ICANN's Whois Proposed Interim Model for GDPR Compliance will inhibit the Cybersecurity Community's Role in Data Protection

Statement by the EC3 Advisory Group on Internet Security

02 April 2018

Synopsis

ICANN's Whois Proposed Interim Model for GDPR Compliance[1] does not adequately account for the legitimate, necessary and proportionate use of Whois data[2] for ensuring the security and stability of the global Domain Name System (DNS) and protecting against DNS-based data protection threats through cybersecurity research, threat detection, analysis, and mitigation.

Background

Domain names are critical component of Internet infrastructure, used for both lawful or malicious purposes. Registering a domain name is an act of publishing an entry in the DNS which serves as infrastructure for routing global Internet traffic. The DNS is a global public database, created under United States government stewardship and now run by a global multistakeholder community, for which registrant data has been published since 1982.[3] Since then, DNS-based cybersecurity threats to data protection have amplified dramatically in scale and impact. All the while, the importance of Whois records in cybersecurity has increased. Analysis of Whois data regularly exposes cybersecurity threats and enables security researchers to enhance defences and map out threat infrastructure.[4] In redesigning Whois data record contents, availability and access, code may in fact override law, effectively hindering lawful, legitimate, and necessary uses of data which are critical to holistic data protection on a global scale. Consequently, the cybersecurity community is concerned about the Proposed Interim Model.[5]

The Proposed Interim Model does not guarantee the most crucial data element in a Whois record

In current form, ICANN's Proposed Interim Model does not account for the criticality of email addresses as the only reliable registrant data element in a Whois record. The Proposed Interim Model erroneously equates a web contact form as a fungible substitute for the current email address entry. However, unlike the name, address, organization, and phone number fields, which may be erroneous, the email address corresponds to an actual, functioning email account, which is used to establish a registrar account and conduct the domain name registration. Email addresses are easy to create and customizable, meaning that a domain name

[1] ICANN, Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation, 8 March 2018, https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf

[2] EC3 Advisory Group on Internet Security, The Indispensable Role of Whois for Global Cybersecurity, 25 January 2018, https://www.icann.org/en/system/files/files/gdpr-statement-ec3-europol-icann-proposed-compliance-models-25jan18-en.pdf

[3] Harrenstien, K., and White, V., "NICNAME/WHOIS," RFC-812, Network Information Center, SRI International, March 1982.

[4] Brian Krebs, Breadcrumbs, KrebsonSecurity, https://krebsonsecurity.com/category/breadcrumbs/; https://www.threatconnect.com/blog/using-fancy-bear-ssl-certificate-information-to-identify-their-infrastructure/

[5] Brian Krebs, Who Is Afraid of More Spams and Scams?, KrebsonSecurity, 16 March 2018, https://krebsonsecurity.com/2018/03/who-is-afraid-of-more-spams-and-scams/

registrant may have multiple email addresses, only one of which would need to be associated with a domain name registration. Regardless of whether an email address is identifying or an opaque pseudonym, anonymous to others, it serves as a unique data point for correlating domain name registrations. This is used on a regular basis by the cybersecurity community for determining the reputation of a domain name, associating it with past known cybersecurity threats, performing threat attribution, and determining related components of cybersecurity threat infrastructure.

The Proposed Interim Model does not guarantee bulk access to Whois data

The Interim Model does not account for the need to access more than one Whois entry at a time, a practice which is necessary to identify patterns of cybersecurity threats through correlation analysis.[6] This practice contributes to the security and stability of the DNS, a key component of ICANN's mission, and is regularly relied upon by law enforcement authorities.

The Proposed Interim Model does not guarantee the cybersecurity community's access to Whois data

The Whois database has been used as a resource for remedying technical issues since its inception. Over time, these technical issues have evolved from early DNS issues, such as domain name registrant's improper configuration settings, to modern cybersecurity threats stemming from maliciously-registered or compromised legitimate registrations used to breach or otherwise unlawfully process personal data. All the while, the criticality and utility of the Whois database has increased. The role of cybersecurity in data protection, against threats to the security and stability of the Domain Name System, is more important than ever. Nonetheless, the Proposed Interim Model does not guarantee a mechanism through which the cybersecurity community may access Whois data. Instead, potential access is dependent upon the creation of an accreditation system in the future, leaving an indefinite period of time during which Whois will "go dark" for the cybersecurity community. This is particularly problematic as we approach the summer months, which have shown especially heightened activity in years past.[7]

Cybersecurity is a global necessity

Domain name registrants represent a fraction of Internet users and an even smaller proportion of those affected by the DNS. Today, the DNS supports a global ecosystem[8] vulnerable to

[6] Mark Felegyhazi, Christian Kreibich, and Vern Paxson. On the potential of proactive domain blacklisting. In Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more, pages 66. USENIX Association, 2010

[7] Maciej Korczynski, et. al., Statistical Analysis of DNS Abuse in gTLDs Final Report, 9.8.2017, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

[8] EU cybersecurity initiatives, ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

cybersecurity threats[9] affecting energy[10], transportation[11], water[12], financial market infrastructures[13], healthcare[14], digital infrastructure, election systems[15], and personal data repositories[16]. Moreover, law enforcement agencies focused on data protection and broader cybercrime do not do their work in a vacuum. Instead, they rely in part on the tools, resources, and analysis created by the private sector cybersecurity community's access to Whois records. Now is not the time to reduce the resources available to those protecting these critical components of modern society.

Statement should inform public discussions and analysis

The EC3 Advisory Group on Internet Security invites EC3 to share this statement with ICANN and the Article 29 Working Party in order to inform the public discussions on the future of Whois and to ensure that any further developments take into consideration the criticality of the cybersecurity community's continued need to access Whois data to protect against DNS-based threats to data protection.

About the EC3 Advisory Group on Internet Security

The Advisory Group on Internet Security is an advisory group to the Programme Board of the European Cybercrime Centre (EC3), comprised of private sector and non-profit members representing a wide-range of expertise in all the aspects of internet security, including from the CERT community related to the fight against cybercrime and also a balanced representation in terms of background and geographic regions. More information about the Advisory Group can be found at https://www.europol.europa.eu/publications-documents/terms-of-reference-and-mandate-of-advisory-group-internet-security and https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners

[9] Europol, Attacks on Critical Infrastructure, https://www.europol.europa.eu/iocta/2016/attacks-on-ci.html

[10] Hannah Kuchler, Financial Times, Hackers infiltrate systems of energy companies, 6 Sep. 2017, https://www.ft.com/content/8c51cdae-9298-11e7-bdfa-eda243196c2c

[11] Laurens Cerulus, Cyberattack underway on Europe's energy and transport companies, Politico.eu, 28 Jan. 2018, https://www.politico.eu/article/cyberattack-under-way-on-europes-energy-and-transport-companies/

[12] Anca Gurzu, Hackers threaten smart power grids, Politico.eu, 4 Jan. 2017, https://www.politico.eu/article/smart-grids-and-meters-raise-hacking-risks/

[13] James Rothwell, et. al., Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down, The Telegraph, 27 June 2017, https://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/

[14] Julia Carrie Wong & Olivia Solon, Massive ransomware cyber-attack hits nearly 100 countries around the world, The Guardian, 12 May 2017, https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

[15] Ben Wofford, How to hack an election in 7 minutes, Politico.eu, 6 Aug. 2016, https://www.politico.eu/article/how-to-hack-an-election-in-7-minutes-united-states-russia/

[16] John McCrank, Equifax says 15.2 million UK records exposed in cyber breach, Reuters, 10 Oct. 2017, https://www.reuters.com/article/us-equifax-cyber/equifax-says-15-2-million-uk-records-exposed-in-cyber-breach-idUSKBN1CF2JU