April 25, 2018

TO: Mr. Göran Marby, CEO, ICANN
John Jeffrey, General Counsel, ICANN
gdpr@icann.org

FROM: APWG, FIRST, and M3AAWG

RE: Temporary Access Method for Non-Public Whois Data, and accompanying accreditation policy points

Dear ICANN:

This document describes a short-term method for authorized parties to access non-public WHOIS data via designated IP addresses. This method is well-known, used in similar cases, and can be deployed in a GDPR-compliant manner. This document addresses questions raised by the Article 29 Data Protection Working Party in its letter to ICANN of 11 April 2018.[1] We kindly request that ICANN factor this proposal into any applicable short-term policy-making plans, and to convey pertinent information to the Article 29 Working Party.

Access would be provided to approved parties (such as security actors) under an approved code of conduct or accreditation/certification program crafted per GDPR guidelines, and enforced by legally binding mechanisms. That access *policy* and the access *method* are two different but related topics. This document does not attempt to describe an entire access policy/program, but does state some organizational and technical measures that should be incorporated into the access policy/program that is created. Below we focus on the *technical access method*.

This short-term access method takes advantage of existing technologies and systems and is practical to implement quickly. The goal is to ensure that authorized parties can have access to vital data while ICANN works out longer-term solutions and deploys the RDAP protocol, processes that may take a year or more. If security actors and law enforcement bodies do not receive access to the data after May 25, in a reliable and predictable fashion, the ability of defenders to find and mitigate Internet crime and fraud will be severely hampered. The Internet, and all personal data on computers connected to it, will become much less safe.

[1] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf

ICANN Org itself will also need a continued access method. ICANN Organization must be able to query contact records in WHOIS every day in order to operate its WHOIS accuracy complaint system, perform compliance investigations, and run its accuracy measurement program.[2] These essential compliance and complaint processes help fulfill the accuracy requirements of the GDPR, which emphasizes that "every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted."[3]

The method below can be used to provide access to both private security actors and law enforcement. While the legal bases under which law enforcement can access the data may differ from the legal bases for non-governmental entities, law enforcement will still need a *technical method or means* to query the data.

The access method would work as follows:

1. As part of the accreditation program vetting process, approved parties designate their rationale(s) for access under GDPR, i.e. their legitimate reasons for accessing the data and the use(s) they will put it to.
2. Approved parties also designate the IP addresses from which they wish to query WHOIS servers.
3. The accrediting bodies provide those IP addresses to ICANN, which collects the IP addresses and access (processing) rationale of each party into a single list.
4. All WHOIS server operators (registries and registrars) will be required to pick up that list from ICANN on a daily basis. They must whitelist access via port 43 from the approved IP addresses, and provide full WHOIS data ("thick" data, containing contact data) for queries coming from those IP addresses.
5. All port 43 operators must designate the locations of their WHOIS servers to be used for this authorized access program. A list of such will be maintained by ICANN and made available to the parties approved for access.

The above process allows a WHOIS server operator to know who the authorized parties are, which party is accessing exactly what data at its server, when, and for what purpose. Below are additional notes about logging.

The method is secure for the following reasons:

A. Port 43 access managed by IP range is appropriately secure for this usage. The method grants access only to allowed parties. IP address restrictions are a widely used and effective method used by a variety of organizations to block access from public (non-approved) locations.

B. Such connections cannot normally be spoofed or forged. Per RFC 3912[4], "WHOIS is a TCP-based transaction-oriented query/response protocol that is widely used to provide information services to Internet users." Since TCP connections are done via three-way handshakes to create a stable and reliable session[5], unlike some other protocols, it is not normally possible to spoof

[2] See ICANN's WHOIS Accuracy Reporting System (ARS) Project at https://whois.icann.org/en/whoisars and information about contact accuracy requirements at https://www.icann.org/resources/pages/inaccuracy-2013-03-22-en

[3] See GDPR Recital 39 and Article 5(1)(d)

[4] https://tools.ietf.org/html/rfc3912

[5] https://tools.ietf.org/html/rfc7414

connections using forged IP addresses[6]. While the WHOIS protocol does not have robust security built into it[7], the WHOIS protocol can be reliably provisioned to limit access to specific IP ranges and log data transfers by IP address. All gTLD registrars and registry operators are contractually required to comply with RFC3912.

C. The approved parties should be required to provide IP addresses that will be used ONLY for accredited WHOIS access, and not for any other purpose, so that access is not possible from the entirety of their networks.

D. Access controlled by IP allows WHOIS server operators to log exactly what approved party has queried what domain name in WHOIS, and to record timestamps of the queries.

E. If desired, registrars and registry operators may provide a separate port 43 server address (e.g. accred.whois.registrarname.com) instead of the public version (e.g. whois.registrarname.com) to be used exclusively by accredited entities with access to it limited by IP addresses. Some operators currently do this.

F. Note that IP address is currently one of the ways that domain registry operators use to authenticate accredited registrars to access their shared registry systems (SRS). While registries layer additional security measures on top of IP-controlled access, that extra security is appropriate in that case because registrars are gaining access to create and modify registry records and perform billable transactions. In contrast, WHOIS servers simply supply data. They do not allow or involve the creation or modification of data, and are operationally separate from the live registry databases.

The method is practical and implementable quickly for the following reasons:

G. ICANN maintains a list of registrars' IP addresses in its secure RADAR database.[8] Registrars currently use this list to white-list each others' IP addresses to provide privileged WHOIS access to each other. (This allows them to obtain registrant and admin contact details to facilitate domain transfers between registrars.) Our plan would leverage this existing list/information distribution resource.

H. The plan would require registrars and registry operators to make minimal changes to their systems. Some port 43 WHOIS operators such as GoDaddy (the world's largest registrar) already offer tiered WHOIS access via IP address, so the amount of work for those parties is practically zero. Some operators already log what WHOIS queries are made from what IP addresses. All registry operators are already contractually required by ICANN to log and report how many WHOIS queries they serve each month.

I. The work involved is reasonable and proportional, and is called for under GDPR's balanced approach, which seeks both privacy and security. We especially call attention to comments made by governments and governmental bodies who emphasize that continued access by private and public security actors is necessary and justified. These include statements from

[6] Some TCP spoofing attacks are possible, but they do not allow the attacker to set up a session and retrieve data. The authors are also aware of BGP hijacking attacks, which could permit an adversary to access WHOIS data. These attacks are noisy, and among other things require the attacker to have knowledge of the white-listed IP addresses. While feasible, such attacks would be quickly detected and mitigated.

[7] The WHOIS protocol uses plain text and does not feature authentication extensions.

[8] https://radar.icann.org/

ICANN's Governmental Advisory Committee[9], Europol's European Cybercrime Center (EC3)[10], the U.K.'s National Crime Agency[11], and the United States Government[12].

The method can and should be implemented with the following controls. The following are designed to provide compliance with GDPR, and address points made by some relevant authorities:

J. ICANN should require that the WHOIS server operators (the registrars and registries) AND the querying parties log all WHOIS queries made under accredited access. Those performing the queries must also log their usage, recording what domains they queried when, to what WHOIS servers, and for what purpose.

K. Binding terms must require that parties accessing non-public WHOIS data must put appropriate internal controls in place at their organizations. This should include technical and security policies to control the storage of the data, to control and limit access to the data to authorized individuals, and to oversee the usage of the data per intended purposes.

L. Access logs must be made available for auditing by data protection authorities. We agree with the European Commission that "The logging and documentation of the queries and safety of the searches should be made available to the competent oversight authorities for the purposes of verifying the lawfulness of data processing, monitoring and auditing and ensuring proper data integrity and security."[13] As always, data protection authorities have the right to enforce GDPR, and data subjects also have the ability to pursue remedies for non-compliance.

M. ICANN or another controlling authority should have provisions that allow it to audit log records for possible misuse.

N. Authorized users that have more than one legitimate purpose for processing data would be expected to designate a separate IP address for each of their purposes. This would allow granular tracking of exactly what queries were made by whom and for what purpose.

O. Requirements should be put in place to ensure that query and log data itself remains confidential by default and can only revealed under specific and narrow legal and contractual justifications. The revelation of log data could, for example, compromise law enforcement investigations and compliance efforts. The European Commission has stated that "Consideration should be given to ensure confidentiality of the requests."[14]

P. Binding terms must state that parties accessing non-public WHOIS data are subject to GDPR's data retention obligations.

Q. Registrars and registry operators must not limit when or how often authorized parties access the data, unless such queries endanger the very stability of the server. It is not the role of the server operator to determine what domains accredited parties are allowed to query.

[9] https://www.icann.org/en/system/files/files/gdpr-comments-gac-icann-proposed-compliance-models-08mar18-en.pdf

[10] https://www.icann.org/en/system/files/files/gdpr-comments-ec3-icann-proposed-compliance-models-02apr18-en.pdf

[11] https://www.icann.org/en/system/files/files/gdpr-comments-nca-icann-proposed-compliance-models-29jan18-en.pdf

[12] https://www.icann.org/en/system/files/files/gdpr-comments-us-government-article-29-wp-whois-20apr18-en.pdf

[13] https://www.icann.org/en/system/files/files/gdpr-comments-european-commission-union-icann-proposed-compliance-models-07feb18-en.pdf

[14] https://www.icann.org/en/system/files/files/gdpr-comments-european-commission-union-icann-proposed-compliance-models-07feb18-en.pdf

R. Regarding data minimization:
    a. Per GDPR, any accredited user will be expected to only process the personal data that it actually needs to process in order to achieve its processing purposes. They will be obligated to minimize the number of queries they make.
    b. The technical solution described above will provide a domain's contact records. A contact record contains the following fields: name, an optional organization field, physical address, telephone number, and email address. It is reasonable to access contact records rather than just isolated data fields within them. Security actors examine entire contact records to determine the veracity of the various data fields, perform correlations, and to reach out to domain contacts by various means. Law enforcement bodies need an entire contact record to establish identity and perform investigations. Other parties will require contact records to file legal proceedings and Uniform Dispute Resolution Policy (UDRP) cases. Finally, access to full contact records rather than just isolated fields is necessary for compliance purposes.
    c. Access to full contact records is essential for compliance purposes, as noted above.

About Us

The Anti-Phishing Working Group (apwg.org) is a not-for-profit research, educational, and industry association dedicated to responding to cybercrime through data exchange, research, and public awareness. The APWG operates cybercrime data exchanges, publishes cybercrime statistics, and presents international cybercrime conferences. It has more than 2,200 members worldwide, including Internet infrastructure and service providers, financial services companies, telecom providers, government CERTs, antivirus firms, and academic researchers.

The Forum of Incident Response and Security Teams (www.first.org) is the premier organization and recognized global leader in incident response. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. Founded in 1990, FIRST consists of computer security incident response teams from more than 414 corporations, government bodies, universities and other institutions across 85 countries.

The Messaging, Malware and Mobile Anti-Abuse Working Group (www.m3aawg.org) is an industry association that develops cooperative approaches for fighting online abuse. It systematically focuses on operational issues of Internet abuse including technology, industry collaboration, and public policy. M3AAWG's membership includes Internet Service Providers (ISPs), telecom companies, Email Service Providers (ESPs), social networking companies, leading hardware and software vendors, major brands, major antivirus vendors, and numerous security vendors.