September 2023: Domain Activity Highlights

Posted on October 10, 2023

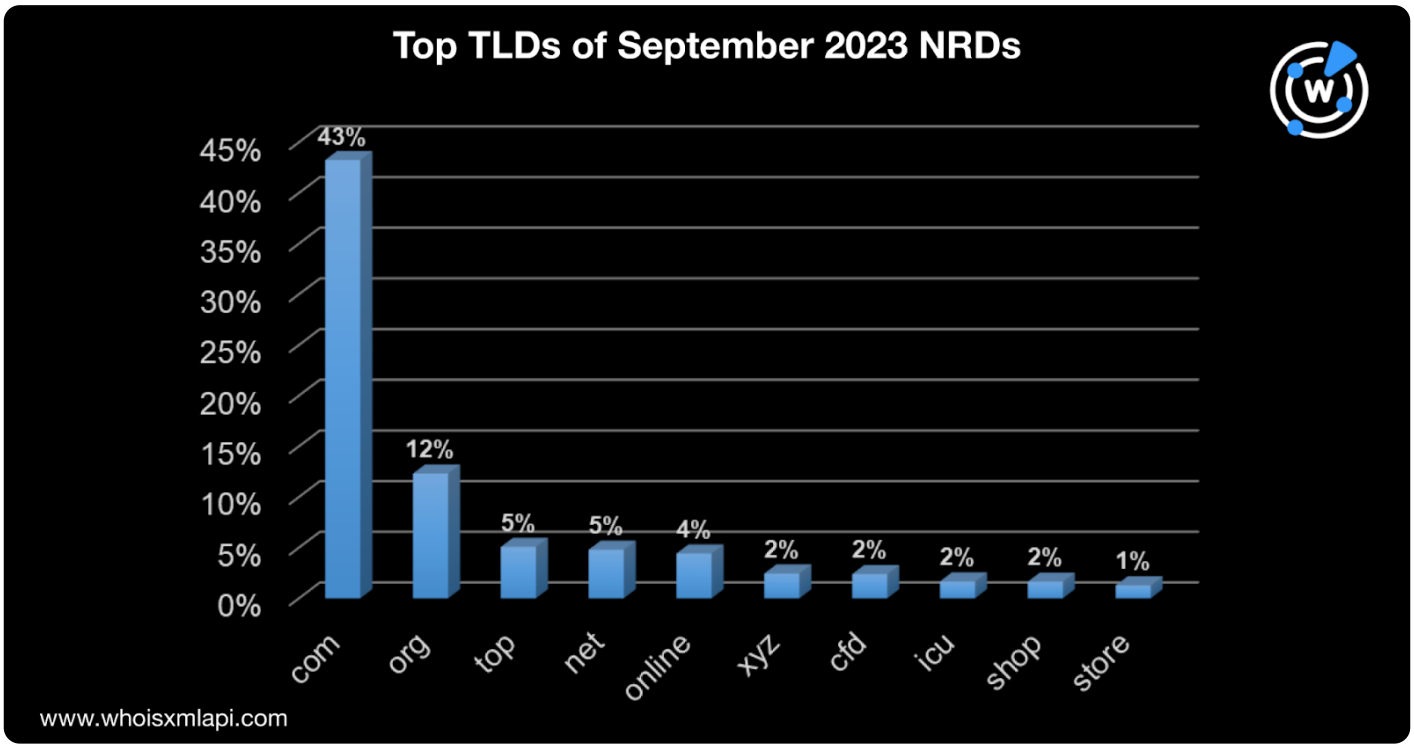
WhoisXML API researchers studied a randomized sample of 30,000 domains out of the millions registered on 1–30 September 2023. We determined commonalities in their WHOIS data, registrant country, registrar, and TLD.

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 the month's most imitated brands based on text string usage. This study's findings and links to threat reports developed using DNS, IP, and domain intelligence sources are summarized below.

Zooming in on the September NRDs

TLD Distribution

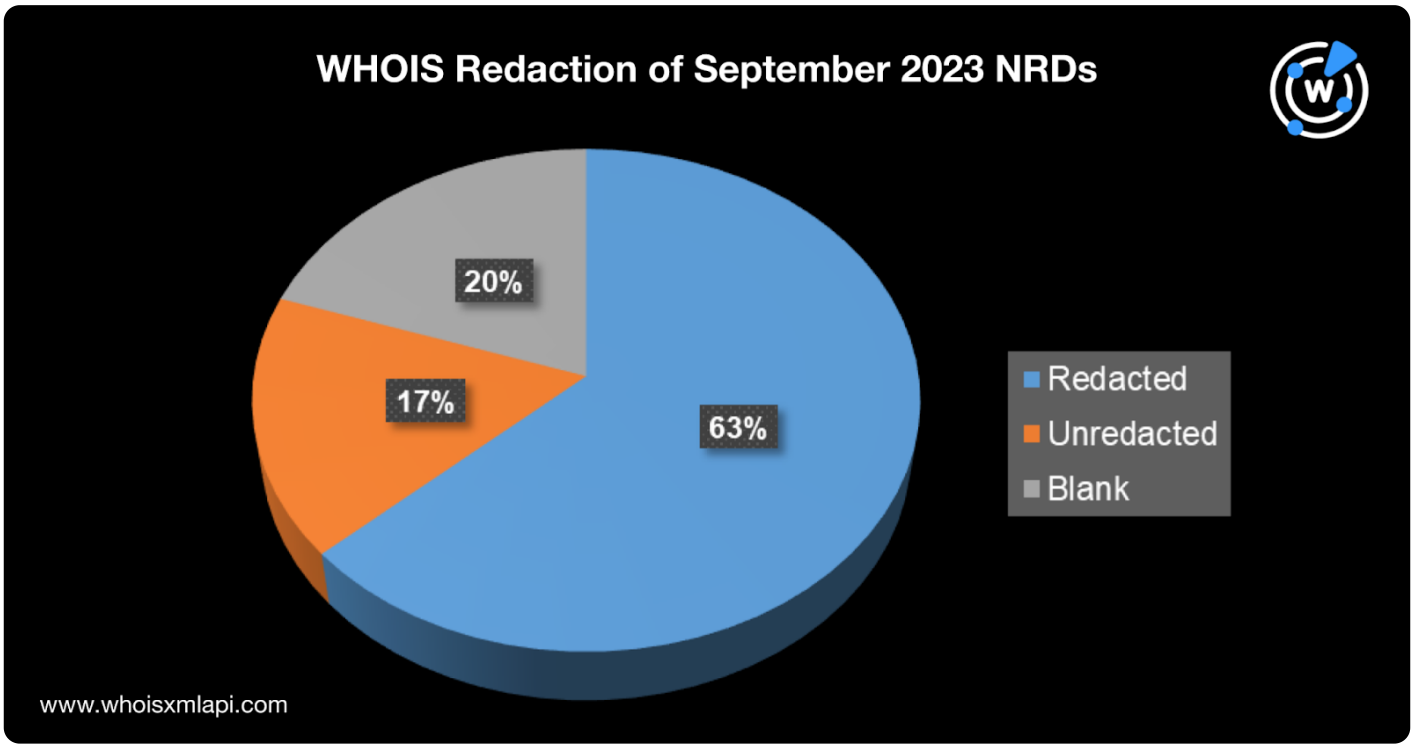
The top 10 TLD extensions in September 2023 remained essentially unchanged from previous months, with .com remaining the most popular, accounting for 43% of the total domain registration volume. The TLDs that rounded up the top 3 were .org (12%), .top and .net (5% each), and .online (4%). They were followed by .xyz, .cfd, .icu, and .shop (2% each) and .store (1%).



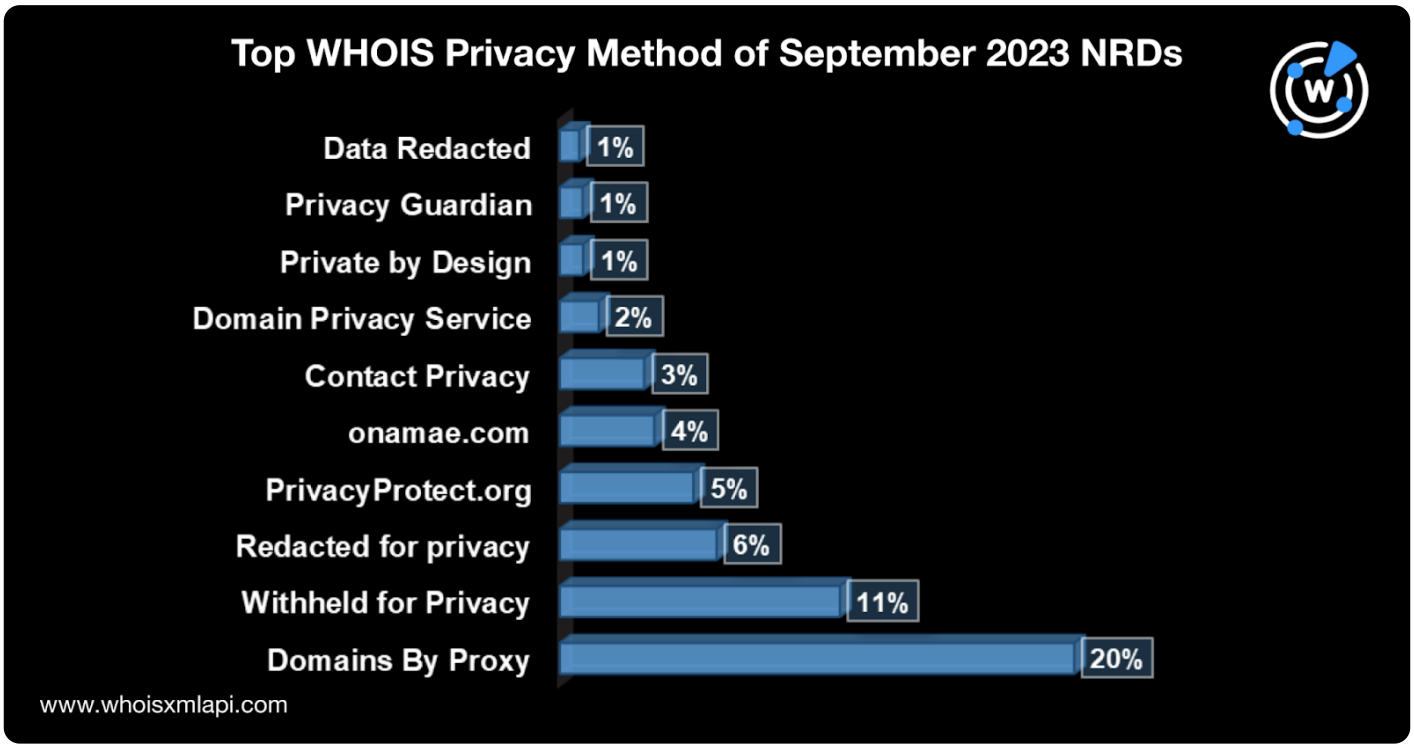
The top 10 TLD extensions accounted for 79% of the total new domain registration volume, while the rest were distributed across more than 630 other TLDs.

WHOIS Data Redaction

About 63% of the new domains had redacted WHOIS records. Only 17% made their registrant organizations public, while around 20% left the field blank.



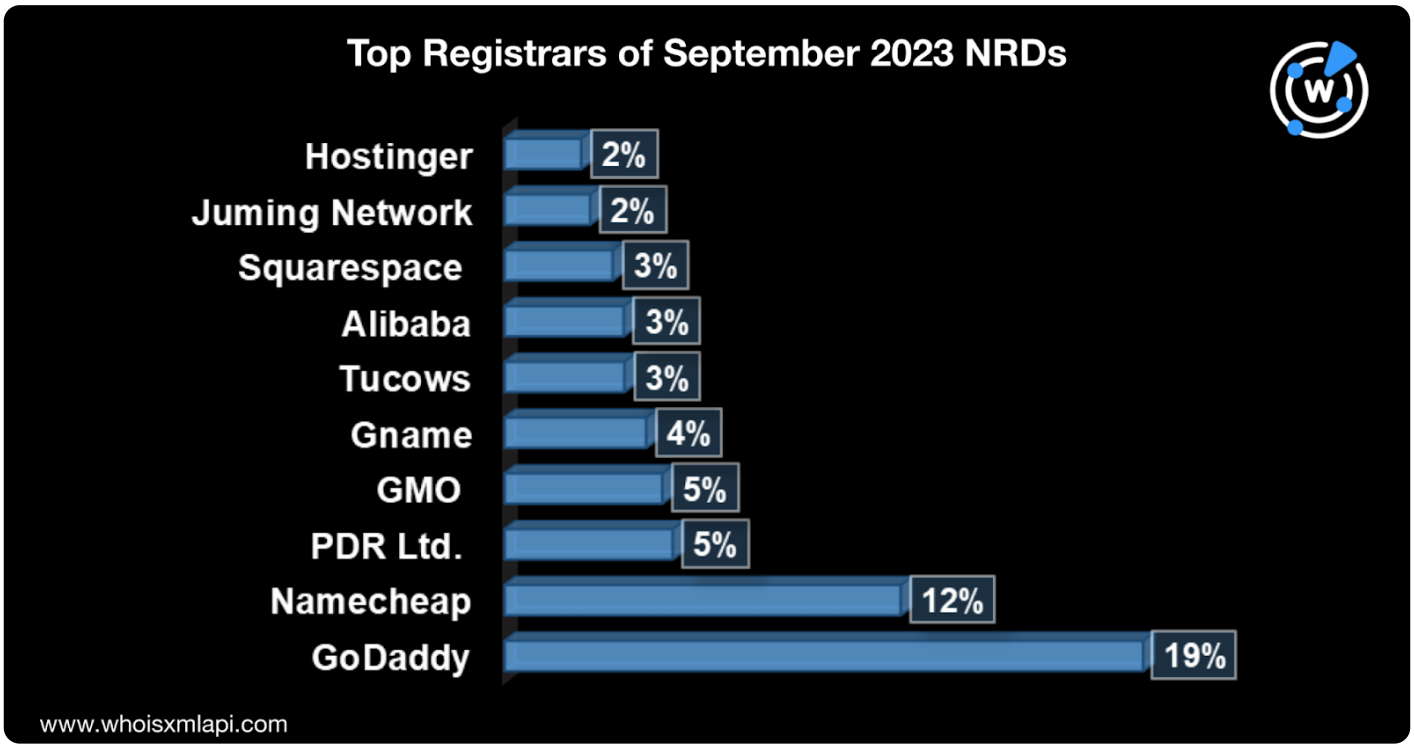
Domains By Proxy was the most popular privacy redaction service provider, accounting for 20% of the new domain registrations. It was followed by Withheld for Privacy (11%), Privacy Protect (5%), Onamae (4%), Contact Privacy (3%), Domain Privacy Service (2%), Private by Design (1%), and Privacy Guardian (1%).



Several NRDs' registrant organization fields also contained labels like **Redacted for privacy** and **Data Redacted**.

Registrar Distribution

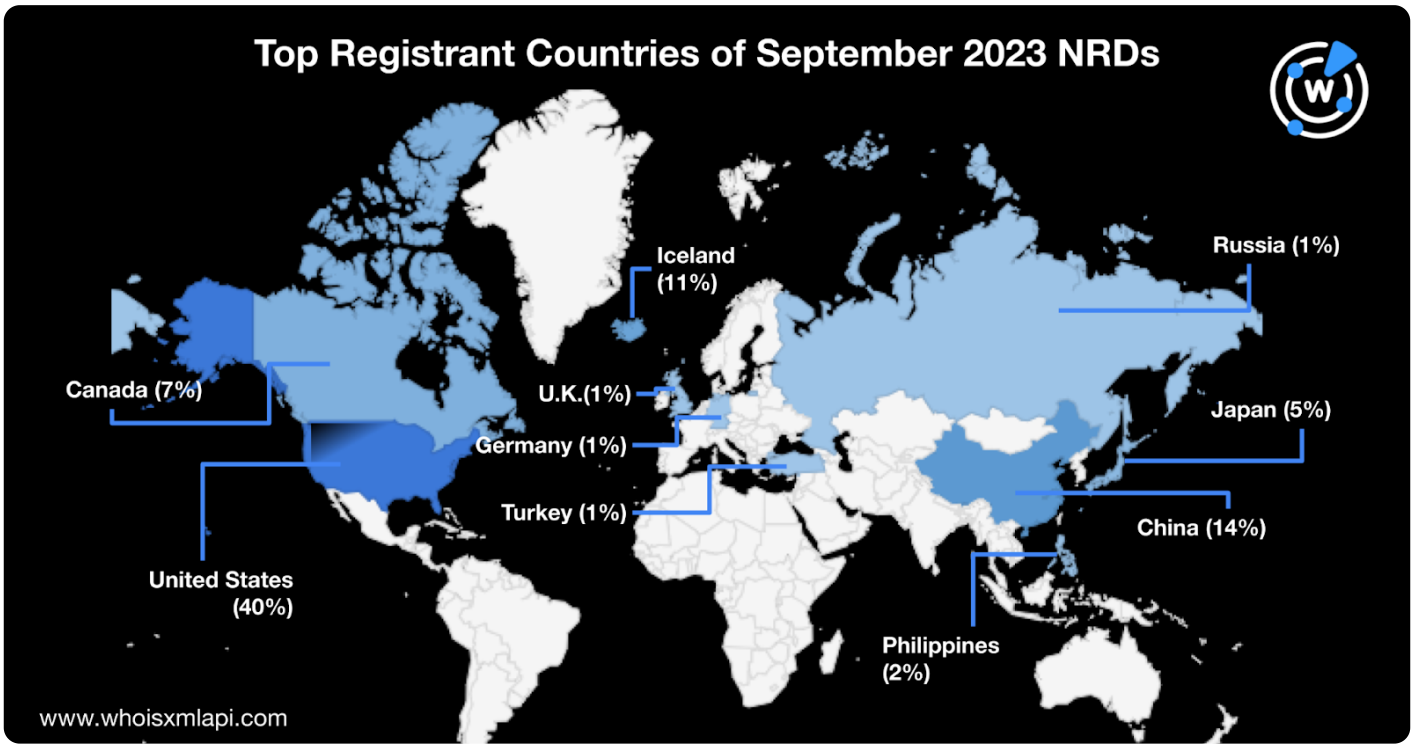
Data shows that GoDaddy remained the top domain registrar, accounting for 19% of the new domain registrations. Namecheap followed close behind with a 12% share. PDR Ltd. and GMO Internet had 5% shares each. Gname had 4%, while Tucows, Alibaba, and Squarespace each had 3%. Juming Network and Hostinger rounded out the top 10 with 2% shares each.



The top 10 registrars accounted for 58% of the total registration volume. The rest of the domains were distributed across more than 580 other registrars.

Top Registrant Countries

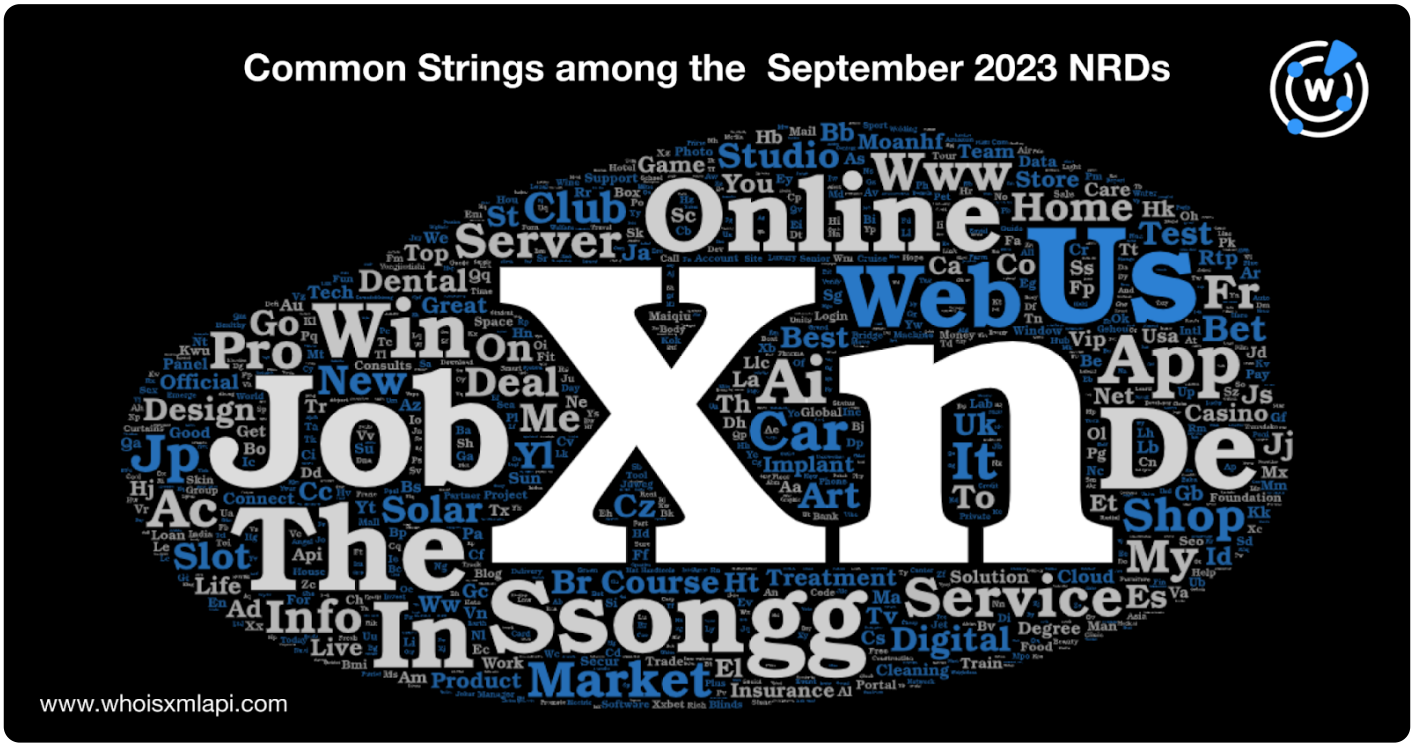
The U.S. remained the top registrant country with a 40% share. China and Iceland were distant runners-up, with 14% and 11% shares, respectively. They were followed by Canada (7%), Japan (5%), and the Philippines (2%). Russia, the U.K., Germany, and Turkey rounded out the top 10, each with a 1% or less share.



The top 10 registrant countries accounted for 83% of the total registration volume. The rest of the domains were distributed across more than 115 other countries.

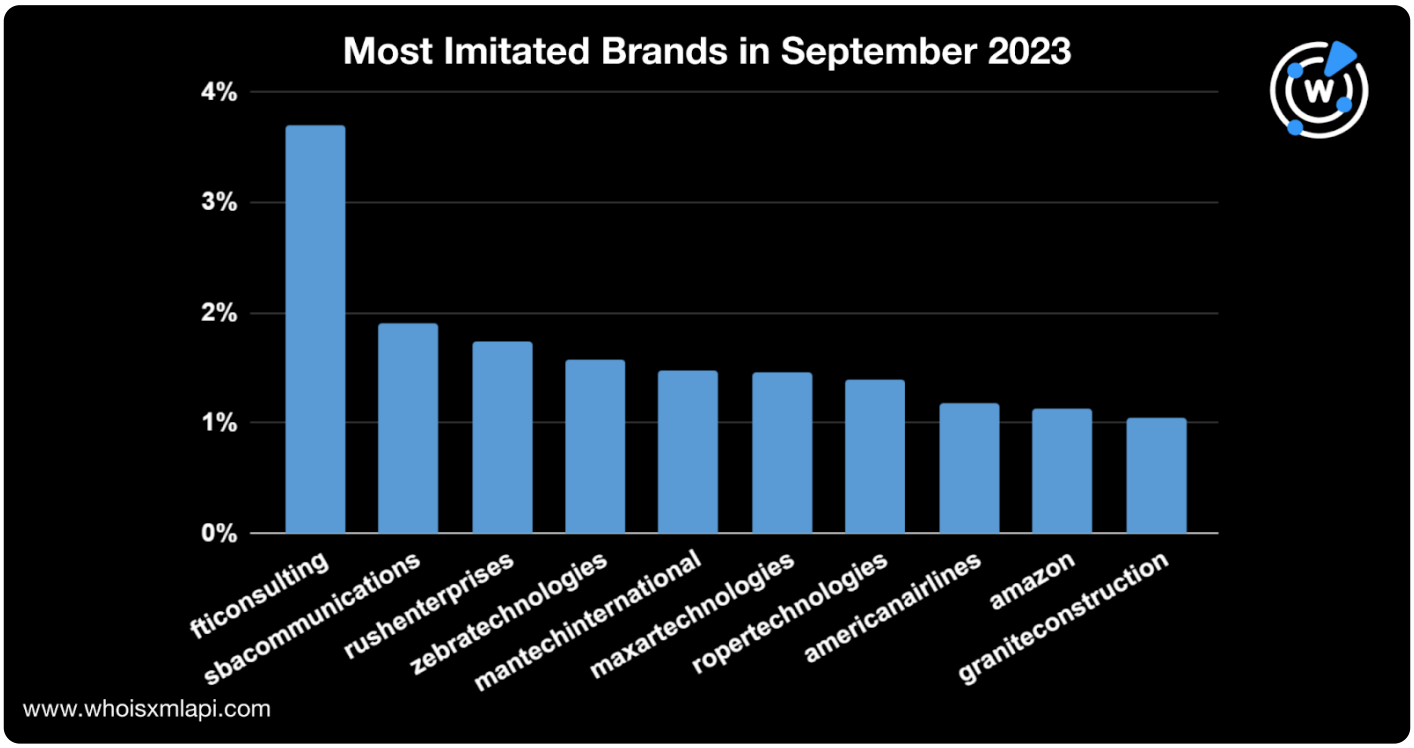
Appearance of Common Strings among the SLDs

Internet- and tech-related terms were the most commonly seen strings among the September NRDs, including **web**, **online**, **www**, **app**, and **service**. The words **market**, **job**, and **home** were also commonly used. Finally, the popularity of **xn** suggests that internationalized domain names (IDNs) remained popular.



Early Warning Phishing Detection

Our recent analysis of a sample of the Early Warning Phishing Feed comprising thousands of domains revealed that the most frequently appearing string was **fticonsulting**, which appeared in almost 4% of the suspicious domains. Other popular strings were **sbacommunications**, **rushenterprises**, **zebratechnologies**, **nantechinternational**, **maxartechnologies**, **ropertechnologies**, **americanairlines**, **amazon**, and **graniteconstruction**.



Cybersecurity through the DNS Lens

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

- **Decoy Dog, Too Sly to Leave DNS Traces?:** WhoisXML API researchers investigated indicators of compromise (IoCs) related to Decoy Dog, which led to the discovery of thousands of artifacts comprising 90 IP- and 2,000+ string-connected domains.
- **Examining WoofLocker under the DNS Lens:** Our researchers dove into the DNS to analyze hundreds of IoCs reported over the course of WoofLocker's eight years of operation. This exercise found 1,000+ unpublished domains that shared some of the IoCs' dedicated IP hosts and more artifacts.
- **Thawing IcedID Out through a DNS Analysis:** WhoisXML API researchers uncovered more than 70 connected artifacts, including email addresses and domains potentially linked to IcedID malware.

- **Searching for Smishing Triad DNS Traces:** We identified more than 2,500 domains potentially associated with Smishing Triad's latest campaign. Of these domains, more than 600 have already been flagged as malicious.

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.