August 2023: Domain Activity Highlights

Posted on September 12, 2023

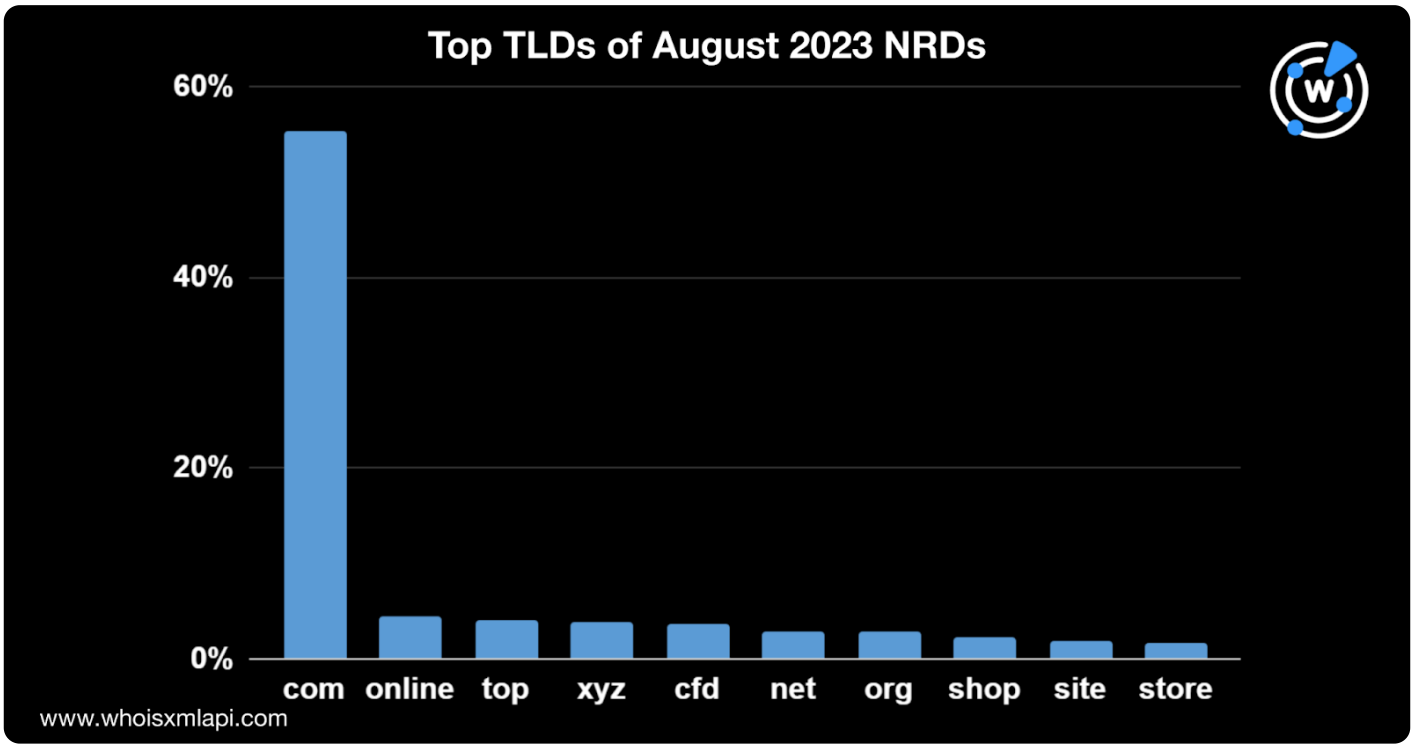
Of the millions of domains registered on 1–31 August 2023, the WhoisXML API researchers studied a randomized sample of 31,000 to determine commonalities in their WHOIS data, registrant country, registrar, and TLD.

In addition, we examined the domains' text string usage to uncover potentially emerging trends. We also tapped into our predictive intelligence sources to determine some of August's most imitated brands or text strings. This study's findings in addition to links to threat reports developed using DNS, IP, and domain intelligence sources are summarized below.

Zooming in on the August NRDs

TLD Distribution

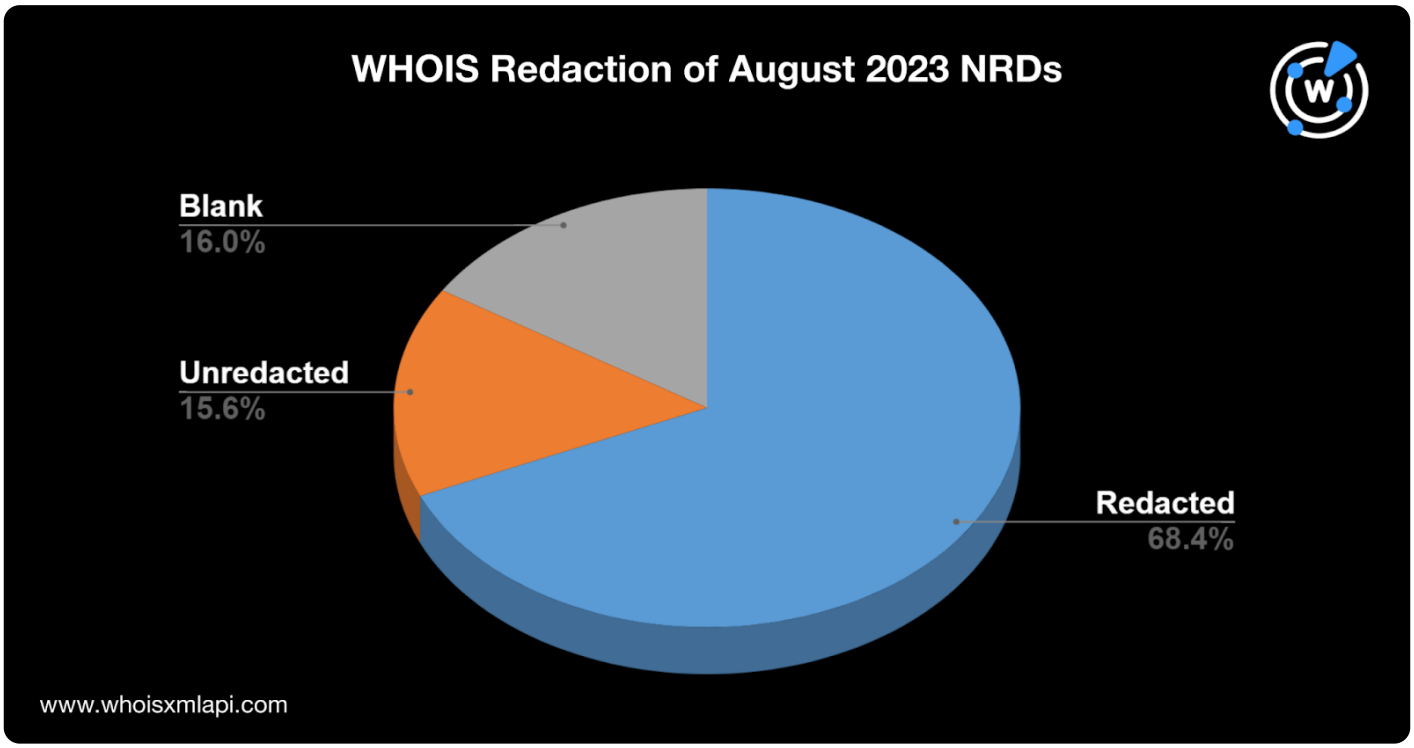
Most of the top 10 TLD extensions in the past months continued to be so in August 2023. The .com TLD remained the most used, accounting for 55% of the total domain registration volume. The rest of the top 10 TLD extensions were .online with a 5% share; .top, .xyz, and .cfd with 4% each; .net, and .org with 3% each; and .shop, .site, and .store with 2% each. These are shown in the chart below.



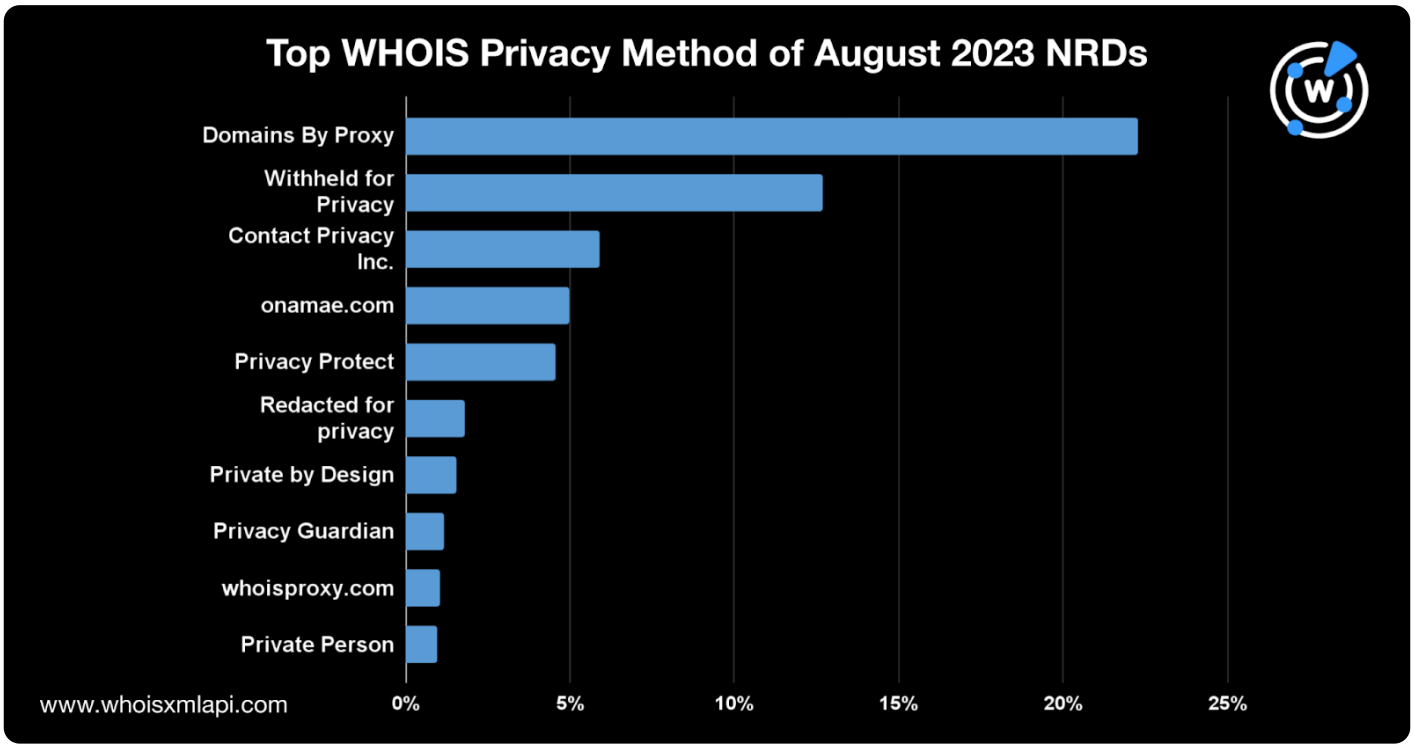
The top 10 TLD extensions accounted for 83% of the new domain registration volume, while the rest were distributed across more than 620 other TLDs.

WHOIS Data Redaction

A majority of the new domains had redacted WHOIS records, with only 15.6% that made their registrant organization public, while 16% left this field blank.



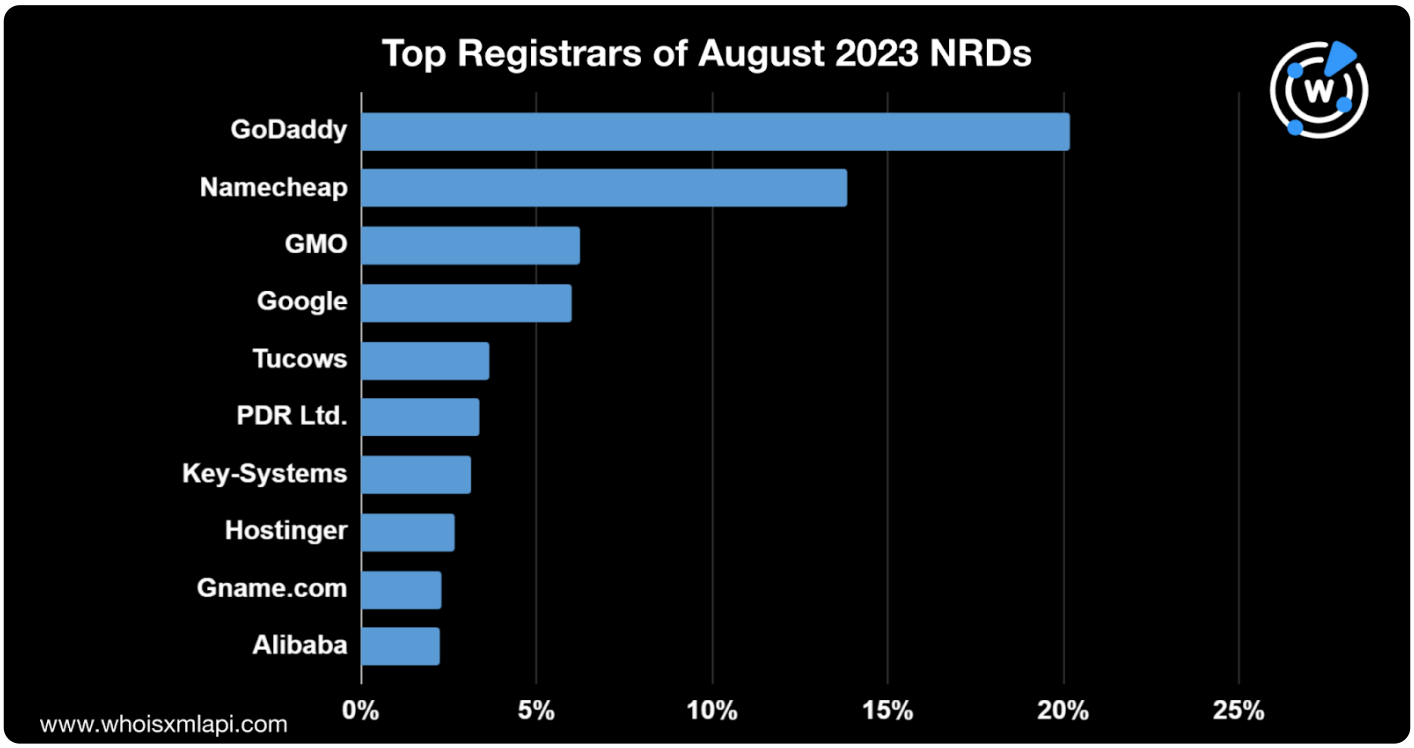
Domains By Proxy remained the most popular privacy redaction service provider for our sample, accounting for 22% of the new domain registration volume. It was followed by Withheld for Privacy (13%), Contact Privacy (6%), Onamae (5%), Privacy Protect LLC (5%), Private by Design (2%), PrivacyGuardian.org (1%), and Whoisproxy (1%).



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

Registrar Distribution

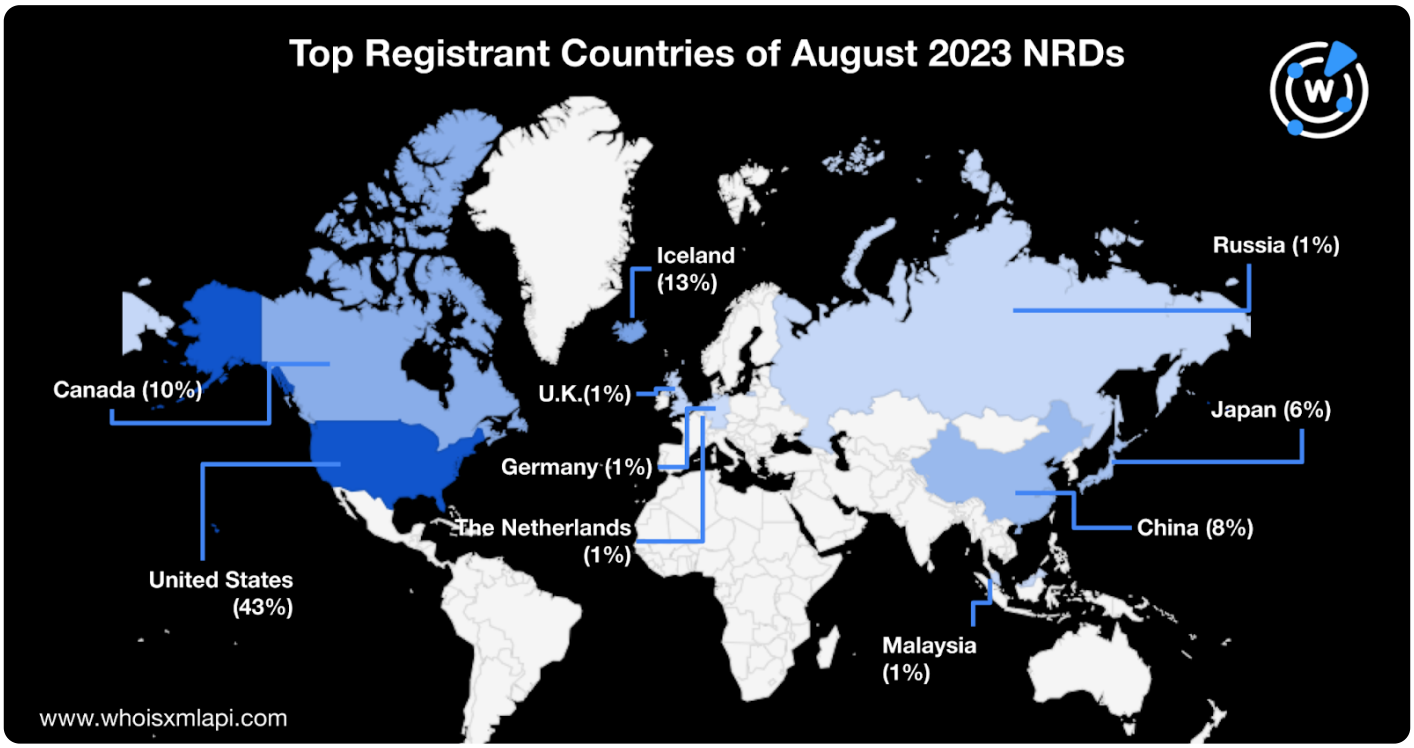
GoDaddy remained the leading registrar for our sample, accounting for 20% of the total domain registration volume. Namecheap followed with a 14% share; Google and GMO Internet Group with 6% each; Tucows with 4%; PDR Ltd., Key-Systems, and Hostinger with 3% each; and Gname and Alibaba with 2% each.



The top 10 registrars accounted for 64% of the total registration volume. The rest of the domains were distributed across more than 400 other registrars.

Top Registrant Countries

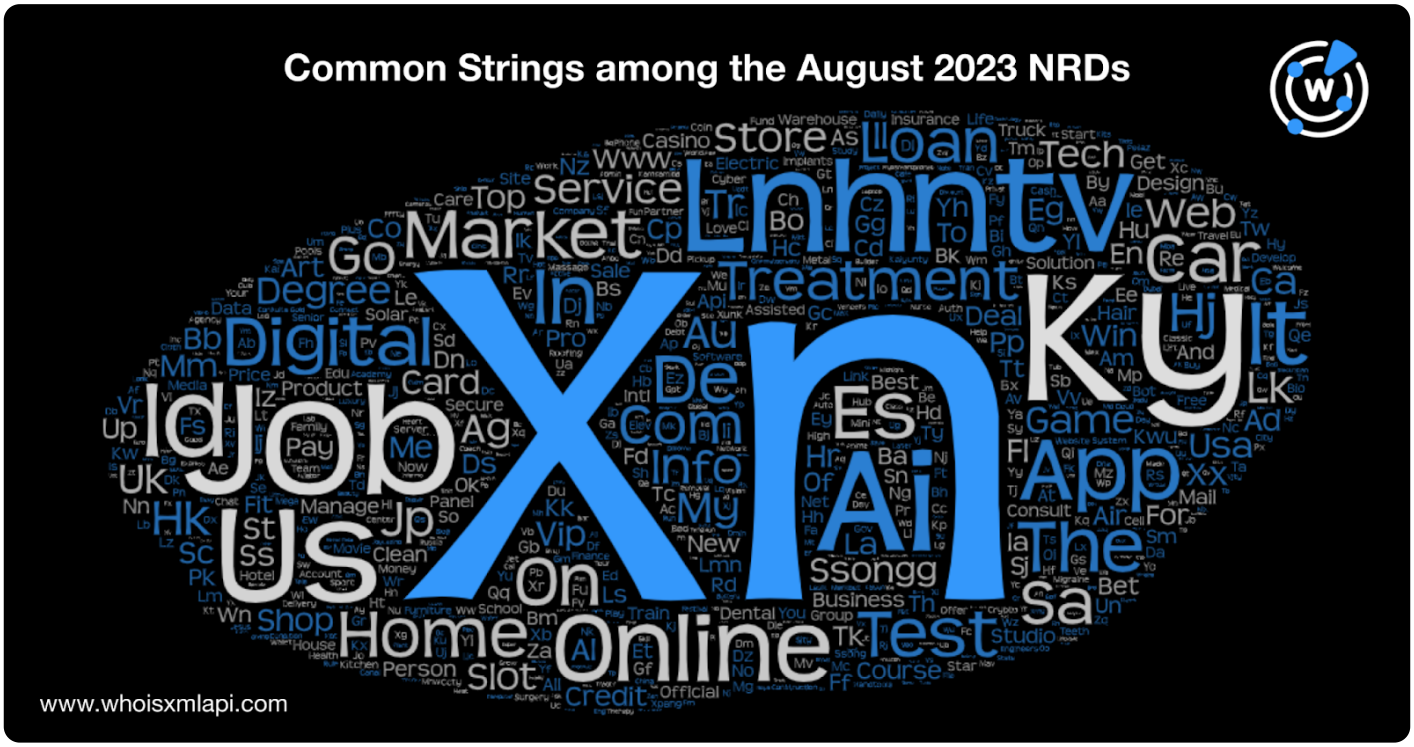
Data shows that the U.S. remained the leading specified registrant country for new domain registrations, accounting for 43% of the NRDs in August. Iceland and Canada followed with 13% and 10% shares, respectively. The rest of the top 10 registrant countries were China (8%), Japan (6%), the U.K. (2%), Russia (1%), Malaysia (1%), the Netherlands (1%), and Germany (1%).



The top 10 registrant countries accounted for 87% of the total registration volume. The rest of the domains were distributed across more than 130 other countries.

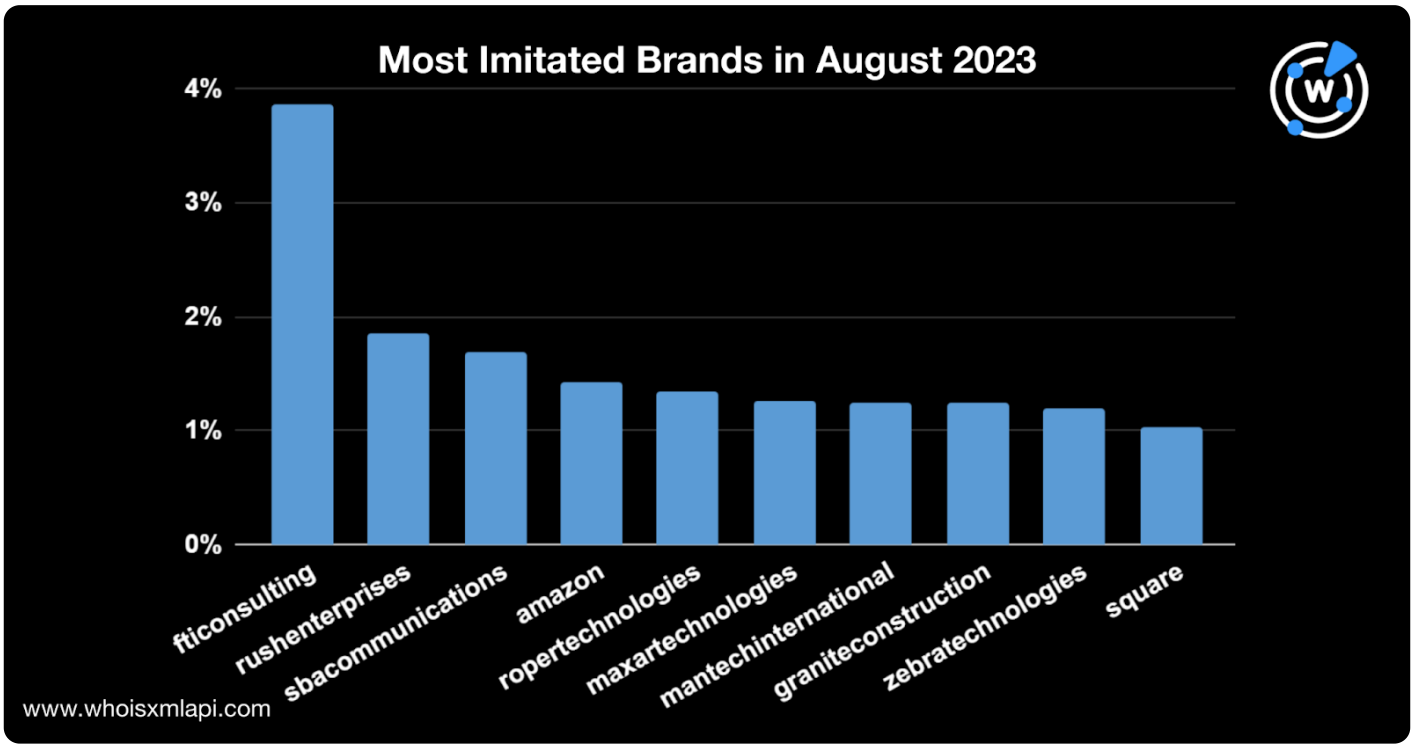
Appearance of Common Strings among the SLDs

Internet- and tech-related terms were among the most common strings found for the sample of August NRDs. Examples include **app**, **online**, **service**, and **digital**. The appearance of the words **loan**, **job**, and **home** is also noteworthy. In addition, **xn** remained very popular, hinting at the continuous usage of internationalized domain names (IDNs).



Early Warning Phishing Detection

Furthermore, we analyzed a sample of several thousand domains from the Early Warning Phishing Feed to determine some of the most imitated brands. Of the 495 search strings the data feed looked up, **fticonsulting** appeared in the most number of NRDs, accounting for 4% of the total early warning phishing domains. The strings **rushenterprises** and **sbacommunications** followed, with 2% each, while **amazon**, **ropertechnologies**, **maxartechnologies**, **mantechinternational**, **graniteconstruction**, **zebratechnologies**, and **square** each accounted for 1% of the early warning phishing domains.



Cybersecurity through the DNS Lens

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

- **Will Redis Remain on Threat Actors' Radar?:** WhoisXML API researchers investigated indicators of compromise (IoCs) related to CVE-2022-0543 or the Redis Lua Sandbox Escape and Remote Code Execution Vulnerability, which led to the discovery of more than 20,000 web properties containing the string **redis**.
- **Finding WyrmSpy and DragonEgg Ties to APT41 in the DNS:** WhoisXML API sought to determine ties between APT41 and WyrmSpy and DragonEgg by examining publicly available IoCs.
- **DNS Insights behind the JumpCloud Supply Chain Attack:** Our researchers took a closer look at the JumpCloud supply chain attack IoCs via a DNS deep dive, which led to the discovery of hundreds of potentially connected artifacts.

- **AI Tool Popularity: An Opportunity for Launching Malicious Campaigns?:** WhoisXML API and Bayse Intelligence teamed up to identify web properties that attackers could use to target eight of 2023's best AI productivity tools.

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.