April 2023: New Domain Activity Highlights

Posted on May 4, 2023

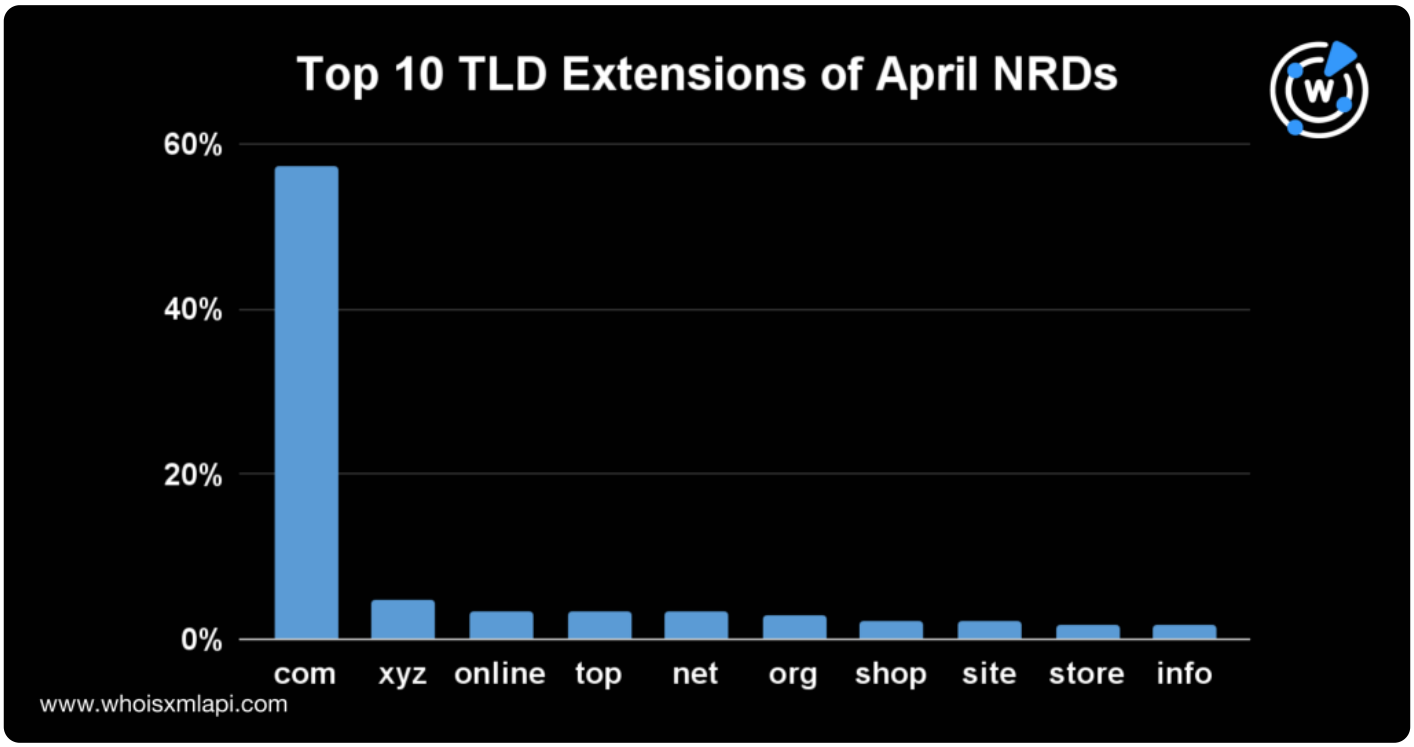
Of the millions of domains registered during 1–30 April 2023, WhoisXML API researchers studied a randomized sample of 29,000 domains to determine commonalities in their registrant country, registrar, and TLD. Our analysis also included looking into the domain registration volume for the riskiest or most-abused TLDs.

Additionally, the researchers examined domain text string usage to uncover potentially emerging trends. This study's findings and links to threat reports developed using DNS, IP, and domain intelligence sources are summarized below.

Zooming in on the April NRDs

TLD Distribution

The top TLD extension remained .com, accounting for 57% of the domains registered in April. The rest of the top 10 TLDs trailed significantly behind, including .xyz with a 5% share; .online, .top, .net, and .org with shares of 3% each; and .info with a 2% share. The e-commerce-focused .shop, .site, and .store extensions also made the top 10, each accounting for 2% of the total registration volume.

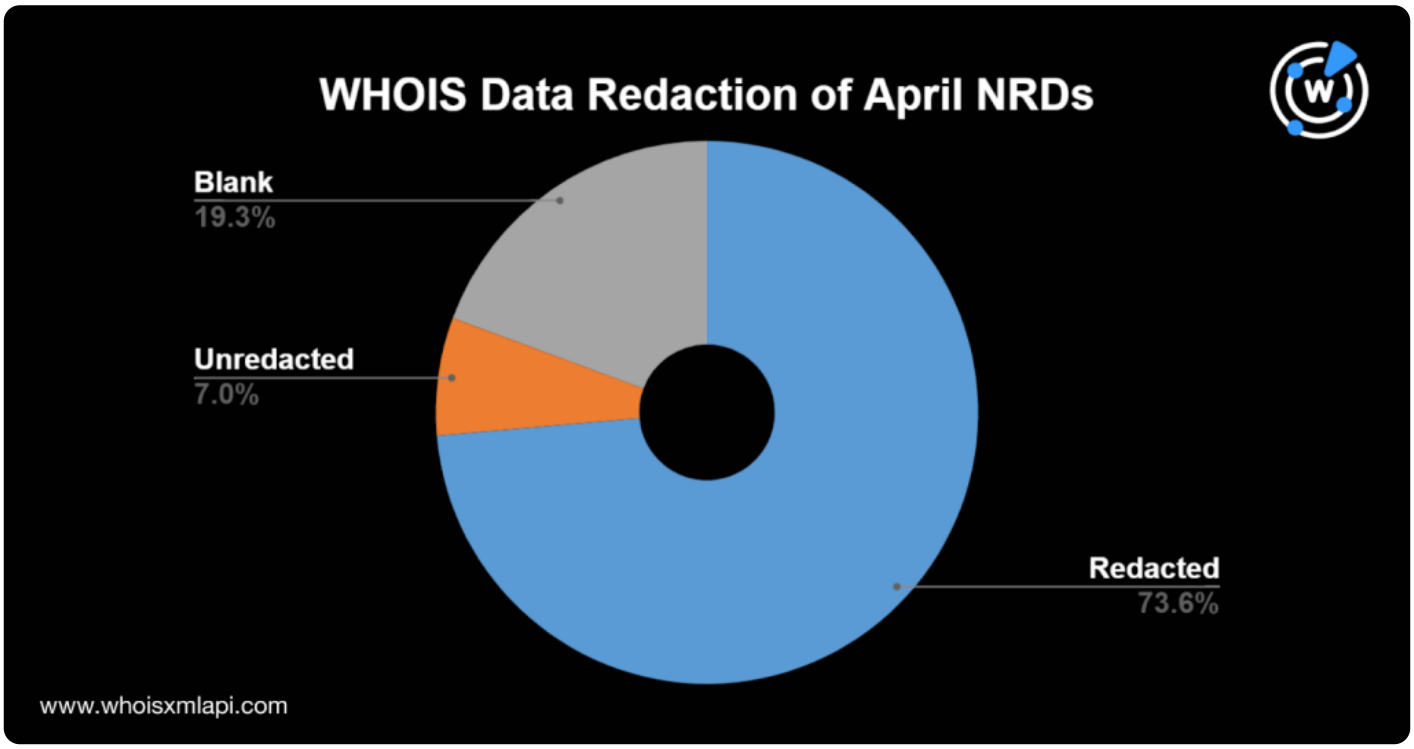


About 11.4% of the April NRDs had the riskiest TLD extensions named by Infoblox in their Q4 2022 Cyber Threat Report. These TLDs had the worst reputation, having a high volume of malicious domains and were considered high-confidence and -risk TLDs. The table below shows a sample of these extensions.

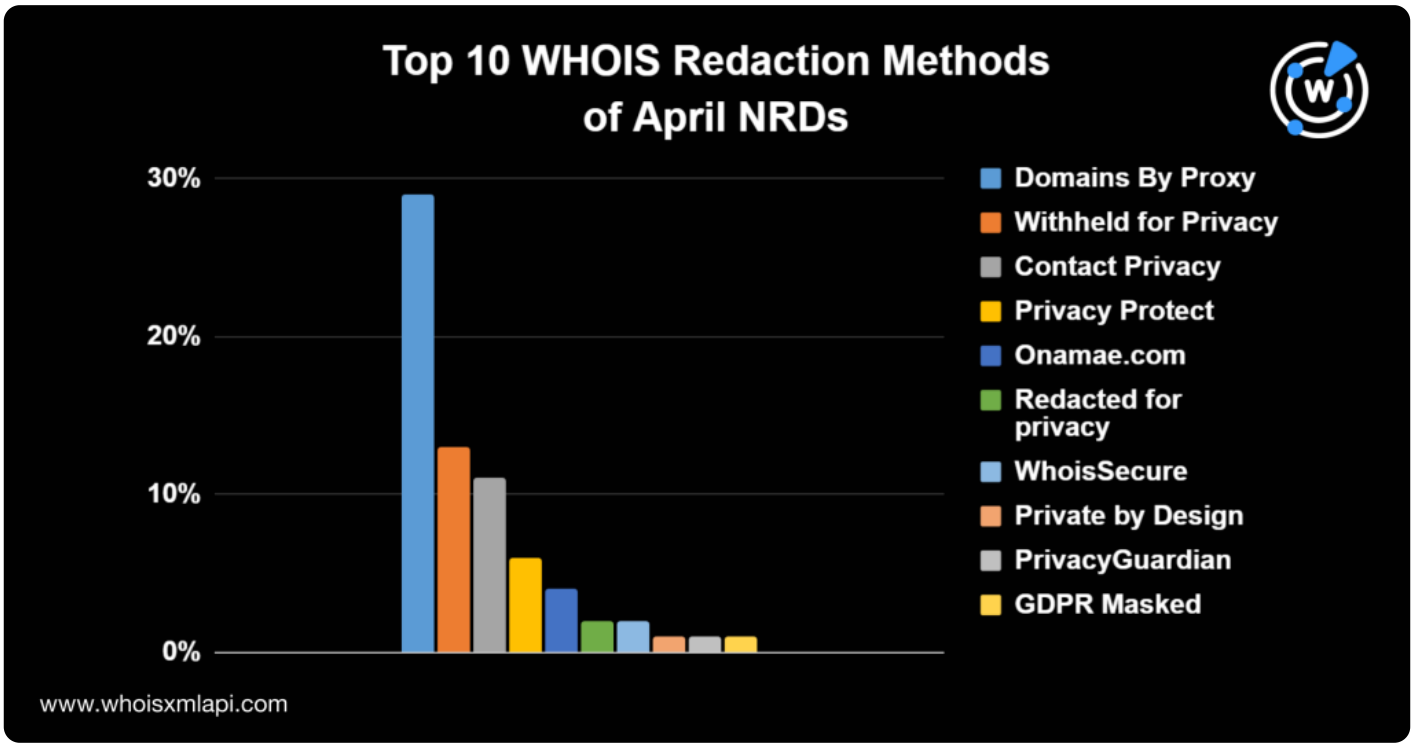
TLD	Domain Registration Share against the Total April NRD Volume
.xyz	4.785%
.top	3.395%
.click	0.724%
.buzz	0.613%
.live	0.501%

WHOIS Data Redaction

Based on the NRDs' registrant organization, 74% had redacted WHOIS records, indicating a slight decrease from the previous month. About 19% of the registrants left the organization field blank, while only 7% had public registrant details.

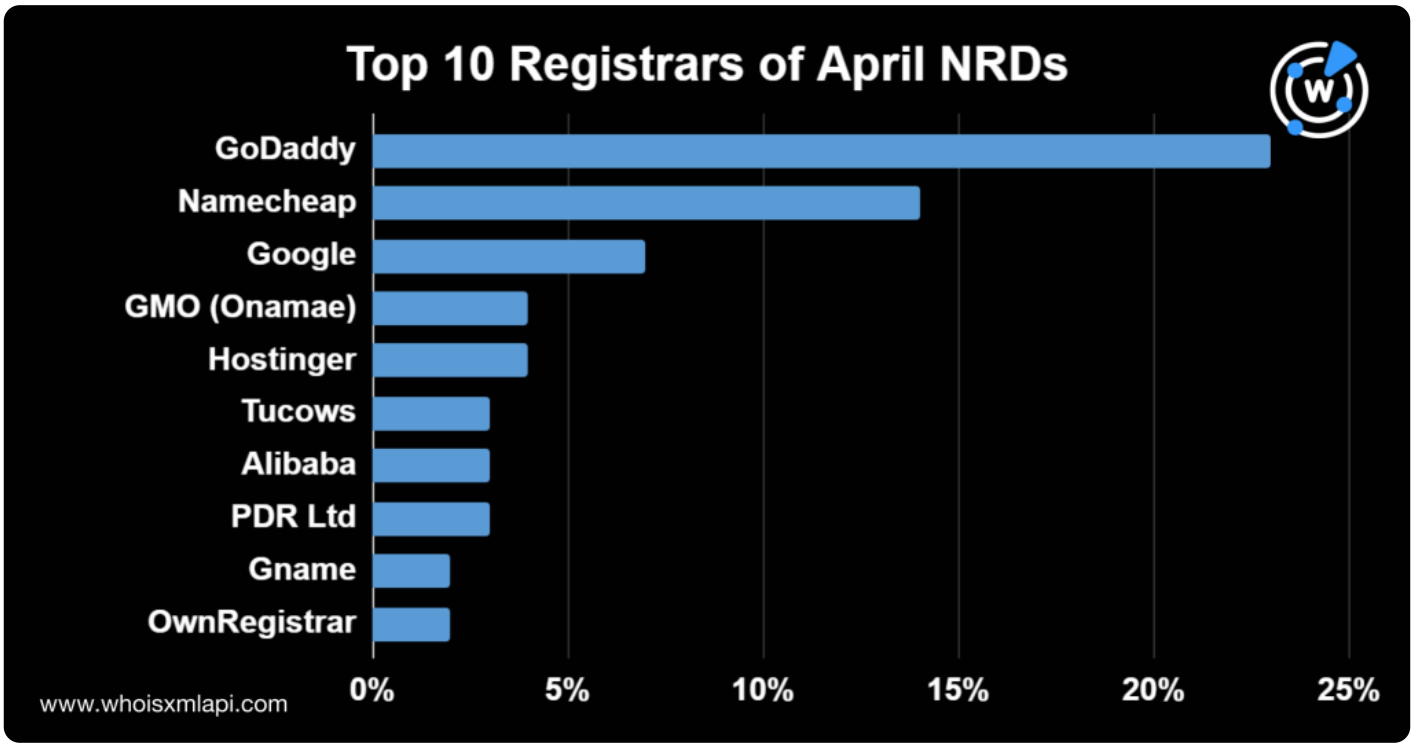


Domains By Proxy was the top WHOIS privacy protection provider, with a 30% share, followed by Withheld for Privacy EHF (13%); Contact Privacy, Inc. (8%); and Privacy Protect LLC (6%). The chart below shows the top 10 redaction service providers.



Registrar Distribution

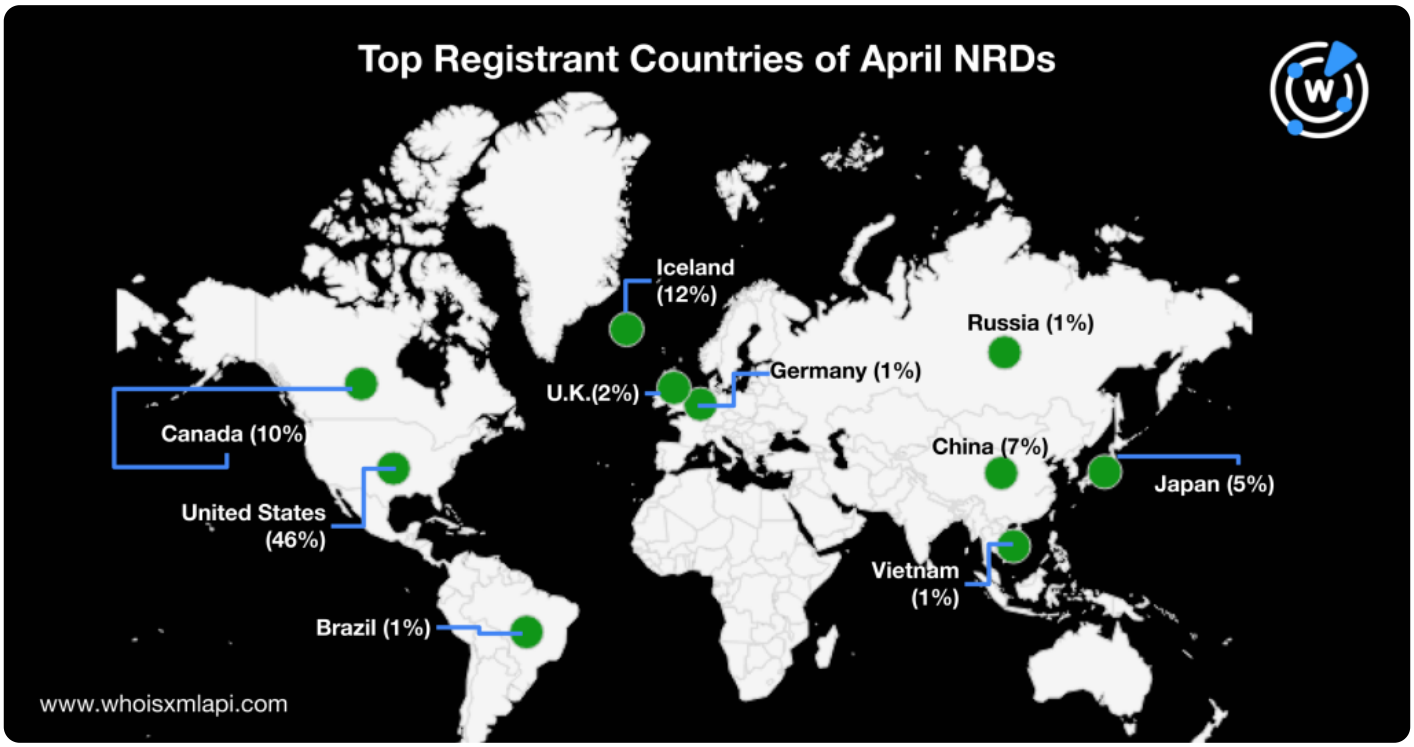
GoDaddy remained the top registrar in April 2023, accounting for 23% of the total domain registration volume. Namecheap took the second place with a 14% share, followed by Google (7%), Hostinger and GMO Internet (4% each), Tucows (3%), Alibaba (3%), PDR Ltd. (3%), Gname.com (2%), and OwnRegistrar (2%).



The top 10 registrars accounted for 65% of the total registration volume. The rest of the domains were distributed across more than 350 other registrars.

Top Registrant Countries

About 46% of the April NRDs were registered in the U.S., while Iceland and Canada accounted for 12% and 10% of the registrations, respectively. Other countries that made it to the top 10 registrant countries in April were China, Japan, the U.K., Russia, Germany, Brazil, and Vietnam.



Appearance of Common Strings among the SLDs

Xn remained among the most-used text strings, highlighting the continued popularity of internationalized domain names (IDNs). Also, tech terms, such as ***app*** and ***ai***, remained common among the NRDs. ***Gpt*** was also repeatedly used.

The appearance of ***game***, ***bet***, ***best***, and ***job*** is also noteworthy. The word cloud below shows these and other commonly used strings.

Cybersecurity through the DNS Lens

Below are some of the threat reports we published in April.

- **Discovering Potential BEC Scam Vehicles through the DNS:** WhoisXML API researchers analyzed publicly available indicators of compromise (IoCs) connected to business email compromise (BEC) scams targeting executives and discovered thousands of additional artifacts.

- **Looking for Traces of Social Media-Based Celebrity Scams in the DNS:** Our researchers found 1,600+ artifacts connected to IoCs tagged in malicious campaigns impersonating politicians and celebrities.

- **Detecting Possible Fraud Vehicles Specific to Latin America and the Caribbean:** We zoomed in on fraud proliferating in Latin America and the Caribbean (LAC), discovering nearly 10,000 cybersquatting domains targeting the region's airline and digital wallet

industries.

- **Drawing the Line between SYS01 and Ducktail through DNS Traces:** We looked into the DNS-based commonalities between SYS01 stealer and Ducktail, two malware families recently found going after Facebook business owners and advertisers. Our investigation led us to 3,000 IP-connected domains.

- **Black Basta Ransomware DNS Investigation Led to OneNote and Courier Impersonation:** Our team investigated IoCs related to Black Basta ransomware, discovering nearly 1,000 domains sharing the IoC domains' WHOIS infrastructure, some of which were malicious and imitated OneNote and courier services.

You can find more reports created in the past months here.

Feel free to contact us for more information about the products and capabilities used to analyze domain registration events or support other use cases.