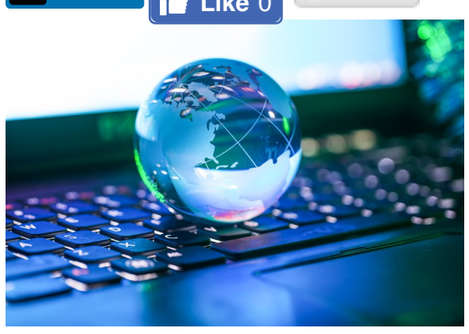
Security

Policy eliminates pre-emptive protection of internet infrastructure abuse

By Networks Asia staff | Tuesday, October 30, 2018 - 14:26

Share Like 0 Tweet Email Share (http://www.addthis.com/bookmark.php?v=250&username=questex) Print



A joint APWG-M^{3}AAWG survey of cybercrime responders and anti-abuse personnel indicates ICANN's Temporary Specification for domain name WHOIS data has eliminated interventions that previously allowed investigators to stop new cybercrimes while still in the preparatory stages -- and has markedly impeded routine mitigations for many kinds of cybercrimes. The survey (http://www.m3aawg.org/WhoisSurvey2018-10) was submitted to ICANN on Oct. 18 by the Anti-Phishing Working Group and the Messaging, Malware and Mobile Anti-Abuse Working Group (APWG-M^{3}AAWG).

With responses from 327 professionals, the survey revealed that losing the ability to attribute domain names to criminals or victims of abuse has irreparably eliminated their capacity to issue warnings about new abuses that known bad actors are perpetrating, even when the WHOIS registrant data is pseudonymous, according to Peter Cassidy, APWG Secretary General.

ICANN's Temporary Specification for gTLD Registration Data, established in May in response to the European Union's General Data Protection Regulation (GDPR), impedes investigations of cybercrime -- from ransomware attacks to distribution of state-sponsored strategic disinformation.

Analyses of responses from the survey reveal that cyber-investigations and mitigations are impeded because investigators are unable to access complete domain name registration data. Requests to access non-public WHOIS by legitimate investigators for legitimate purposes under the provisions of the Temp Spec are routinely refused.

"The biggest impact has been to determine who has registered a criminal/fraudulent domain, and the ability to use that information to find other domains registered by the same actor. That devastates our ability to find all of the fraudulent domains registered by the same entity," one typical respondent wrote in the APWG-M^{3}AAWG GDPR WHOIS User Survey report.

APWG and M^{3}AAWG concluded their analysis with recommendations for ICANN to:

- Establish a mechanism for WHOIS data access by accredited, vetted qualified security actors.
- Restore redacted WHOIS data of legal entities.
- Adopt a contact data access request specification for consistency across registrars and gTLD registries.
- Establish a WHOIS data access scheme that does not introduce delays in collecting or processing and is not burdened by per-request authorizations.
- Reassess the current redaction policy and consider replacing restricted personal data with secure hashes that can be used as a proxy for tracing criminal actors across data resources.
- Publish point of contact email addresses to provide investigators with an effective means of identifying domains associated with a victim or person of interest in an investigation.

The full survey can be found at:

http://docs.apwg.org/reports/ICANN_GDPR_WHOIS_Users_Survey_20181018.pdf (http://docs.apwg.org/reports/ICANN_GDPR_WHOIS_Users_Survey_20181018.pdf)