Lawful and Legitimate WHOIS and Proxy Requests Under GDPR
Snapshot of 2020 Year to Date Numbers (ICANN 69)

Summary

- The following overview summarizes response rates for WHOIS and Proxy data requests from **two leading enforcement vendors and one law firm** on behalf of multiple clients and brands for well-documented and supported requests. Purposes cited in the requests included cybersecurity, DNS abuse, and IP infringement.
- Total WHOIS requests: 4228, Proxy requests: 1342
- WHOIS Requests sent to 221 registrars and 52 registries.
- **79% of WHOIS requests to registrars - 60% of WHOIS requests to thick registries were not fulfilled** -- **for an aggregate of 25% success rates**. This represents a slight decrease from ICANN 68's reported rates of 26%.
- **91% of Proxy requests for the customer's contact data were unfulfilled, and 32% of all Proxy requests had no response at all.** The latter represents a slight improvement from the ICANN 68 Meeting's 43% rate of responsiveness.
- All contributors report resistance by clients in submitting additional reveal requests due to the futility in receiving actual disclosures.
- **Phishing-related requests or obviously fraudulent domains (including COVID ones) are rarely fulfilled even for signatories of the Domain Abuse Framework.**
- The lack of WHOIS data results in an under-detection of phishing domain names, causing delays in mitigation of phishing attacks.

Detailed Breakdown of Request Responses

WHOIS Requests for Redacted Information 4228 requests	Percent	PROXY - 1342 requests	Percent
Fully Compliant (1037)	25%	127	9%
No Response at all (1177)	28%	424	32%
Rejected for Pay for Reveal or Other Reasons (530)	13%	105	8%
Rejected for Legal Action (UDRP/Subpoena required) (1240)	29%	208	15%
Dropped or Suspended (73)	2%	8	1%
Auto Acknowledgement with No Follow-Up (260)	6%	92	7%
Requires Additional Action (311)	7%	77	6%
Average days for acknowledgement	4	2	
Average days for compliant response	7	7	

Additional Information

- After two years after the adoption of the Temporary Specification, we still see a large number of registrars that do not respond at all. One vendor reported 32 registrars that do not respond at all to WHOIS requests. It's clear ICANN has not conducted any meaningful audits or enforcement actions to bring registrars into compliance.
- 87 registrars responded to WHOIS requests but did not provide registrant data citing legal authority, requiring a subpoena or UDRP filed.
- The aggregate number of requests over the last two years have dropped substantially due to futility (e.g. where a registrar universally rejects requests and demands a subpoena or UDRP many entities have stopped submitting requests).
- Phishing-related requests or obviously fraudulent domains are rarely fulfilled even for signatories to the Domain Abuse Framework. This trend continued even with regard to COVID related domain names. Examples: <coronavirusmedicalkit.com> (FBI request), <facebookcovid19.com>.
- According to the Interisle Phishing Landscape 2020 Report, the practical lifetime of a phishing attack is only 21 hours. That is the average time from the first visit by a victim to the last visit by a victim. This study reveals that sixty-five percent of maliciously registered domain names are used for phishing within five days of registration. With responses to WHOIS requests averaging 7 days, the information is received too late to protect consumers.
- This Interisle Phishing Landscape 2020 Report notes that the lack of WHOIS data results in an under-detection of Phishing domain names. This is because there is no quick way to verify whether a domain name is registered to the brand holder or an imposter seeking to defraud consumers.
- One vendor reports that in some cases where registries and registrars are trying to cooperate with security investigations, their data arrives long after the phishing attack is over and the culprit has moved on to their next target.
- There are virtually no responses for privacy/proxy reveal requests from most registrars. This is problematic as NABP's White Paper notes that 90% of the COVID related domains identified utilized anonymized domain name registrations.
- There are inconsistent results depending on the type of WHOIS query made; some machine lookups through Port 43 or RDAP provide thin or unredacted data, but additional WHOIS may be available through the registrar's website. See the Interisle Report: Domain Name Registration Data at the Crossroads for more details.
- Examples of uncooperative behavior by some prominent registrars:
    - Requestors are obliged to use an online form, which is non-functioning, or which significantly limits the number of characters allowed for requests, making it difficult to provide the necessary information to support the request.
    - Various registrar email addresses send automated responses without follow-up on the request or send requestors back to a non-functioning online form.
    - Requestors are obliged to provide very detailed information, and then are told the registrant is a proxy service and no useful WHOIS data is provided.