Access to WHOIS critical for online security

Why are we hearing about WHOIS now?

One of the essential functions of the Internet Corporation for Assigned Names and Numbers (ICANN) is to oversee domain names. In line with this objective, its WHOIS protocol has been used for over two decades to record and display the contact details of domain name registrants. In addition, the registered contacts in WHOIS provide clear point of contacts for Certification Authorities (CAs) to seek authorization when issuing SSL certificates. This WHOIS data provides much needed transparency online and as such protects users, customers and the Internet ecosystem as a whole.

However, access to this critical data has been severely restricted following the coming into force of the European Union's General Data Protection Regulation (GDPR) in May 2018. And importantly, this has less to do with the actual Regulation, but more with the approach ICANN, in a unique position as a joint data controller not in possession of data being regulated, and the registrars and registries which hold the data have taken to complying with it, significantly undermining an essential tool.

The signatories of the Cybersecurity Tech Accord embrace the individual's right to privacy articulated under the GDPR. We also emphasize the critical importance of maintaining a stable and secure Internet, which is central to ICANN's purpose as spelt out in Article 1.1(a) of its bylaws[1]. We believe that the GDPR strikes an appropriate balance between individual privacy and the ability to use certain types of data to protect citizens and maintain a stable and secure Internet, and that there is no conflict between GDPR compliance and the use of WHOIS data for legitimate purposes, such as cybersecurity. Indeed, the GDPR includes provisions which foresee the processing of data for security purposes, and since Reverse WHOIS is one of the most useful tools we have for identifying cybercriminals and disrupting their operations, it is essential that this legitimate purpose be correctly defined and maintained.

Where we are today

In the last few months ICANN has taken initial steps to try and rectify the situation. A temporary policy adopted in May 2018 represents a starting point for developing subsequent policy. Unfortunately, with it ICANN also reduced the quantity of, and ease of access to, WHOIS data, going further than we believe is necessary to bring WHOIS into compliance with the GDPR. The divergent interpretation of what constitutes "reasonable access" to data have led to differing approaches by registrars and registries and a fragmentation of WHOIS.

This was in late June followed by the Unified Access Model, which is intended to provide a framework for an accreditation model for third parties with legitimate interests to become accredited in order to gain access to redacted WHOIS data. While a welcome step forward, particularly given its focus on working with the multi-stakeholder community to identify a viable path forward, the initiative comes late and falls short of what is needed today. There is an acute need for ICANN to implement a solution for accreditation and access – even if temporary. Until then, the ability of cybersecurity companies and law enforcement authorities to tackle the increasing number of threats we see to the security of the Internet will continue to be hampered by our limited access to WHOIS data.

---

[1] *"The mission of the Internet Corporation for Assigned Names and Numbers is to ensure the stable and secure operation of the Internet's unique identifier systems"*

The urgency of enabling accreditation

The examples highlighted below illustrate the vital importance of access to data, including email address, for the network security and public interest purposes of Cybersecurity Tech Accord signatories and many other companies and organizations. However, as highlighted above, while ICANN has taken the first steps towards ensuring access, we do not yet have an accreditation program in place. This has created a situation where individual requests need to be made for data for each separate domain, which substantially hinders and slows down the efforts of cybersecurity practitioners and law enforcement authorities.

We therefore urge ICANN to accelerate their work towards a uniform approach to accreditation which is mandatory for registries and registrars. It is critical that the accreditation solution enables legitimate users to get back to a situation where there is broad, persistent and frictionless access to WHOIS data for legitimate purposes. We also believe that it is critical that cybersecurity professionals preserve the ability to analyze data that is crucial for them to disrupt cybercrimes, including through the continued possibility to conduct Reverse WHOIS searches or consultation of current and historical WHOIS data in an aggregated fashion.

The Cybersecurity Tech Accord signatories hope that ICANN will ensure that contracted parties will continue to not be able to redact the non-personal data of legal persons, which fall outside the scope of the GDPR.

Finally, we also applaud those in the ICANN community that have independently put forward ideas for a draft accreditation and access model, and therefore provided a basis from which we can build upon. It is nevertheless clear that success of the Unified Access Model will not only depend on whether it can be fully developed and adopted by all parts of the ICANN community as part of the ICANN multi-stakeholder process, but also on the commitment of ICANN to expedite implementation. Until this challenge is rectified we will experience a material impact on the safety and security of businesses and individuals online.

Cybersecurity and WHOIS

Cybercriminals rely on domains to launch coordinated and automated attacks on a global scale. As a result, the global WHOIS directory is the only viable means to obtain the information necessary to identify criminal actors, prevent harms and protect the online ecosystem. For example:

- Cybersecurity professionals use WHOIS data to disrupt malicious attacks by identifying the email address registered to a malicious domain and then using "Reverse WHOIS" searches to identify all other domains linked to that email address which might therefore also be used in the same or other attacks.
- Malicious online activity often impacts large numbers of people almost simultaneously, so investigators must be able to rapidly analyze massive amounts of current and historical WHOIS data to help identify key participants in the attack and map the Internet infrastructure that they are controlling and deploying.
- Attackers often use domain names that are similar to major brand names. These domains are often used by hackers to communicate with malware installed on targeted computers. By looking up WHOIS data, companies can sue the domain owners for trademark infringement and take over the offensive domains. The companies are then able to observe and strategically disrupt hacking operations.
- Increasingly, criminals take control of legitimate servers or websites and leverage them for malicious purposes. Without ready access to detailed WHOIS information, cybersecurity professionals will have to treat all malicious domains as being owned by criminal actors, thus increasing the possibility of collateral damage from actions to tackle the criminal activity.

About the Cybersecurity Tech Accord

The Cybersecurity Tech Accord is a public commitment among more than 40 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace.