19 April 2018

Dear ICANN,

On behalf of the Board of Directors of the Forum of Incident Response and Security Teams (FIRST), we wanted to take a brief moment to follow up on our message dated March 15th, 2018.

Over the last few weeks, FIRST has been collecting experiences of our members in their **use of the WHOIS directory and services**. Our members see WHOIS as a valuable resource for abuse reporting, incident response and security investigations. We have shared some of these thoughts on our web site at https://www.first.org/blog/.

Some of the clearest and most common examples of its use in security include:

- Frequent use of WHOIS data to determine where to send a takedown request of malicious code or phishing sites, or to contact the owner of a site to notify them that the site has been compromised;
- Determining whether or not a site is registered by an individual or organization that has previously registered a domain name which was used for malicious purposes, or that is the registered name holder of domain(s) currently being used maliciously.

Access to WHOIS for the security community is essential in the fight against cybercrime. A prolonged interruption will only profit criminals, and negatively affect privacy of internet users.

As an association of organizations in the security response community, **FIRST encourages the ICANN Board to instruct ICANN org to move forward with a sense of urgency to implement an accreditation plan for access to WHOIS**. We support the previous recommendations by APWG and M3AAWG to establish a community group, including the anti-abuse and incident-response communities, to facilitate the creation of an accreditation model for qualified applicants from the security community. FIRST welcomes any opportunity to participate in such an expert task force to draft those requirements, and to contribute our perspective as an association of over 414 security teams in 85 countries.

We believe an **enforceable interim model**, while the accreditation requirements are being developed, is critical to ensure continued access to WHOIS data beyond May 25th, 2018. We reviewed the comments by the WP29 regarding the lack of security controls on IP-based access to WHOIS data. We agree there are limitations to the ability of IP-based authentication to provide significant levels of security.

However, it does propose an already supported, well understood and maintainable step-based approach over today's lack of authentication. While a more sophisticated mechanism will need to be designed and developed to provide long-term accredited access, we support the proposal to enforce use of an intermediate IP whitelist for access to WHOIS data for anti-abuse, threat intelligence, and incident response while the accreditation plan is being implemented. Temporary disruption of continuous access for security purposes such as incident response, abuse reporting, threat intelligence and anti-abuse is otherwise likely to impair the technical and organisational security measures that are being relied on currently to ensure a reasonable level of security.

Therefore, we specifically recommend that the ICANN org create a special task force of security experts to sketch out how the IP-based access could be implemented in a manner that mitigates the WP29 concerns while still protecting the security of the unique identifiers during any interim period to avoid a blackout in May. Any such temporary policy will require careful consideration of rate limiting alongside the white listing.

19 April 2018

We also wanted to repeat the **criticality of including valid organizational contact information in the public WHOIS** data set for at least newly registered organizational domains. There is no reason why personal data of individual name holders should continue to be collected if it unnecessarily limits what is displayed in the public WHOIS. Therefore, a temporary policy should also address the formatting requirement of the organizational email address to allow a valid “admin” or “manager” user at a particular domain (or possibly an anonymized or pseudonymous proxy address) .

There is no true privacy without security. We strongly believe one of the key criteria that should be met is that registrars should be transparent to users on which data is exposed, and to whom. Having a clear, universal message to users around how their data is stored, and presented to both the security communities, and the internet at large, is key to making expectations clear.

We read with great interest the proposal of the Anti-Phishing Working Group, dated April 5th of 2018. FIRST is eager to work with its industry peers, including M3AAWG and APWG, with whom we are already in contact, to help define an accreditation model that will allow our members, and the wider security community to gain access to WHOIS data.

Best regards,

Thomas Schreck	Maarten Van Horenbeeck	Serge Droz	Aaron Kaplan
Chair	Board Member	Board Member	Board Member
thomas@first.org	maarten@first.org	serge@first.org	aaron@first.org

Founded in 1990, the Forum of Incident Response and Security Teams (FIRST) consists of internet emergency response teams from more than 360 corporations, government bodies, universities and other institutions across 78 countries in the Americas, Asia, Europe, Africa, and Oceania. It promotes cooperation among computer security incident response teams. For more information, visit: https://www.first.org.