The Indispensable Role of Whois for Global Cybersecurity

Statement by the EC3 Advisory Group on Internet Security

25 January 2018

Synopsis

Whois data is an indispensable resource for ensuring the security and stability of the global DNS and protecting against DNS-based cybersecurity threats because of its role in facilitating cybersecurity research, threat detection, analysis, and mitigation.

Background

The Internet Domain Name System (DNS) is frequently abused by malicious actors engaged in activities that damage, interrupt, and abuse network and information systems. This digital infrastructure is a unique privately-run, decentralized, publicly-accessible global resource, that adheres to common international protocols for its security, stability and overall utility. At a time when the magnitude and impact of cybersecurity incidents is rapidly scaling, private cybersecurity researchers, non-profits, and companies play an increasingly crucial role in investigating, disrupting, preventing, and mitigating such threats. Consistent with these realities, the European Union has placed a particular emphasis on encouraging public-private cybersecurity partnerships.[1]

Ensuring cybersecurity and protecting potential victims from DNS-based cyber-attacks involves many stakeholders. The Europol EC3 Advisory Group on Internet Security, which includes many of the largest and most experienced Internet security firms in the world encompassing a variety of specialties and areas of expertise, believes it is imperative that any assessment of new Whois implementations consider the overwhelming legitimate purpose of processing Whois data for DNS abuse enforcement, Internet security and stability, and global cybersecurity efforts. The distinct roles played by law enforcement, in pursuing justice, and the private cybersecurity community, in protecting against cyber-attacks, should not be conflated and viewed as interchangeable when determining the future of Whois access. On the contrary, restricting Whois access merely to law enforcement would drastically impair global cybersecurity efforts.

We share the EU's strong commitment to protecting personal data and are in fact in the business of protecting such information by securing our customers and the broader digital ecosystem against breaches. Many organizations in the cybersecurity industry are concerned that ceasing the ability to leverage Whois data might have unintended consequences that undercut cybersecurity efforts, which protect personal and other information. As the GDPR itself acknowledges, ensuring network and information security constitutes a legitimate interest for data protection.[2]

---

[1] ENISA, Cybersecurity cooperation Defending the digital frontline, October 2013, https://www.enisa.europa.eu/publications/cybersecurity-cooperation-defending-the-digital-frontline/at_download/fullReport; See also: Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 415, 13.9.2017, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450

[2] *See Generally* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such

Whois is necessary for cybersecurity

Almost all cyber-attacks, including targeted cyber intrusions and broader online criminality that leads to data breaches, require infrastructure which is subject to DNS registration at some point in the attack lifecycle. As such, the international Whois protocol plays a critical role in identifying malicious infrastructure and thus defending against or preventing attacks. Accessing Whois registrant information is an essential element of the cybersecurity community's efforts to maintain the overall security and stability of the global Internet, and any loss of access would seriously degrade these efforts.

Among other things, the processing of Whois data is necessary for the legitimate purpose of protecting the Internet as an open global resource and defending those who can be affected by DNS-based threats. DNS abuse remains significant and widespread as the size of the DNS as an attack vector has greatly expanded.[3] Most cybersecurity investigations, or technical processes determining the safety of domain names, rely upon Whois queries. Such real-time queries provide what is sometimes the only information available to timely identify and protect against advanced persistent threats, cybercrime infrastructure (such as fast-flux botnets), and other DNS abuse. For example, phishing emails are a major source of data breach around the world. Yet, based on our experience, we know that many phishing campaigns are prevented or limited due to the ability of defenders to query the domain names associated with suspicious embedded links, email addresses, or servers, and thus identify malicious activity before users have been exploited. Removing this expedient access from defenders would therefore have an immediate and profound effect on the success rate for phishing attacks.

Correlation of Whois data further enables the identification of common perpetrators, particularly when there are large campaigns or repeat offenders, aiding prevention as well as remedial investigation. For example, domain names used for malicious purposes may share common registrant data, such as the same email address, even if they are registered with different registrars and assigned to different TLD registries. Defenders can pre-emptively block such linked malicious domain names to prevent subsequent attacks. Removing access to Whois would again lead to an immediate and direct impact on defenders' abilities to conduct this sort of protective activity.

Cybersecurity uses for prominent Whois fields include:

Registrant name: Necessary for determining whether a domain name was registered for legitimate or malicious purposes, detecting suspicious registrations, contacting victims, preventing DNS hijacking, identifying miscreants, and as a pivot point to find other affiliated

---

data, and repealing Directive 95/46/EC (General Data Protection Regulation); *See also* GDPR Recital 49, GDPR Article 32, GDPR Article 25

[3] 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

domain names. Even bogus information, common in cybercrime and often times not personal data of a natural person, is important for correlating other domain names linked to the same attack infrastructure, campaign, or other early warnings of a domain name about to be used for malicious purposes.

Registrant email: Necessary for contacting victims or miscreants, preventing DNS hijacking, detecting suspicious registrations, preventing cybersecurity incidents, determining associated domain names. As a verified, functional component and unique identifier, this is perhaps the most valuable part of registrant Whois data for cybersecurity researchers. It is used for correlating other domain names linked to the same attack infrastructure, campaign, or other early warnings of a domain name about to be used for malicious purposes and for preventing repeat cybersecurity incidents.

Phone number and address: This field is necessary determining whether a domain name was registered for legitimate or malicious purposes, contacting victims or miscreants, preventing DNS hijacking, detecting suspicious registrations, preventing cybersecurity incidents, determining associated domain names.

Name server: Necessary for identifying the server to which a domain name will route traffic and is used to determine if a domain name is directing traffic to a known cyber threat indicator or common cyber threat infrastructure.

Registrar: Necessary for determining where a domain name is registered to report abuse, notify victims, and correlate trends.

Registration date: Necessary for determining when a legitimate registration may have been compromised, a domain name was registered for malicious purposes, and determining the relationship between domain names used in common cyber threat infrastructure.

Expiration date: Necessary for determining when a legitimate registration may have been compromised, a domain name was registered for malicious purposes, and determining the relationship between domain names used in common cyber threat infrastructure.

Updated date: Necessary for determining when a legitimate registration may have been compromised, a domain name was registered for malicious purposes, determining the relationship between domain names used in common cyber threat infrastructure, and when records may have been changed for malicious purposes.

These data points, along with other technical fields that may be populated in Whois records, are impactful not only as real-time security indicators but also used to investigate malicious actors and diminish their asymmetrical advantage in building out cross-border cybercrime infrastructure. In the Mirai botnet case, the private sector cybersecurity community analysed Whois records, filled with bogus information, to successfully identify the culprit, Daniel Kaye, as being responsible for victimizing more than 900,000 Deutsche Telekom customers.[4] In other

[4] Brian Krebs, Who is the GovRAT Author and Mirai Botmaster 'Bestbuy'?, KrebsonSecurity, 5.7.2017, https://krebsonsecurity.com/2017/07/who-is-the-govrat-author-and-mirai-botmaster-bestbuy/

examples, Whois data has provided further insight into the Wannacry outbreak[5], iCloud phishing campaigns[6], and DDoS attacks.[7]

Cybersecurity is necessary for the DNS

In the EU, under the Network and Information Security (NIS) Directive, operators of essential services and other companies must take appropriate and proportionate measures to manage the risks posed to the security of networks and information systems which they use in their operations.[8] Covered services include domain name registries and registrars, which are digital infrastructure operators, as well as other entities critical to society and the economy, all of which must take into account compliance with international standards when meeting these obligations. The work of the cybersecurity community to legitimately leverage DNS information empowers such infrastructure operators and would-be victims to manage their security risks.

The DNS is a unique privately-run, decentralized global resource, that adheres to common international protocols for its security, stability and overall utility. Private cybersecurity companies play an indispensable role investigating, disrupting, preventing, and mitigating malicious cyber incidents and largescale cyber-attacks. In the past year alone, widespread cyber-attacks, such as Wannacry and the DDoS attacks launched by the Mirai botnet, have disrupted the Internet on a large scale. Removing the cybersecurity community's access to Whois data will thwart existing cybersecurity mitigation techniques and further empower the ability of cyber attackers to scale their infrastructure with more persistent campaigns. Given the centrality of DNS abuse to an enormous volume of malicious cyber activity, and the current role of cybersecurity companies and independent researchers in defending would-be victims via Whois data, such access remains necessary and is vital to a multi-stakeholder approach to cybersecurity.

Safeguarding the DNS protects a global resource

At its heart, the DNS is a global public database. Public Whois records correlated to each domain name entry have been part of the DNS since its inception. Registering a domain name is more than a mere transaction. Rather, it is a request to publish in the global public database powering a critical component of the Internet and modern society. Ensuring that this database functions, preventing it from being used to harm others, enforcing the rules and safeguards set by the global Internet community, enabling research, and other legitimate interests makes processing of and access to Whois data necessary.

---

[5] Brian Krebs, Who Is Marcus Hutchins?, KrebsonSecurity, 5.9.2017, https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/

[6] Brian Krebs, If Your iPhone is Stolen, These Guys May Try to iPhish You, KrebsonSecurity, 14.3.2017, https://krebsonsecurity.com/2017/03/if-your-iphone-is-stolen-these-guys-may-try-to-iphish-you/

[7] Brian Krebs, Spreading the DDoS Disease and Selling the Cure, KrebsonSecurity, 19.10.2016, https://krebsonsecurity.com/2016/10/spreading-the-ddos-disease-and-selling-the-cure/

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Statement should inform public discussions

The EC3 Advisory Group on Internet Security invites EC3 to share this statement with ICANN in order to inform the public discussions on the future of Whois and to ensure that any further developments take into consideration the crucial role played by Whois data in the cybersecurity community's efforts 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