredited cybersecurity practitioners for anti-abuse purposes -- a public interest issue as these barriers significantly impede efforts to protect the public from a broad range of cyber-attacks and inhibit necessary forensic investigations.

This document is intended to provide the reader with a summary of activities taken in the past four years by M^{3}AAWG in determining the impact these restrictions are having on anti-abuse measures while offering insight into and support for proposed solutions.

Background

The General Data Protection Regulation (GDPR) was adopted by the European Union (EU) in April 2016 and took full effect on 25 May 2018 across the EU countries. In response, ICANN developed a Temporary Specification for gTLD Registration Data (Temporary Specification) to establish temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR. ICANN indicated the objective of the Temporary Specification was to comply with the

GDPR while maintaining the existing WHOIS system to the greatest extent possible. To accomplish this, ICANN planned on maintaining a robust collection of Registration Data (including Registrant, Administrative, and Technical contact information) while restricting most Personal Data to layered/tiered access[1].

Importance of WHOIS for Cybersecurity Experts and Practitioners

WHOIS records are an essential resource used by cybersecurity experts, law enforcement agents, message security service providers, anti-virus service providers, blocklist providers and others to protect end users, attribute criminal activity, understand malware campaigns, flag malicious domains, and more. These records play a role in more or less any mitigation or response strategy that addresses Domain Name System (DNS) abuse and cybercrime reliant upon the DNS infrastructure. As there is no other avenue to tying a registration to a responsible party, appropriate WHOIS access 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 and services that rely on it are deeply linked.

Use of WHOIS Records by Cybersecurity Experts and Practitioners

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, confirm a phishing report, uncover a malware command and control domain, 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. An example of the second use case, 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

[1] gtld-registration-data-temp-spec-17may18-en.pdf (icann.org) 2nd paragraph.

domains are identified. While not all cybercrimes and attacks require large numbers of quickly replaceable names, this approach is common.

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 can initiate defensive measures including takedowns and inclusion in blocklists.

A Brief History of M3AAWG's Response to the Temporary Specification

Leading up to the implementation of GDPR in 2018, M3AAWG had on numerous occasions provided ICANN with comments[2] while they were preparing their proposed Temporary Specification. Concerned over the impacts on the distributed WHOIS service and anti-abuse work caused by the Temporary Specification, M3AAWG and the Anti-Phishing Working Group (APWG) collaborated to conduct a survey of cyber investigators and anti-abuse service providers that same year. From the analysis of over 300 responses to that survey, M3AAWG and APWG found that the changes to WHOIS access following ICANN's implementation of the Temporary Specification significantly impeded cyber applications and forensic investigations allowing more harm to victims. The full report can be found here:https://www.m3aawg.org/WhoisSurvey2018-10.

In 2020 M3AAWG once again provided comments on Temporary Specification, this time on the Initial Report of the Temporary Specification for gTLD Registration Data Phase 2

Expedited Policy Development Process (https://www.m3aawg.org/documents/en/m3aawg-comments-on-the-initial-report-of-thetemporary-specification-for-gtld). At this

[2] https://www.m3aawg.org/sites/default/files/m3aawg-icann-interim-report-gdpr-2018-01.pdf https://www.m3aawg.org/sites/default/files/m3aawg-icann-calzone-model-gdpr-2018-03.pdf https://www.m3aawg.org/sites/default/files/m3aawg-icann-whois-tiered-access-2018-04.pdf https://www.m3aawg.org/sites/default/files/m3aawg-icann-ip-model-apwg-m3aawg-first-2018-04.pdf

time, we commented that an implementation of a workable System for Standardized Access/Disclosure (SSAD) of Registration Data needs to accommodate various accredited investigators in a cost-effective manner while providing high-volume queries and quick response times without impeding the access to detect, attribute and mitigate abuse on a global scale.

In 2021, M3AAWG and APWG conducted a follow up survey to get an updated understanding of the ongoing impacts of the Temporary Specification on cybersecurity practitioners.

From the 270 survey responses, we found that respondents reported the Temporary Specification continued 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 indicated that the Temporary Specification has reduced the utility of public WHOIS data due to wide-ranging redactions, beyond what is legally required. It also introduced considerable delays, as investigators have to request access to redacted data on a case-by-case basis; often with unactionable results. These 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. Many reporters have given up on asking for WHOIS data, as the answers are either not forthcoming, delayed, or largely unusable for their needs. The full report can be found here: https://www.m3aawg.org/WhoisSurvey2021-06 along with the accompanying covering letter: https://www.m3aawg.org/documents/en/letter-toicann-on-icann-gdpr-user-survey-three-years-later.

In September, M3AAWG and APWG provided their recommendations pertaining to the findings from the 2021 survey (https://www.m3aawg.org/documents/en/recommendations-pertaining-to-findings-fromthe-m3aawg-and-apwg-whois-survey-report). At that time, M3AAWG and APWG provided six recommendations surrounding trusted access, public access and the enforcement of rules.

M3AAWG’s Support for the Recommendations put forward by the SSAC to the EPDP

Considering M3AAWG’s commitment to providing ICANN with advice and insight on determining a workable and successful solution to the Temporary Specification for gTLD

Registration Data, we agree with the recommendations outlined by the Security and Stability Advisory Committee (SSAC) in SAC118 (Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data TeamPhase 2A). Our agreement and support of the four recommendations put forward by SSAC was conveyed via a letter submitted to ICANN (the letter can be found here: https://www.m3aawg.org/sites/default/files/icann-epdp-phase-2a-final-report-commentsjan62022.pdf).

The following paragraphs summarize our comments for each of the recommendations:

The first recommendation put forward by the EPDP recommended that a field or fields be created to facilitate differentiation between legal and natural person registration data and/or if that registration data contains personal or non-personal data. M3AAWG agrees on the need 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.

The second recommendation was to mandate that Contracted Parties who choose to differentiate based on person type follow the guidance and clearly document all data processing steps. M3AAWG agrees that following relevant guidance and creating documentation should be mandatory. Making this voluntary will burden those contracted parties who comply, while enabling those who choose to ignore the recommendation.

The third EPDP Team recommendation was to develop a GDPR Code of Conduct (CoC) that is separate and distinct from the Code of Conduct referenced in the RAA and/or Registry Agreements and takes into consideration the developed guidance concerning legal/natural differentiation. M3AAWG agrees a baseline CoC that applies to all registrars and registries is necessary to establish a functional and uniform system.

The fourth and final recommendation was for the Contracted Parties who choose to publish pseudonymized registrant-based or registration-based email address in the publicly accessible RDDS to do so in a manner consistent with the legal guidance obtained by the EPDP, as well as any other relevant guidance provided by applicable data protection authorities. M3AAWG agrees that 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.

In Closing

At the time of the writing of this blog, we are fast approaching four years since the implementation of GDPR and we still don't have a workable solution for access to WHOIS data by accredited cybersecurity practitioners. On January 25th, ICANN released its System for Standardized Access/Disclosure (SSAD) Operational Design Assessment (ODA) (https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf). This document outlines details on numerous aspects of the proposed solution including how SSAD Requestors could be verified and accredited through a Central Accreditation Authority (Central AA). Furthermore, the document suggests that SSAD development and implementation will take between five and six years at a cost of up to $27 million and annual operations coming in anywhere between $14 and $106 million.Assuming ICANN eventually approves the ODA, and satisfactorily addresses all associated obstacles, the security impediments associated with access to WHOIS data by cybersecurity practitioners will potentially be prolonged up to ten years, resulting in more harm to victims.

Until a workable solution is in place, M3AAWG will continue to research and report on cybersecurity practitioners' abilities to mitigate the harms created through these WHOIS access shortcomings. While directed at ICANN, our efforts are not going unnoticed elsewhere and have influenced other cybersecurity related public policy initiatives[3].

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

[3] Examples include references to our 2021 survey report found in the Study on Domain Name System (DNS) abuse from the Publications Office of the European Union: https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1/language-en/ and hears before the House Committee on Energy & Commerce: https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Te stimony_Lane_CPC_2021.12.09.pdf