M3AAWG Input on NIS2 Directive

M3AAWG, the Messaging, Malware and Mobile Anti-Abuse Working group, appreciates this opportunity to comment on the Revised Directive on Security of Network and Information Systems (NIS) (https://ec.europa.eu/digital-single-market/en/news/revised-directive-security-network-and-information-systems-nis2). We make these comments in our capacities as cybersecurity professionals and researchers committed to ensuring the security and stability of the internet, including the domain name ecosystem.

M3AAWG supports the additions and updates as reflected in the NIS2 draft and notes that many of the new and updated concepts included are key to M3AAWG members who require access to registration data in order to detect threats, investigate new attack vectors and to understand trends aimed at protecting users and the Internet as a whole. This includes law enforcement authorities, both civil and criminal, who rely on the analysis and coloration of Registration Data obtained by private sector researchers and security. Regulation that supports and ensures professionals have access to this data will strengthen the security, stability and resiliency of the Internet as a whole and result in lower abuse rates, less harm inflicted on users and result in decreased criminal impunity on a global scale.

We note that M3AAWG is not alone in its view that access to Domain Name Registration Data (a.k.a. WHOIS data) is critical.

> In its Communication on the EU Security Union Strategy, the European Commission stated that *"access to Internet domain name registration information (WHOIS data) is important for criminal investigations, cybersecurity and consumer protection."*
>
> On February 11, 2021, the European Parliament noted that approximately 75% of requests for access to domain name registration data from parties with legitimate interests remain unanswered and almost all requests that receive an answer are denied.
>
> The Interisle Consulting Group "WHOIS Contact Data Availability and Registrant Classification Study", released on January 25, 2021, found that 86.5% of domain name registrants cannot be identified while also finding that only 11.5% of domain names have been registered to natural persons and are thus subject to the GDPR.
>
> On October 23, 2018, The Council of the European Union expressed the importance of access to domain name registration data and noted "the concerns raised by law enforcement authorities, cybersecurity organizations and intellectual property rights holders about the negative impact of the limitations of access to WHOIS data on their work. Finding a workable solution for access to non-public WHOIS data should be treated as a matter of priority." Unfortunately after more than two years of work, the ICANN community has failed to develop, implement and deploy a working solution.

Suggested Clarifications and Improvements

M3AAWG appreciates the opportunity to provide our input on the current draft text, and detail our suggested clarifications and amendments below for your consideration.

Establishing that access to domain name registration data is a public interest

Given the impact the GDPR has had on the availability of domain name registration data since May 2018 resulting in increasing levels of cybersecurity threats and creating a significant impediment forensic investigations, M3AAWG believes the Commission should establish the public interest nature of domain name registration data and mandate that, at a minimum, the registrant name and a verified registrant email address be published publicly. This publication should apply whether the registrant is a legal or a natural person. Establishing the public interest nature of domain name registration data is equivalent to similar publicly accessible directories, including the European Trademark Register. We argue however that the public interest in these registration data elements (Registrant name and verified email address) are in fact of greater importance to ensuring public welfare, safety and cybersecurity.

As such, we suggest that Article 23.5 be updated to define this public interest and that a new article be added that explicitly required the registrant name and verified email address be publicly available.

Ensuring the term DNS service provider is sufficiently defined

Article 4.9, describes a DNS service provider as "a top-level domain (TLD) name registry, a cloud computing service provider, a data center service provider, a content delivery network provider as referred to in point 8 of Annex I or II entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;"

Given the evolution of the current domain name registration ecosystem over time, M3AAWG strongly suggests that the article fully defines all entities providing domain name registration services. As such, in addition to domain name registries, DNS service providers must also include:

- registrars
- privacy registration service providers
- proxy registration service providers
- domain name resellers

This definition must apply to the language in Articles 23.1, 23.2, 23.3 and Recitals 15, 61, 62.

Explicitly defining what data constitutes domain name Registration data

In several places, the draft NIS2 directive uses the term "complete domain name registration data". For the avoidance of doubt, we believe that the directive should explicitly define the minimum set of registration data elements as follows:

- registrant name
- registrant verified email address
- registrant postal address
- creation, update and expiry dates associated with the registration
- identity of the sponsoring registrar
- all registration status information

Defining DNS Abuse

Recital 60 of the draft NIS2 directive describes preventing and combating "Domain Name System abuse", without defining the scope of DNS abuse. NIS2 should define a definition of DNS abuse that aligns with the ICANN Registry Agreement, which enumerates the following activities that must be prohibited in connection with the use of domain names: "distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law."

Timeliness of Responses from DNS service providers

M3AAWG suggests that the NIS2 directive should improve language that suggests that responses to legitimate requests for registration data should happen without undue delay and, where feasible, not later than 24 hours after receipt of the request. Our experience indicates that many DNS service providers interpret this language generously.

For example Article 23.4 should require that member states ensure the publishing of registration data should happen within 24 hours of the registration. Similarly, Article 23.5 should require that member states shall ensure that entities providing domain name registration services reply within 48 hours to all requests for access.