July 2023: Domain Activity Highlights

Posted on August 3, 2023

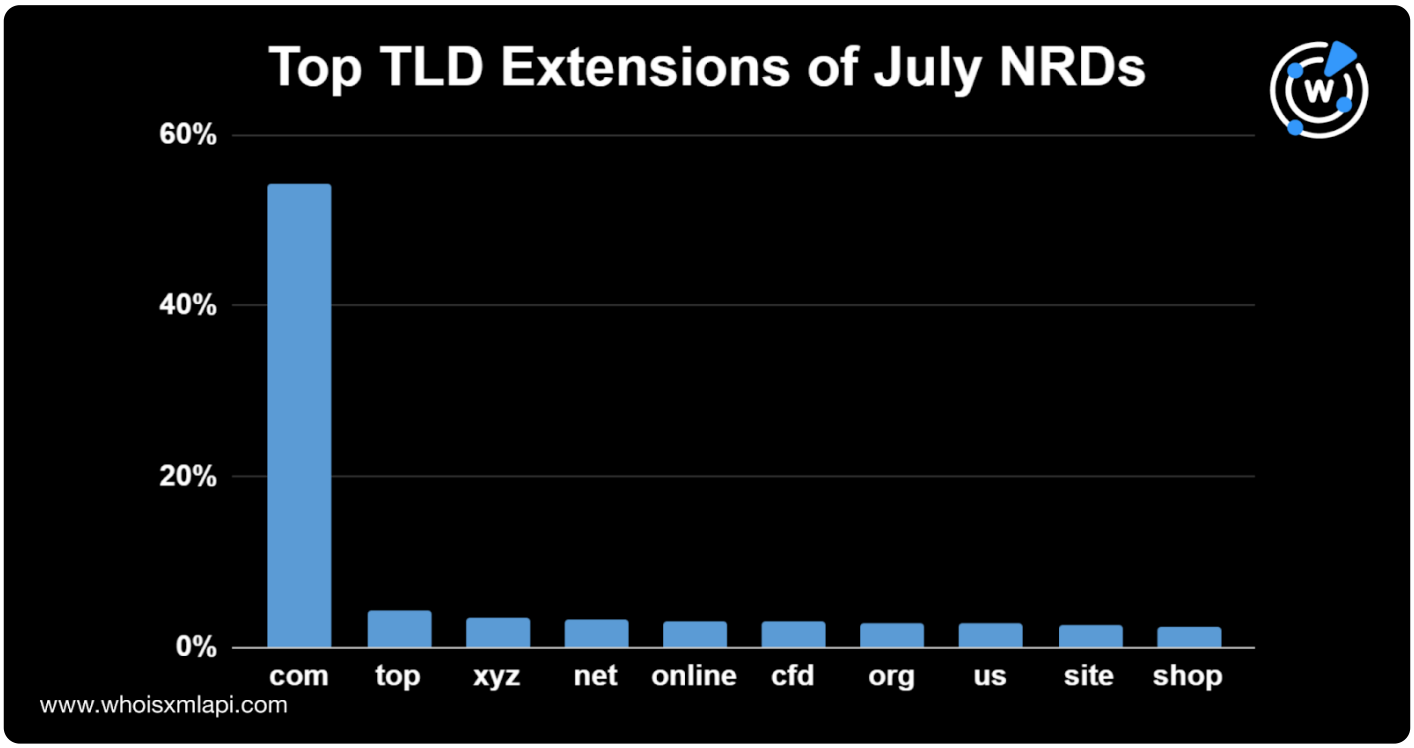
Of the millions of domains registered on 1–31 July 2023, WhoisXML API researchers studied a randomized sample of 31,000 to determine commonalities in their WHOIS data, registrant country, registrar, and TLD.

In addition, we examined the domains' 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 July NRDs

TLD Distribution

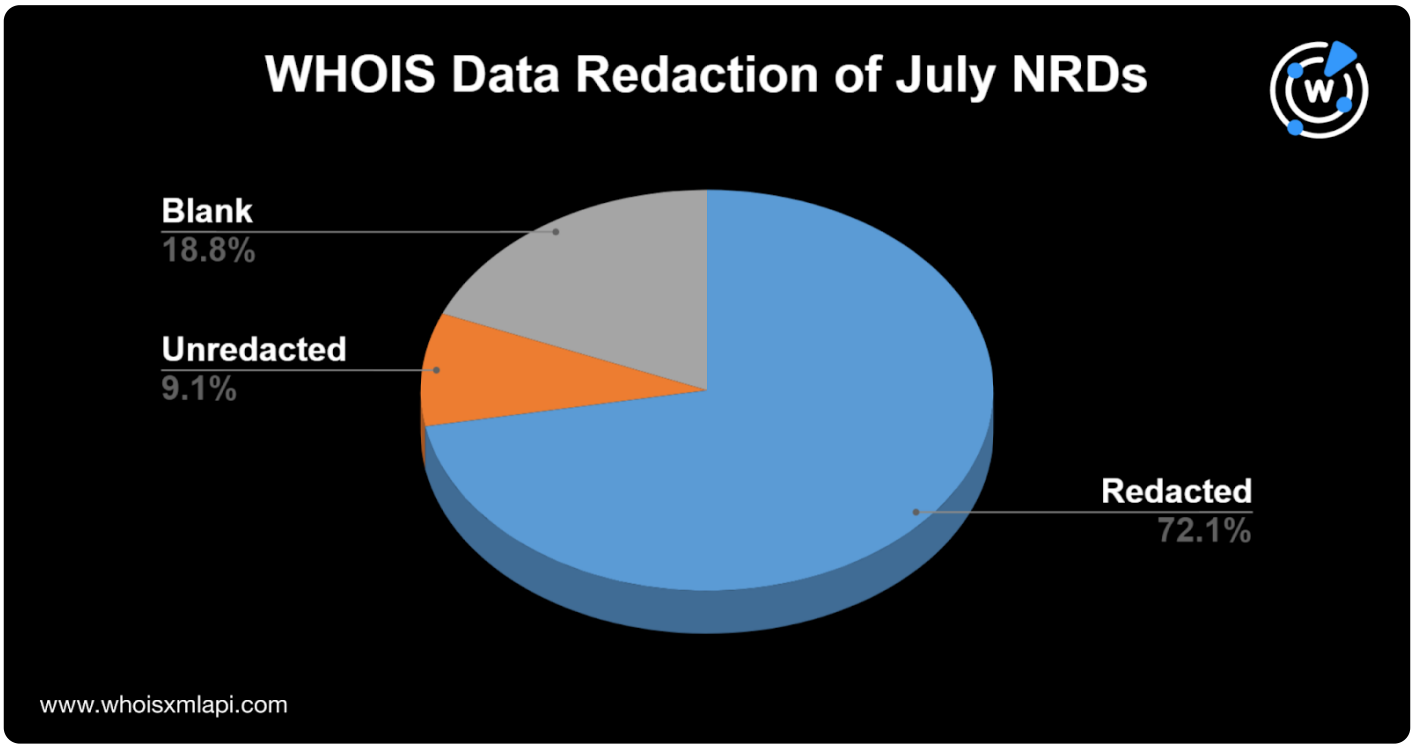
Most of the top 10 TLD extensions in June continued to be so in July, except for .info, which .us replaced. The .com TLD remained the most used, accounting for 54% of the total domain registration volume. The rest of the top 10 TLD extensions were .top (4%), .xyz (3%), .net (3%), .online (3%), .cfd (3%), .org (3%), .us (3%), .site (3%), and .shop (2%), as shown in the chart below.



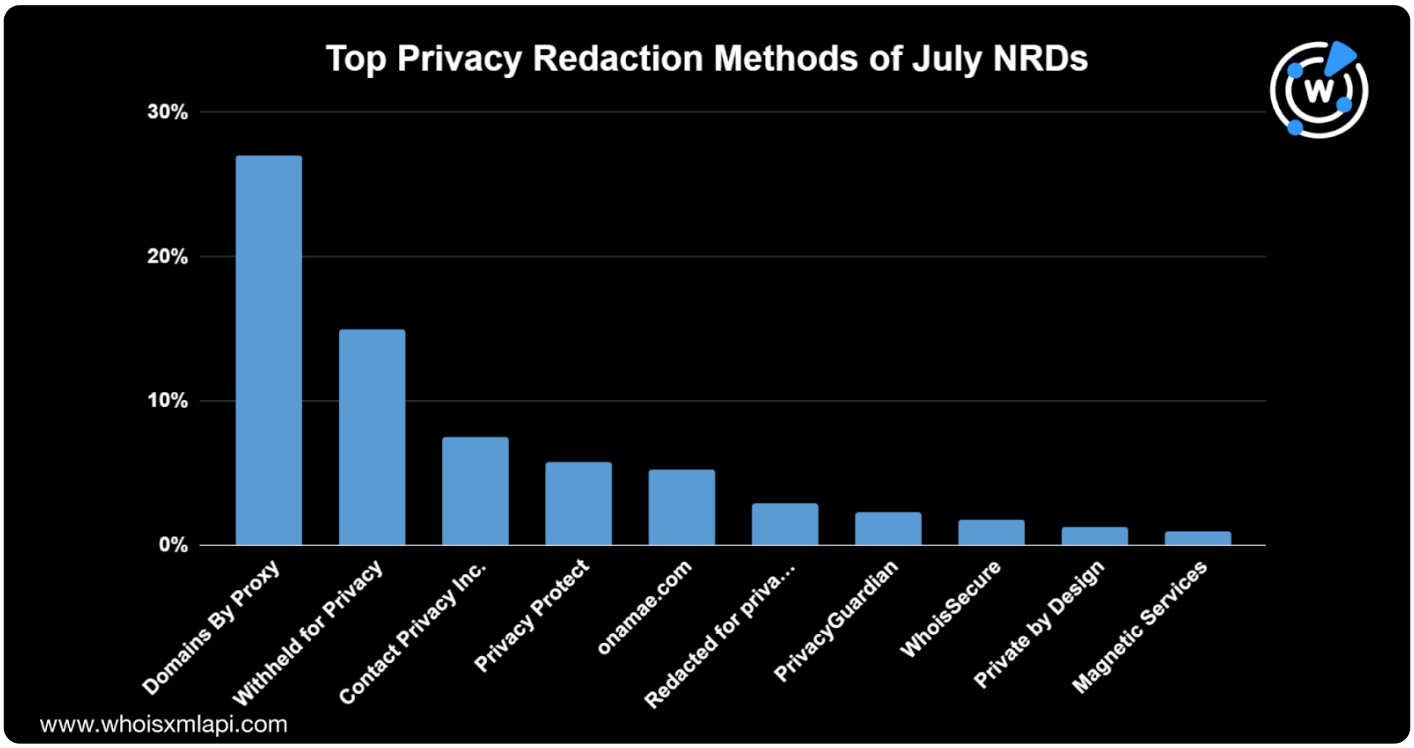
The top 10 TLD extensions accounted for 82% of the new domain registration volume. The remaining 18% were distributed across more than 620 TLDs.

WHOIS Data Redaction

A majority of the new domains had redacted WHOIS records, with only 9% that had their registrant organization public, while almost 19% had this field blank.



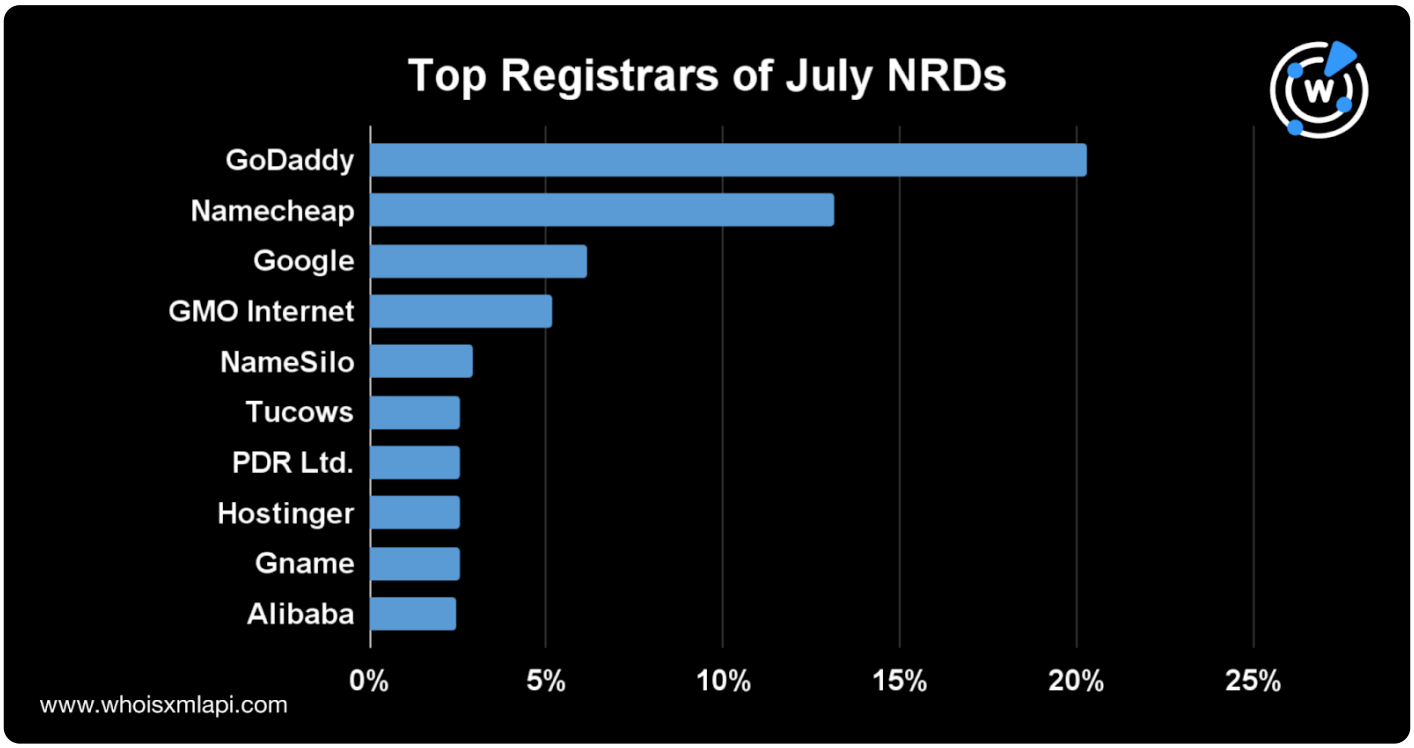
Domains By Proxy remained the most popular privacy redaction service provider, accounting for 27% of the new domain registration volume. It was followed by Withheld for Privacy with a 15% share; Contact Privacy with 7%; Privacy Protect, LLC with 6%; Onamae with 5%; PrivacyGuardian.org and WhoisSecure with 2% each; and Private by Design and Magnetic Services with 1% each.



Several NRDs' registrant organization fields also contained labels like **Private Person**, **Redacted for privacy, Data Redacted,** and **GDPR Masked**.

Registrar Distribution

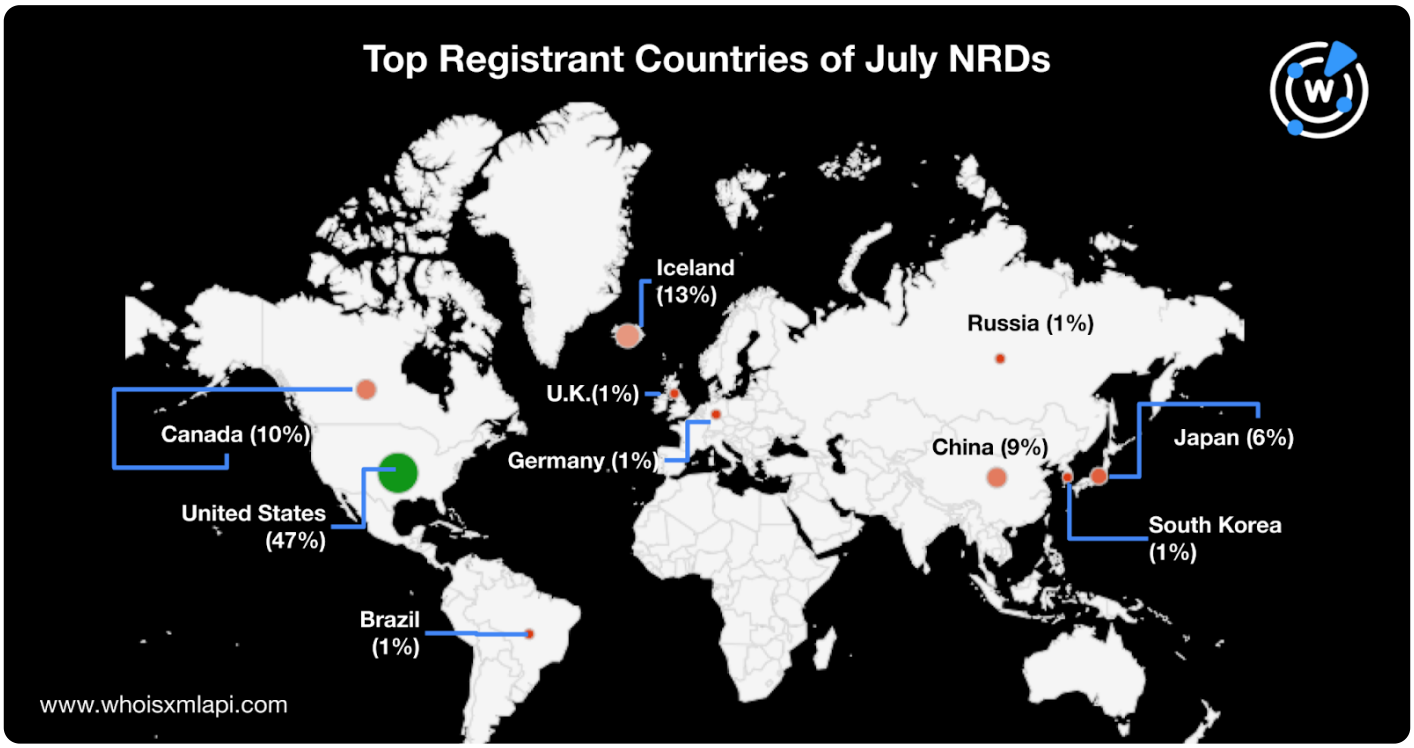
The top registrars remained the same as in June, with GoDaddy leading the pack, accounting for 20% of the total domain registration volume. Namecheap followed with a 13% share; Google with 6%; GMO Internet with 5%; and NameSilo, Tucows, PDR Ltd., Hostinger, and Gname with 3% each. Completing the top 10 was Alibaba, accounting for 2% of the domain registration volume in July.



The top 10 registrars accounted for 60% of the total registration volume. The rest of the domains were distributed across more than 430 other registrars.

Top Registrant Countries

Nearly half of the new domains were registered in the U.S. (47%). As in previous months, Iceland and Canada followed, accounting for 13% and 10% of the total registration volume, respectively. The rest of the top 10 registrant countries were China (9%), Japan (6%), the U.K. (1%), Russia (1%), South Korea (1%), Brazil (1%), and Germany (1%).

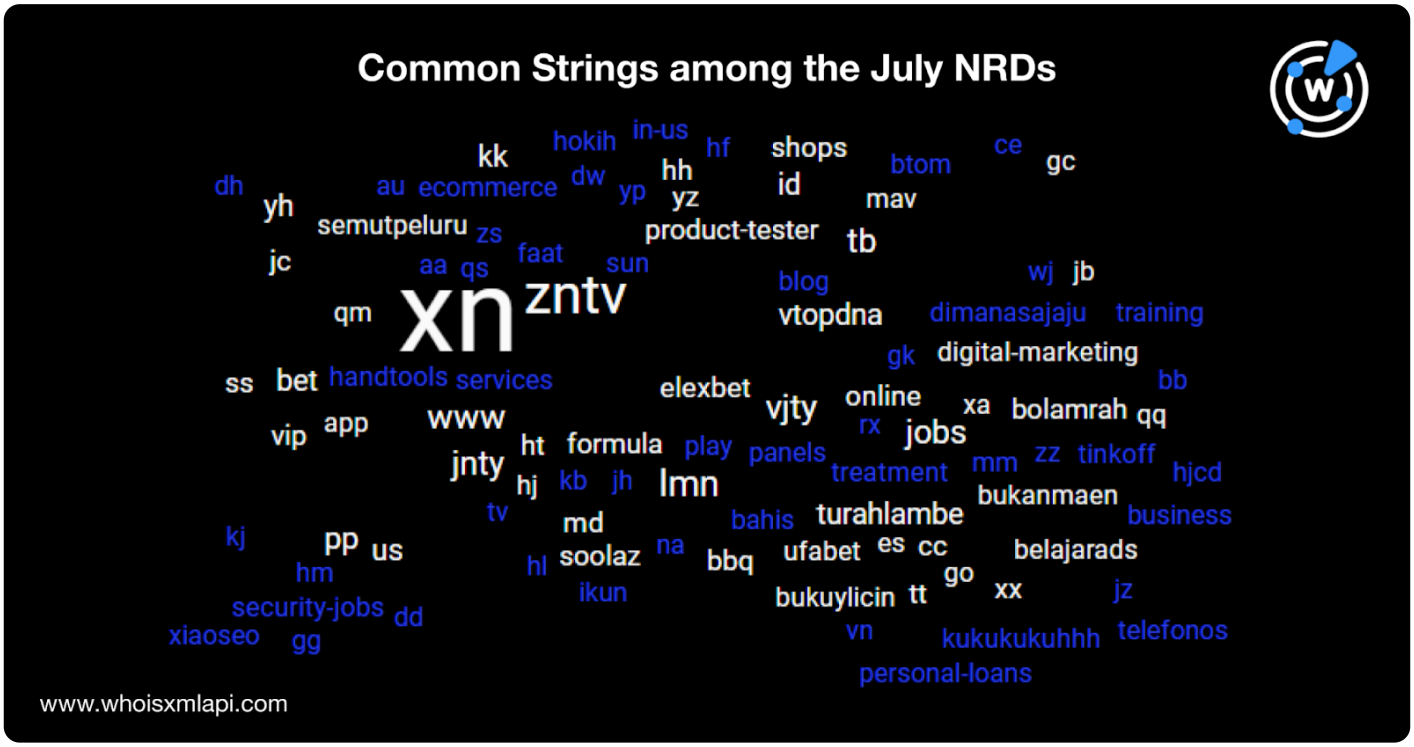


The top 10 registrant countries accounted for 89% of the total registration volume. The rest of the domains were distributed across more than 130 other countries.

Appearance of Common Strings among the SLDs

Terms related to the Internet and technology were among the most commonly found among the new domains. Examples include **app**, **digital-marketing**, **e-commerce**, **services**, **security-jobs,** and **shops**.

The word **bet** also repeatedly appeared alongside other strings, while **xn** remained popular, hinting at the continuous usage of internationalized domain names (IDNs).



Cybersecurity through the DNS Lens

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

- **A DNS Deep Dive into Malware Crypting:** WhoisXML API researchers expanded lists of indicators of compromise (IoCs) connected to malware crypting services, uncovering hundreds of domains hosted on attacker-owned IP addresses.
- **BlackCat Hacks Reddit Again, Take a Look at What the DNS Revealed:** Our researchers analyzed more than a dozen IP addresses tagged as IoCs in the recent cyber attack against Reddit, leading them to 450+ domains containing suspicious strings.
- **MOVEit Exploit-CLOP Ransomware Threat Vector Identification Aided by DNS Intelligence:** Our researchers investigated 139 IoCs related to the MOVEit-enabled CLOP ransomware attacks and found 6,600+ domains containing the string **zoom**.

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.