# Cybersecurity Tech Accord calls on ICANN to establish a mechanism for access to WHOIS data to effectively respond to cyberthreats

*Signatories express concern about the lack of access, highlighting how it has already impacted their ability to protect customers.*

In August, the Cybersecurity Tech Accord signatories addressed the decision of the Internet Corporation for Assigned Names and Numbers (ICANN) to restrict users' access to domain name registration information (WHOIS) following the EU General Data Protection Regulation (GDPR) coming into force (via a Temporary Specification – the "Temp Spec"). We emphasized how this decision had de facto undermined an essential tool to protect internet users from online threats. At the same time, we welcomed ICANN's plans to develop a framework for accreditation and access, but underlined the need for action to be taken immediately. In addition, we expressed concerns that any fragmentation of approaches could lead to the loss of precious data.

While ICANN has kicked off an expedited policy development process, the question of access to WHOIS for legitimate uses, such as cybersecurity and consumer protection, has not yet been addressed. In the intervening period, limits put on access have impaired cybersecurity professionals' ability to minimize the impact of cyberattacks. This was reflected in last month's publication of a survey of over 300 cyber investigators and anti-abuse service providers by M3AAWG, the Messaging, Malware, and Mobile, Anti-Abuse Working Group and APWG, the Anti-Phishing Working Group. It unequivocally found that the changes ICANN has put in place were "*significantly impeding cyber applications and forensic investigations and allowing more harm to victims of cyberattacks*." The challenges experienced included:

- partial data available through the public WHOIS services after redaction were insufficient to investigate or respond to incidents;
- the need to request access to the non-public data elements introduced delays of days where mitigation of cyber incidents prior to the adoption of the Temp Spec was often accomplished within hours;
- the WHOIS contact data that is most relevant to investigators and has evidentiary value to law enforcement and prosecutors, was generally not available through public WHOIS services;
- requests to access non-public WHOIS by legitimate investigators for legitimate purposes were routinely refused.

The Cybersecurity Tech Accord signatories find that these results reflect the reality that we have experienced first-hand. To demonstrate the impact, we wanted to provide a selection of concrete examples of how fighting cybercrime has become more difficult in the last few months:

Facebook's and FireEye's investigations into Liberty Front Press

Use of the WHOIS database has been critical in enabling FireEye to attribute foreign Information Operations (IO) campaigns targeting the United States and European nations. For example, FireEye recently identified an extensive influence operation originating in Iran by linking a network of inauthentic news sites via registration email addresses and Iranian name servers listed in the WHOIS database. Based on that information, in August 2018 Facebook removed 650 pages, groups and accounts for coordinated inauthentic behavior that originated in Iran and targeted people across multiple internet services in the Middle East, Latin America, UK and US.

Investigations uncovered inauthentic news sites supported by a network of domain names and websites that promoted political narratives in line with Iranian interests. Investigators were able to link this network to Iranian state media through publicly available domain name registration information, as well as the use of related IP addresses and Facebook Pages sharing the same admins. Investigators used domain name registrant email

addresses obtained using WHOIS queries, and historical WHOIS collected prior to 25 May 2018, to associate several websites with this attack, and social media accounts affiliated with "Liberty Front Press" were subsequently identified. Over the course of the investigation, WHOIS was repeatedly queried for current registration data for affiliated websites, and investigators "pivoted" between social media accounts, pages or posts and WHOIS using emails, names and addresses to continue to map the inauthentic news site network.

Impact: This investigation began before ICANN's redaction of WHOIS records and is ongoing. During the investigation, WHOIS records for domain names linked to this network literally disappeared before investigators' eyes, causing the investigation to take longer and making it more difficult to identify all domain names linked to this inauthentic news site network. Prior to ICANN updating its WHOIS policy, companies relied on WHOIS records to help detect, investigate and stop a range of abuses, including nation-state influence campaigns. Since investigators are unable to access complete domain registration data in a timely and efficient manner, WHOIS is becoming an unreliable source of threat intelligence.

Facebook's investigation into instagramn.xyz' phishing attack

The domain name <instagramn.xyz> recently was linked to a phishing attack and the WHOIS record was immediately used to identify the ISP hosting the website, submit a complaint, and have it taken offline. Using additional data available in the WHOIS record, Facebook conducted reverse WHOIS searches on multiple WHOIS data elements and identified the registrant, as well as 17,000 domain names the registrant also held. Facebook's analysis of this domain name portfolio identified a total of 50 additional domain names that infringed Facebook, Instagram and WhatsApp trademarks, several of which also were being used for phishing or distribution of malware to users. These websites also were taken down as a result of the submission of a complaint to the ISP identified in the WHOIS records. While ISPs can take websites offline, the corresponding domain names still remain with the registrant perpetrating the fraud. A Uniform Dispute Resolution Policy (UDRP) complaint to recover the 51 infringing domain names was filed and the decision is expected soon.

Impact: Using WHOIS records available prior to 25 May 2018, from one domain name Facebook successfully mitigated phishing and malware attacks against our users and identified over 50 abusive domain names. The excessive redaction of public WHOIS data and failure to provide cybersecurity investigators complete domain registration data in a timely and efficient manner impedes and impairs quick, comprehensive actions to protect users from phishing attacks.

Microsoft's ongoing investigation around Strontium/APT28

A threat actor group referred to as Strontium has been active since 2016 using fake registered domains to redirect phished users, spoof credential login pages and steal credentials. Prior to ICANN updating its WHOIS policy, Microsoft relied on WHOIS records to detect new Strontium domain registrations and successfully protect its customers.

Impact: With ICANN's new approach in place, Microsoft could be disadvantaged in its investigations. For example, recently Microsoft investigators became aware of domains related to Strontium that they had not discovered earlier due to the recent restriction on available domain name information. Fortunately in this instance, there was no evidence that the domains had been used for cyberattacks so customers weren't put at greater risk, but it's easy to see how this could have turned out differently. Microsoft is unable to protect customers against potential malicious domains if the data needed to conduct investigations is unavailable.

Panasonic's work to protect customers and brand from domain phishing attempts

The domain panasonicpro.co.uk was used to steal Panasonic customers' credentials and has been using Panasonic's logo without permission. At the time, Panasonic had full access to the WHOIS registry. It was, therefore, able to determine that the domain was registered by a person living in Dumbarton, UK and could take all the

required steps to prevent this situation from impacting its customers. Since then, the domain has been updated but the company is today unable to determine who is behind it.

Impact: With ICANN's new approach in place, Panasonic's Computer Security Incident Response Team (CSIRT) now does not have any means to establish the ownership of a domain and take all the necessary steps to protect its brand. While panasonicpro.co.uk is in a country code top-level domain (.uk) that is not obligated to follow ICANN rules, it's indicative of the harm suffered by consumers when WHOIS records are not accessible to protect them and stop abuse.

FireEye's investigation into FIN7 domain spoofing

In early June 2018, FireEye observed several ZIP files being hosted on various URLs spoofing Ukraine and Kazakhstan-based banks. In the past, FireEye has observed the cybercriminal group FIN7 establishing look-a-like domains to mimic its targets or related entities, commonly hosting content that spoofs the legitimate websites of the brands they are impersonating. Multiple samples of an unknown JavaScript backdoor—later confirmed to be BIRDDOG malware—all with the filename dog.js, were contained within similarly named ZIP files. FireEye was able to initially link this activity to FIN7 based on domain registration patterns and overlapping WHOIS records, and later confirmed through analysis of the BIRDDOG malware.

Impact: Further analysis of this campaign indicated a potential shift in targeting, and FireEye was able to swiftly provide analysis to customers on a prolific cybercriminal group's changing tactics. Lack of access to WHOIS records would make similar cross-checks very difficult to implement with a tangible impact on cybersecurity professionals' ability to investigate criminal activity in real time.

WHOIS has been, for more than a decade, a vital tool for companies, cybersecurity firms and law enforcement authorities to collect valuable intelligence on online threats and malicious actors. As pointed out, current restrictions on users' real-time access to this registry have had a material impact on the safety and security of businesses and individuals online. There can be no privacy online without strong security. We therefore call on ICANN to take steps now to protect the public interest by ensuring interim access to WHOIS for cybersecurity uses, and to quickly develop a permanent model providing uniform, swift and enforceable access to WHOIS data that balances both.