May 2023: New Domain Activity Highlights

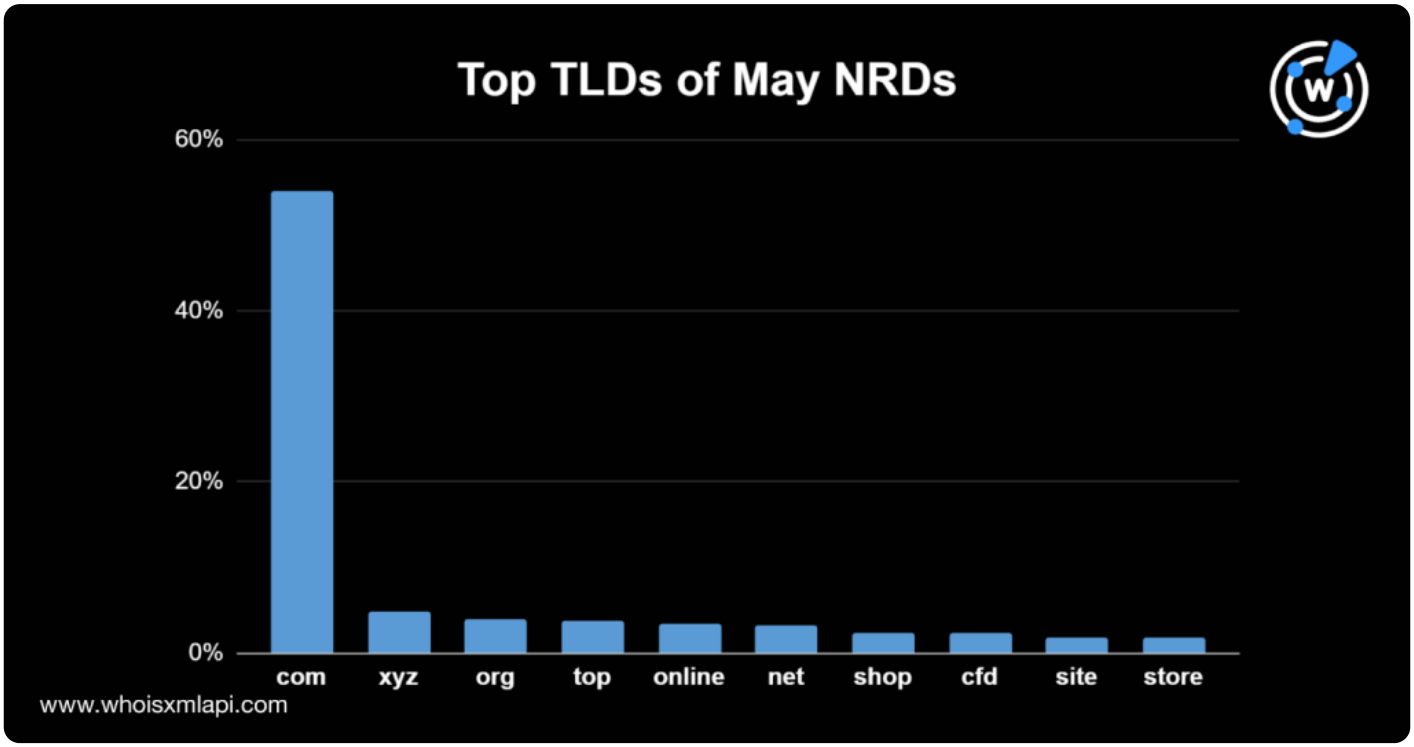
Posted on June 5, 2023

Of the millions of domains registered on 1–31 May 2023, WhoisXML API researchers studied a randomized sample of 31,000 domains to determine commonalities among their registrant countries, registrars, and TLDs. We also examined 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 May NRDs

TLD Distribution

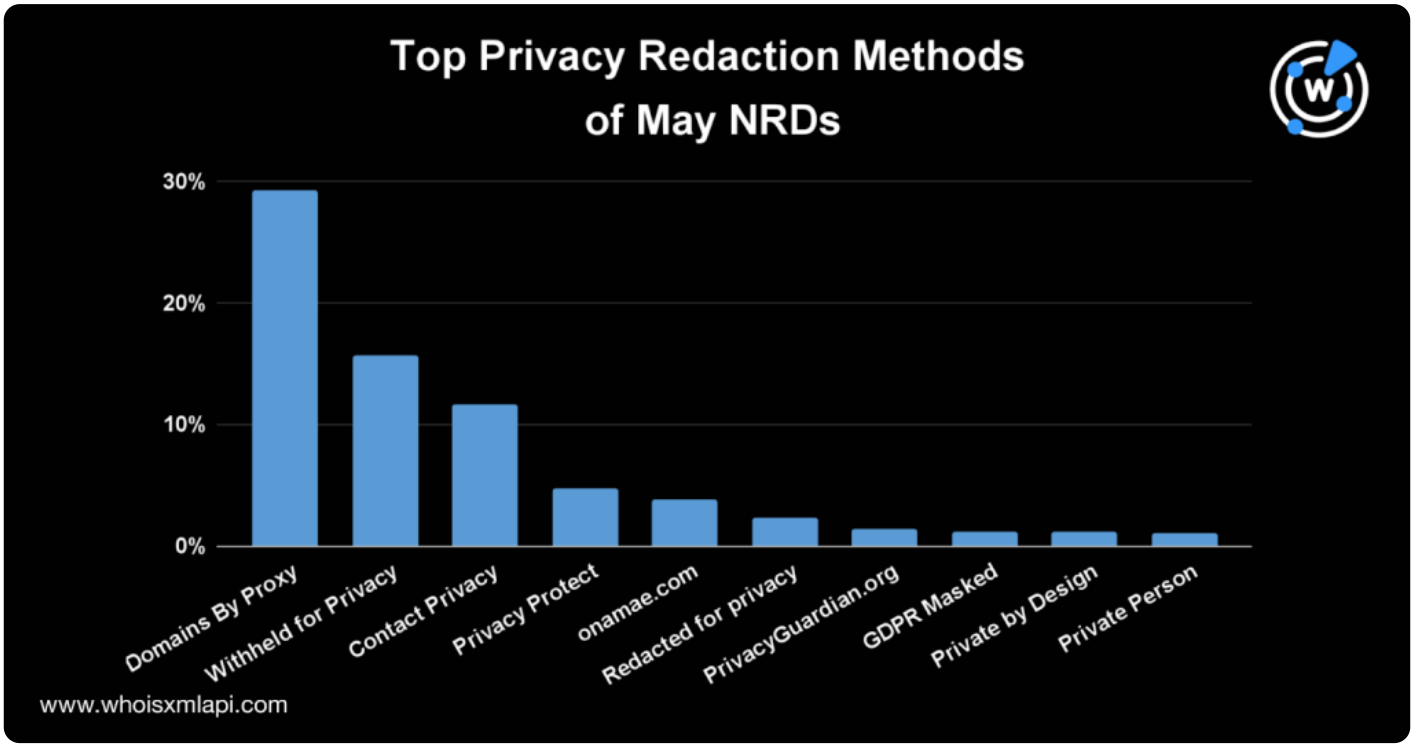
The .com TLD extension remained the most used, accounting for 54% of the total May domain registration volume. In second place was .xyz, with a 5% share. The .org TLD extension went up a notch to the third from the sixth spot in April, with a 4% share. The rest of the top 10 mostly remained the same, except for .cfd, which accounted for 2% of the total and replaced .info.



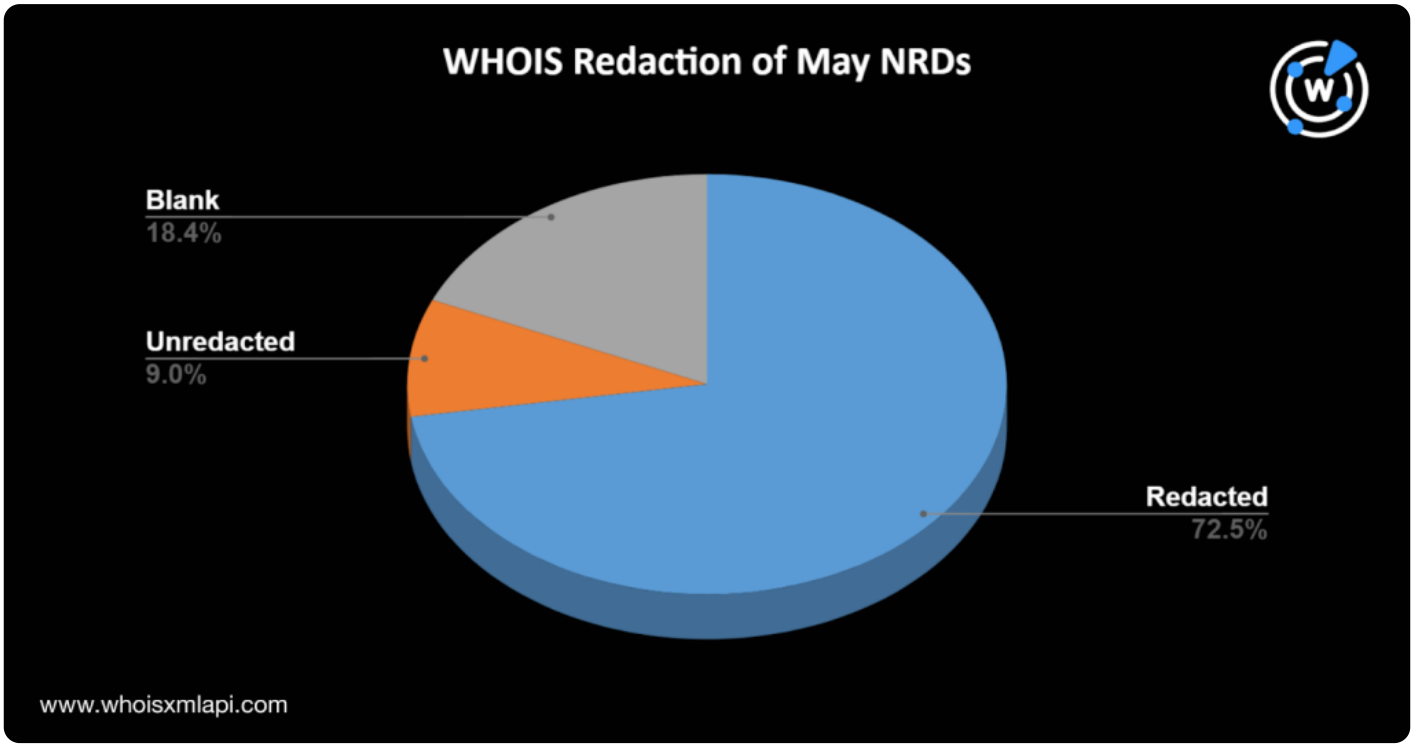
WHOIS Data Redaction

About 73% of the NRDs had redacted WHOIS records, most of which used Domains By Proxy, LLC (29%), followed by Withheld for Privacy (16%) and Contact Privacy (12%). The rest of the top 10 privacy protection service providers were Privacy Protect (5%), Whois Privacy Protection Service by onamae.com (4%), PrivacyGuardian.org (1%), Private by Design, LLC (1%), and Whois Proxy (1%).

Some registrants used the terms ***Redacted for privacy*** (2%) and ***GDPR Masked*** (1%) in their registration organization fields.

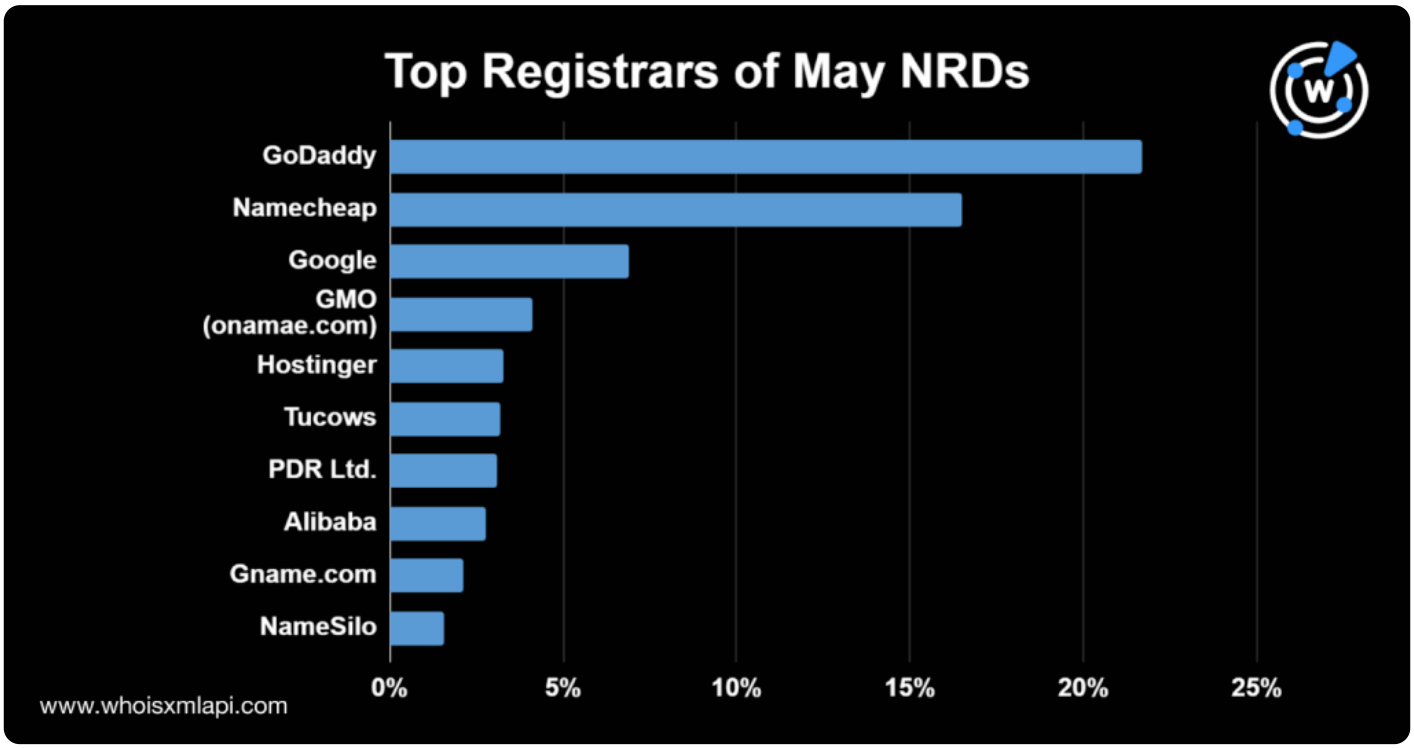


Only 9% of the NRDs had unredacted WHOIS records based on their registrant organization fields. Even fewer had public registrant email addresses. Finally, around 18% of the NRDs left their registrant organization details blank.



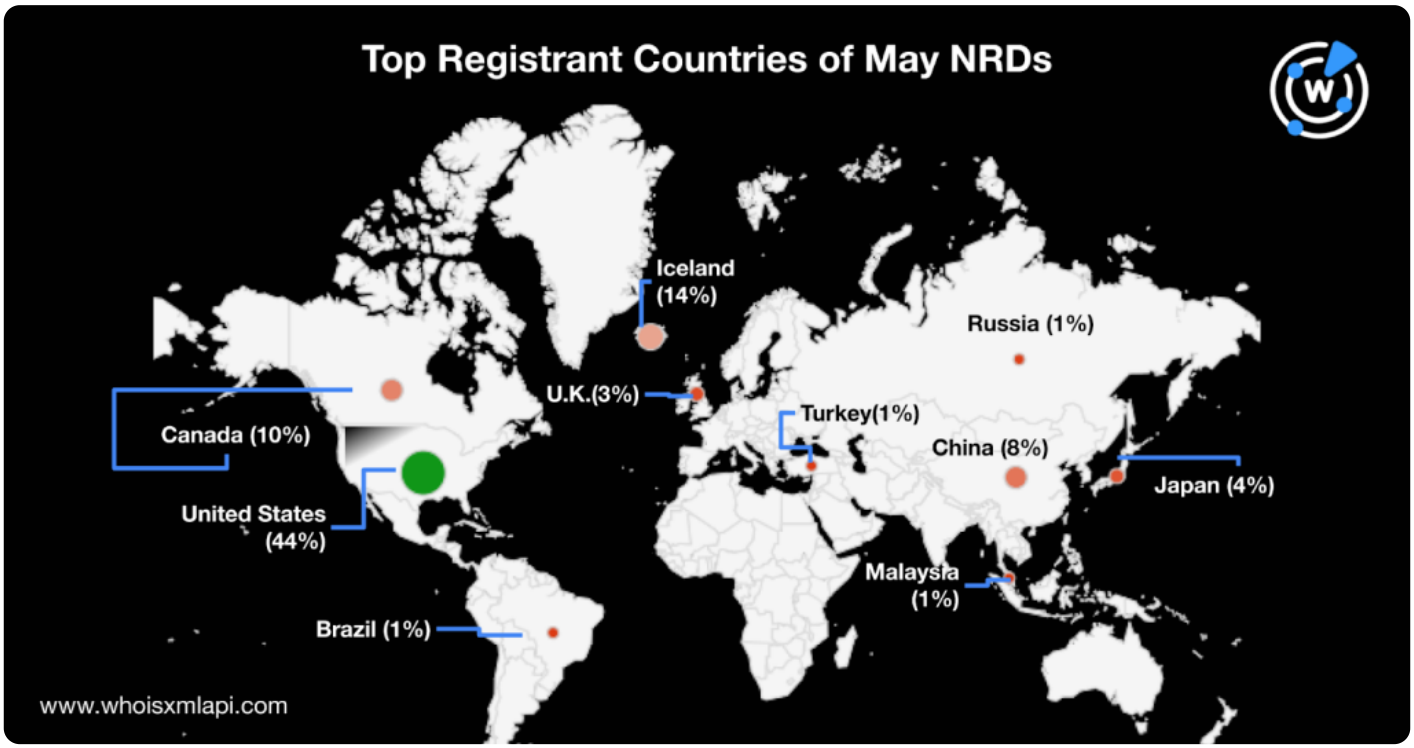
Registrar Distribution

GoDaddy has been the top registrar for months and remained so in May, accounting for 22% of the total domain registration volume. It roughly accounted for the same volume in March and April. The other registrars on the top 10 remained the same, too. They were Namecheap (16%), Google (7%), GMO Internet (4%), Hostinger (3%), UAB (3%), Tucows (3%), PDR Ltd. (3%), Alibaba (3%), Gname.com (2%), and NameSilo (2%).



Top Registrant Countries

The U.S. accounted for 44% of the total NRD volume, followed by Iceland with a 14% share, Canada with 10%, China with 8%, and Japan with 4%. The U.K., Russia, Malaysia, Turkey, and Brazil completed the top 10 registrant countries.



Appearance of Common Strings among the SLDs

The popularity of internationalized domain names (IDNs) continued to ensue, as ***xn*** remained among the most-foundused text strings. Tech terms like ***ai***, ***it***, and ***app*** and e-commerce strings, such as ***shop***, ***store***, and ***sale***, were also commonly found among the NRDs.

The appearance of ***job***, ***bet***, and ***live*** was also noteworthy. The word cloud below shows these and the other commonly used strings.

Cybersecurity through the DNS Lens

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

- **DNS Snooping on Apple iOS 14 Zero-Click Spyware KingsPawn:** WhoisXML API researchers scoured the DNS for artifacts associated with KingsPawn, a new spyware modeled after the NSO Group's Pegasus.
- **When Marketing Vendors Get Attacked, Clients Suffer: Third-Party Risk Discovery in the DNS:** After AT&T suffered a data breach due to a security incident that targeted its marketing vendor, our researchers decided to look into web properties potentially impersonating some of the most popular marketing vendors today.
- **Scouring the DNS for Traces of Bumblebee SEO Poisoning:** WhoisXML API researchers performed a list expansion analysis on dozens of Bumblebee SEO poisoning attack IoCs, enabling us to uncover more than 1,900 potentially connected artifacts.
- **A DNS Deep Dive: That VPN Service May Be OpcJacker in Disguise:** Our researchers

looked into OpcJacker, a data-stealing malware posing as a VPN software installer.

- **Searching for Nevada Ransomware Digital Crumbs in the DNS:** Our research team investigated and expanded the list of IoCs related to the Nevada ransomware that uncovered a possibly related email address and IP addresses and thousands of domains.

You can find more reports we 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.