WhoisXMLAPI

March 2023: New Domain Activity Highlights

Posted on April 5, 2023

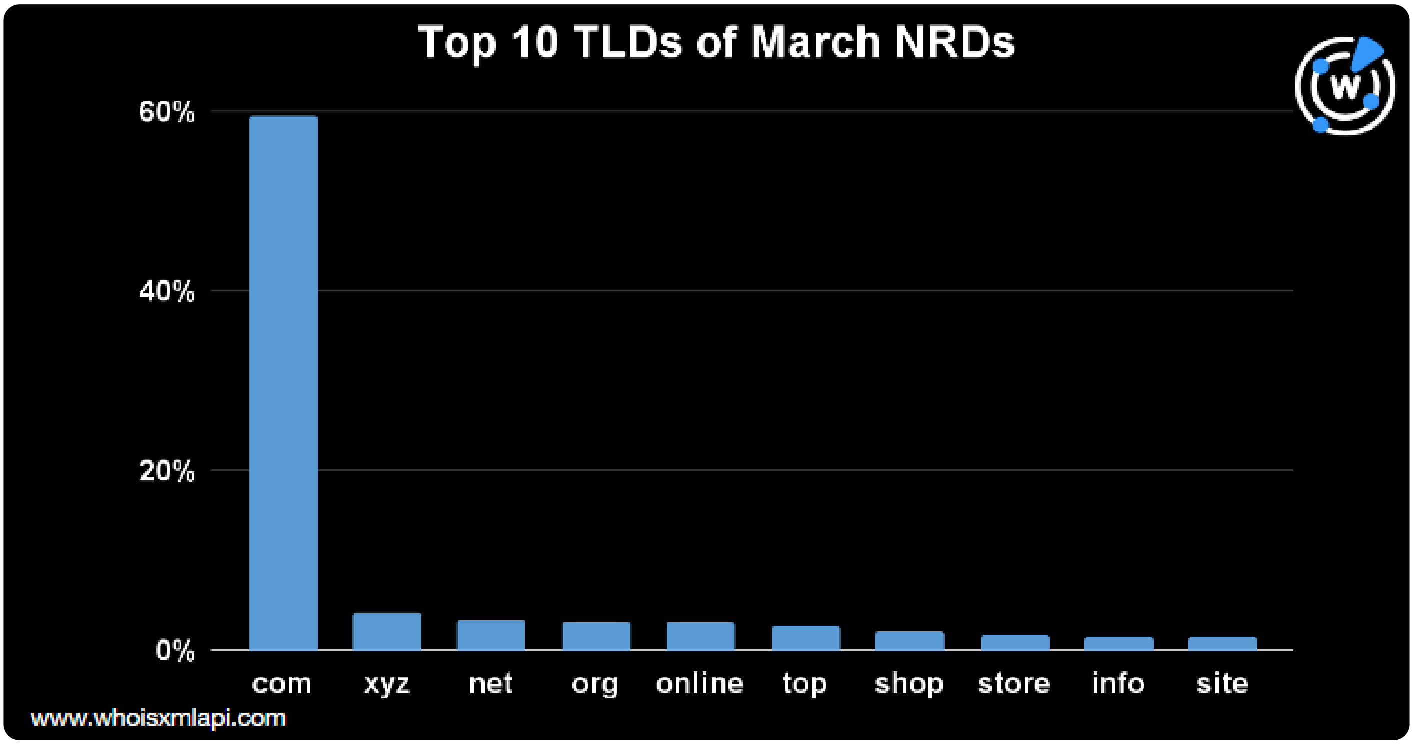
Of the millions of domains registered during 1–31 March 2023, WhoisXML API researchers studied a randomized sample of 31,000 domains to determine commonalities in their registrant countries, registrars, and TLDs. Part of our analysis also included looking into the domain registration volume for the riskiest or most-abused TLDs.

We also analyzed domain text string usage to detect potentially emerging trends. Check out our findings below and links to the threat reports our researchers put together using our domain, DNS, and IP intelligence sources.

Zooming in on the March NRDs

TLD Distribution

The top TLD extension remained .com, accounting for 60% of the domains registered in March. Trailing significantly behind were .xyz and .net with 4% of the total registration volume each. The .org, .online, and .top TLDs followed closely with 3% shares each. The e-commerce-focused .shop and .store extensions also made the top 10, each accounting for 2% of the total registration volume. Rounding out the top 10 were .info and .site, also with 2% shares each.



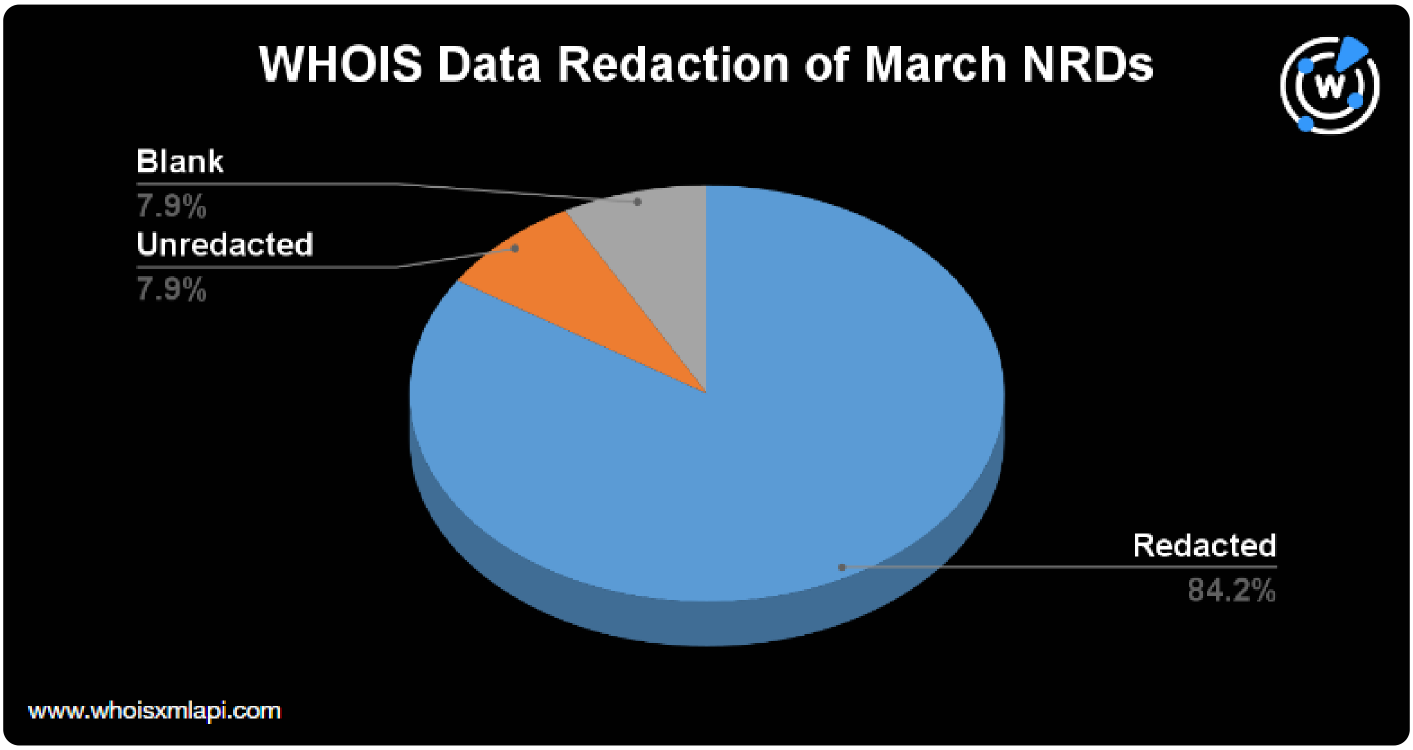
About 10.6% of the March NRDs belonged to the riskiest TLD extensions named by Infoblox in their Q4 2022 Cyber Threat Report. The table below shows some of the TLDs with the worst reputations in terms of number of malicious domains and were considered as high-confidence and high-risk TLDs.

TLD	Domain Registration Share against the Total March NRD Volume
xyz	4.227%
top	2.855%
buzz	0.777%
click	0.723%
live	0.579%

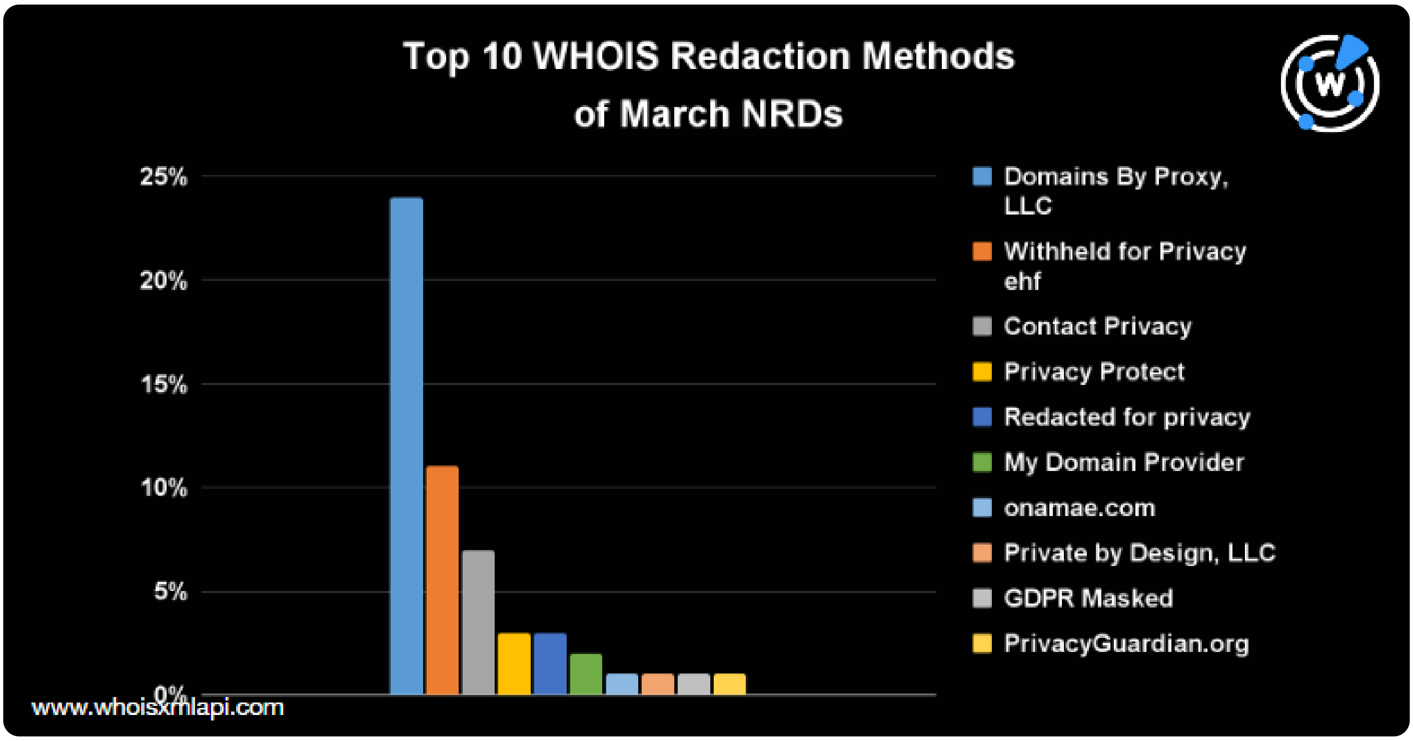
Contact us to get access to the full list.

WHOIS Data Redaction

Only 8% of the March NRDs had public registrant details, highlighting the massive implementation of WHOIS data redaction.



Based on the NRDs' registrant organizations, about 84% had redacted WHOIS records, with most employing the services of privacy protection companies. Analyzing the redaction methods, we found that the top WHOIS privacy protection providers were Domains By Proxy (24%); Withheld for Privacy EHF (11%); Contact Privacy, Inc. (7%); and Privacy Protect LLC (3%). The chart below shows the top 10 most common redaction providers.

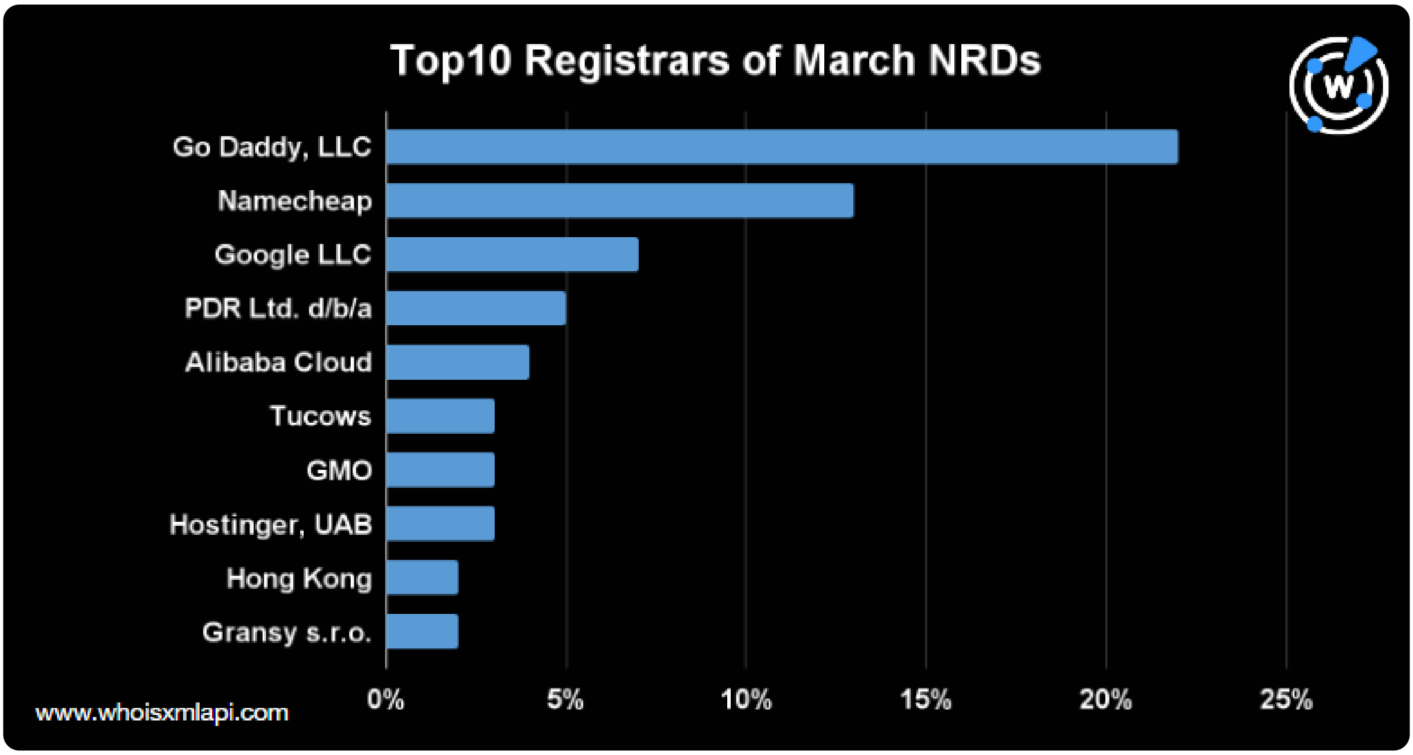


Top 10 WHOIS Redaction Methods of March NRDs

Registrar Distribution

As in January and February, GoDaddy dominated the list of top registrars, accounting for 22% of the total domain registration volume. Almost the same registrars completed the top 10, too. Namecheap took second place with a 13% share, followed by Google and PDR Ltd. with 7% and 5% shares, respectively.

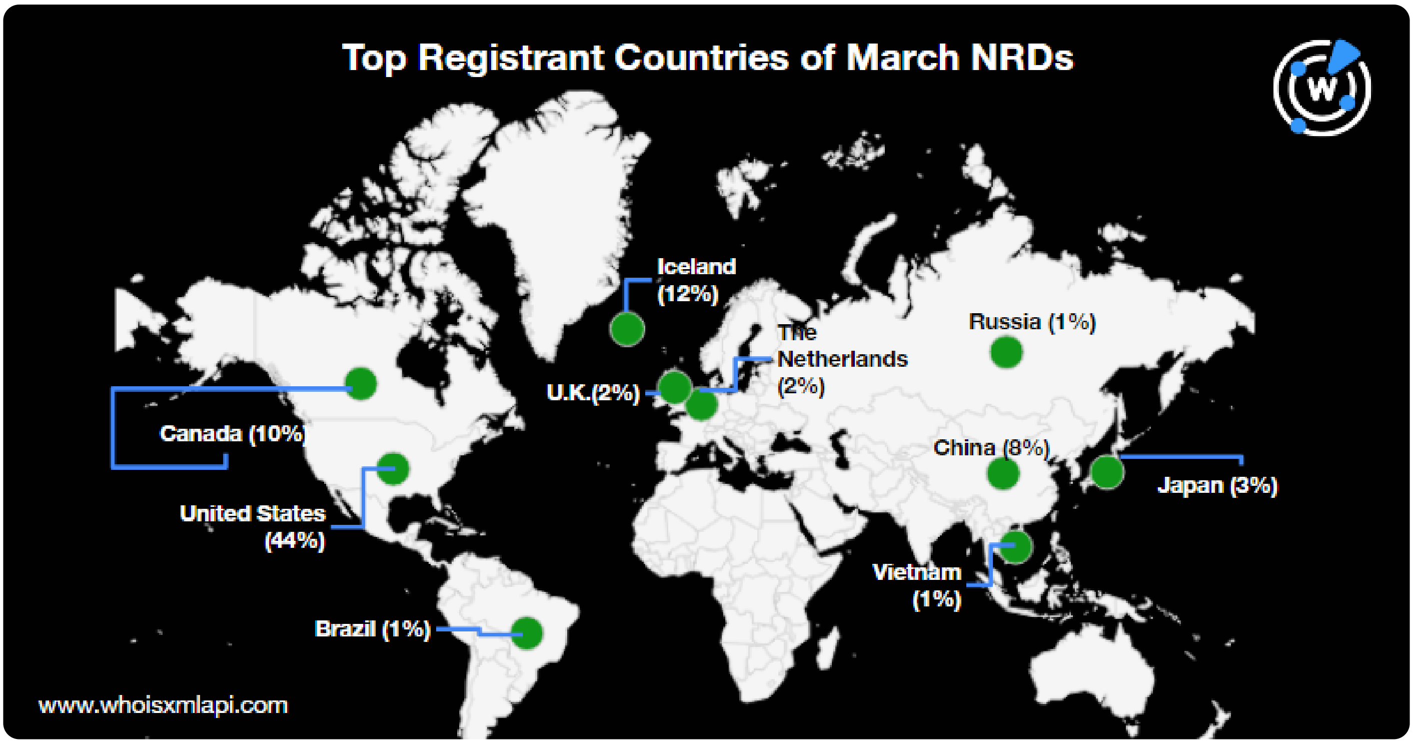
Rounding up the top 10 registrars were Alibaba (4%); Tucows (3%); GMO (3%); Hostinger (3%); Hong Kong Juming Network Technology Co., Ltd. (2%); and Gransy S.R.O. (2%). These are summed up in the following chart.



The top 10 registrars accounted for 63% of the total registration volume. The rest of the domains were distributed across more than 350 other registrars.

Top Registrant Countries

About 44% of the March 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 March were China, Japan, the Netherlands, the U.K., Russia, Brazil, and Vietnam.



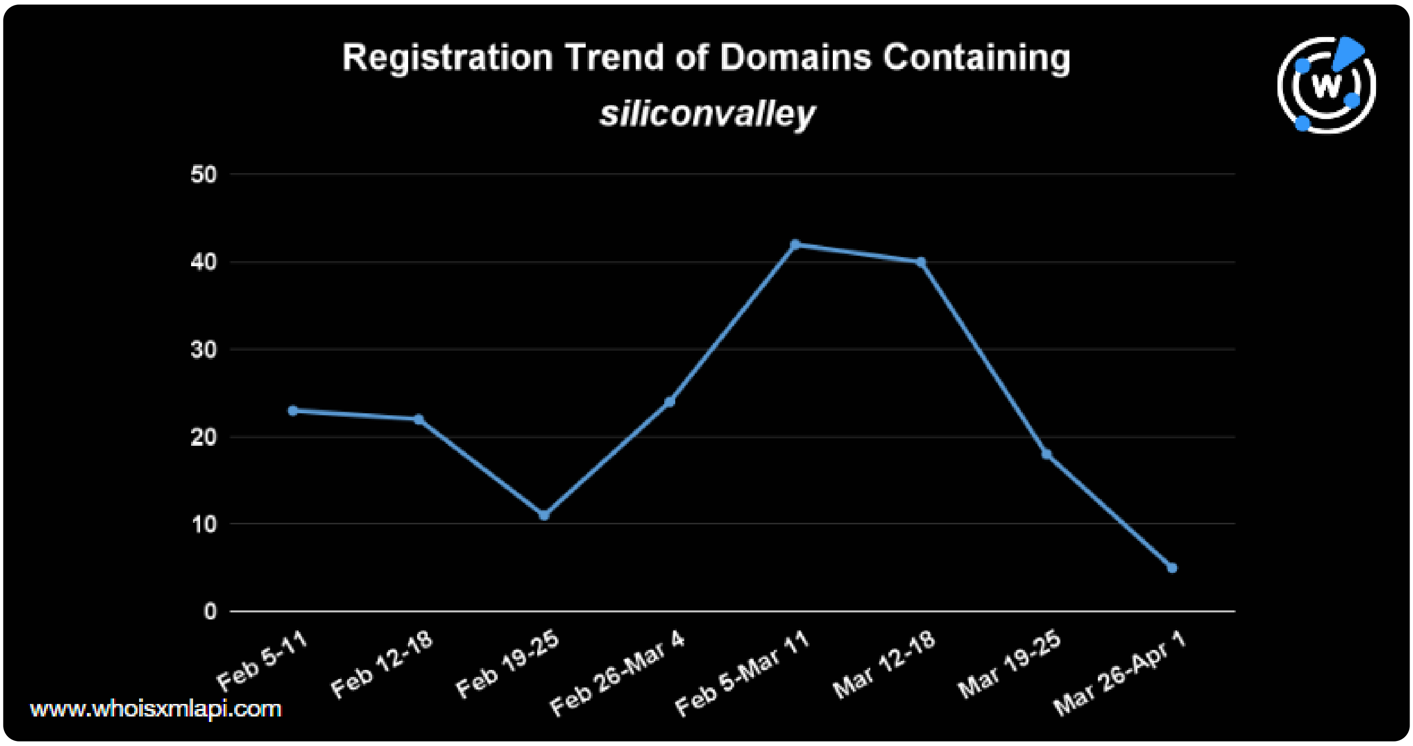
Appearance of Common Strings among the SLDs

Xn was still among the most-used text strings for months now, highlighting the continued popularity of internationalized domain names (IDNs). Also, adjacent generic terms, such as ***online***, ***home***, and ***service*** remained common among the NRDs.

Other repeated strings were tech terms, such as ***ai***, ***digital***, ***app***, and ***web***. The word cloud below shows these and other common strings.

In the News

Among March’s most significant events was the Silicon Valley Bank turmoil. How did the DNS reflect it? The chart below shows a snapshot. It specifically shows a spike in the registration of domains containing ***siliconvalley*** in the week of the bank’s slide. The volume dwindled toward the end of March.



Cybersecurity through the DNS Lens

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

- **Probing Lorec53 Phishing through the DNS Microscope:** WhoisXML API researchers expanded publicly available indicators of compromise (IoCs) believed to have been used by the Lorec53 APT Group in phishing and malware distribution campaigns, leading to the discovery of 1,800+ additional artifacts.

- **Is Your Intranet Vulnerable to Attacks? Investigating Intranet Impersonation in the DNS :** Following a recent Reddit security incident where attackers mimicked the platform's intranet gateway, we studied intranet impersonation in the DNS and uncovered hundreds of recently added cybersquatting domains targeting popular intranet providers.

- **Shining the WHOIS and DNS Spotlight on International Fraud:** Our IoC expansion analysis of email addresses used in online scams led us to 3,000+ connected domains.

- **Beyond Healthcare IoCs: Threat Expansion and EHR Impersonation Detection:** We looked into one of the threats targeting healthcare organizations. Our investigation into Cuba ransomware IoCs uncovered thousands of artifacts and cybersquatting domains targeting popular EHR software providers.

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.