October 2023: Domain Activity Highlights

Posted on November 6, 2023

WhoisXML API researchers analyzed a random sample of 31,000 domains out of the millions registered in October 2023. We identified commonalities in their WHOIS data, registrant countries, registrars, and top-level domain (TLD) extensions.

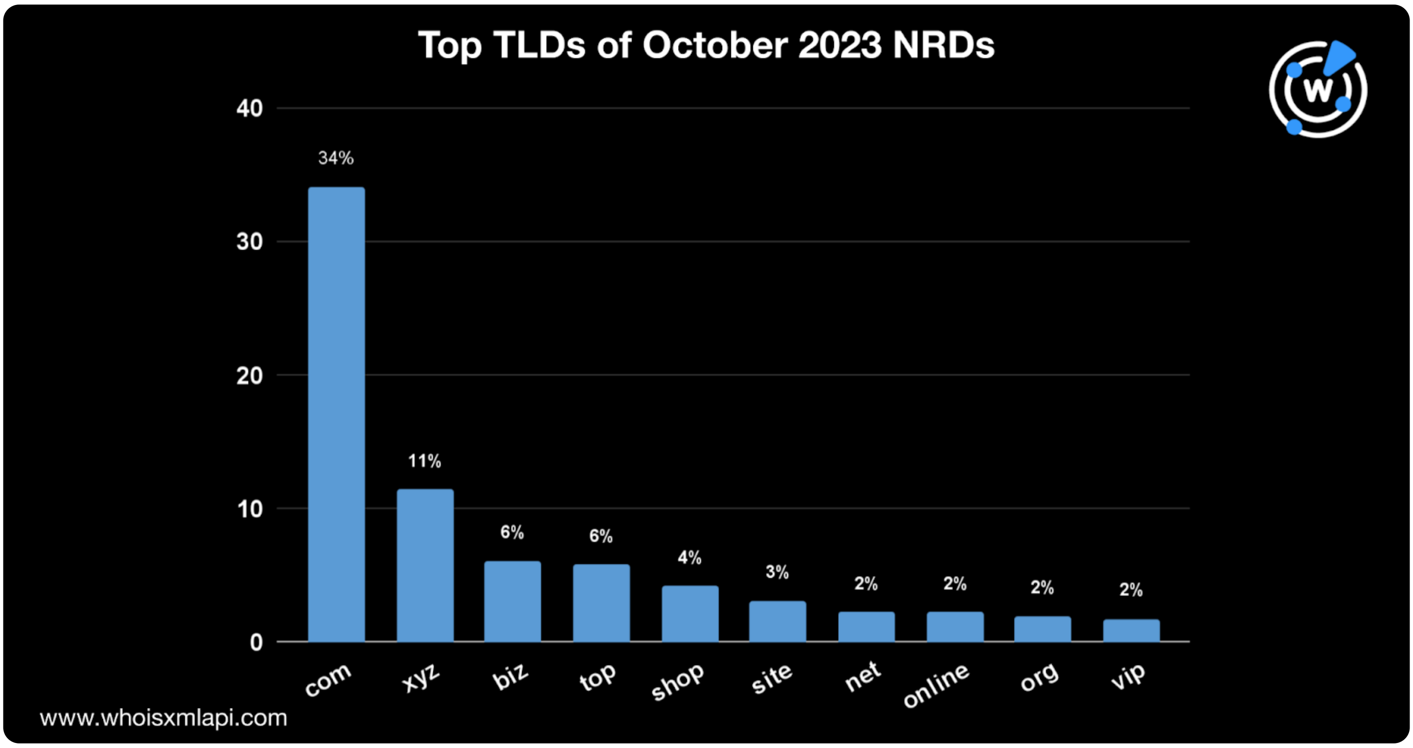
In addition, we examined the domains' text string usage to discover potential emerging trends. We also used our predictive intelligence sources to identify some of the most imitated brands during the month based on text string usage. The findings of this study and links to threat reports developed using DNS, IP, and domain intelligence sources are summarized below.

Zooming in on the October NRDs

TLD Distribution

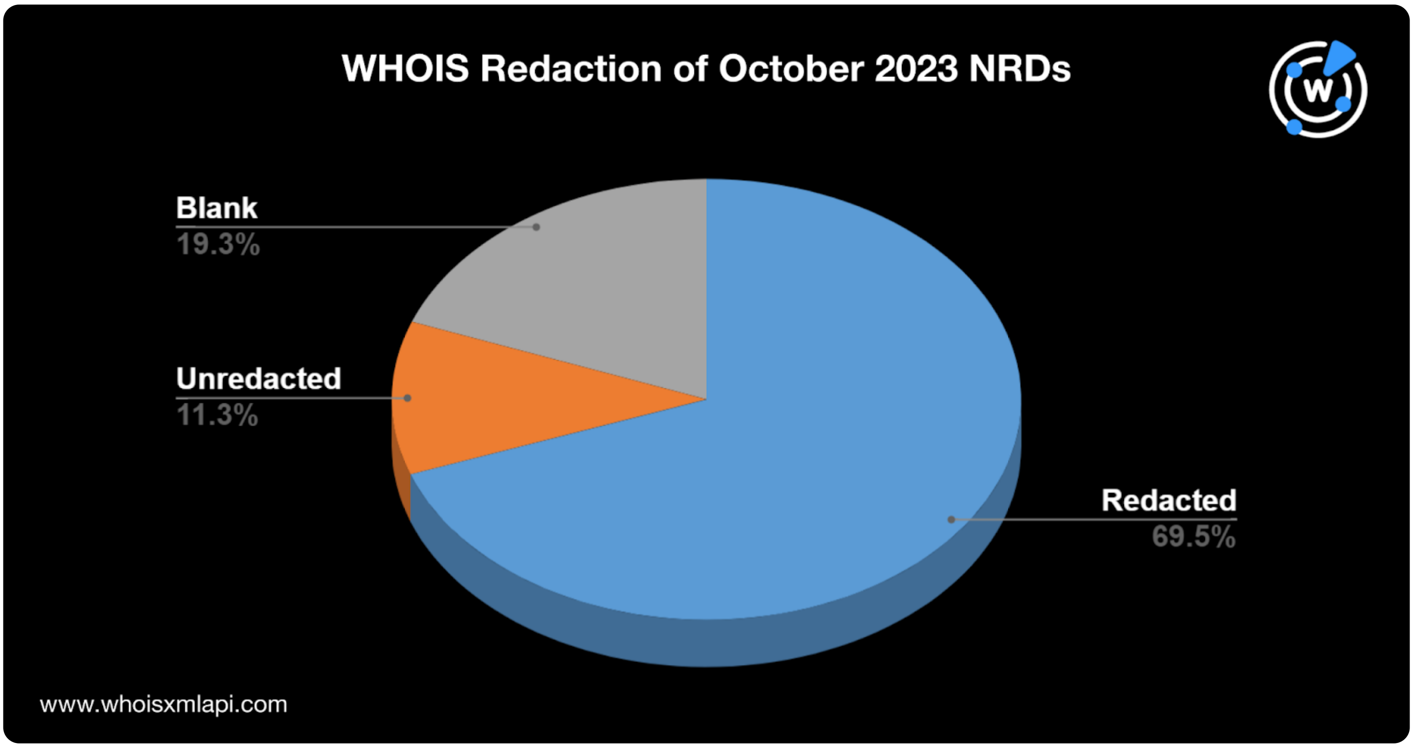
The most popular TLDs in October 2023 remained largely unchanged from the previous months, with .com still the most widely used, accounting for 34% of all the domain registrations. .xyz (11%), .biz (6%), .top (6%), .shop (4%), .site (3%), .net (2%), .online (2%), .org (2%), and .vip (2%) rounded out the top 10.

The top 10 TLDs accounted for 73% of all the new domain registrations, with the remaining 27% distributed across more than 630 other TLDs.

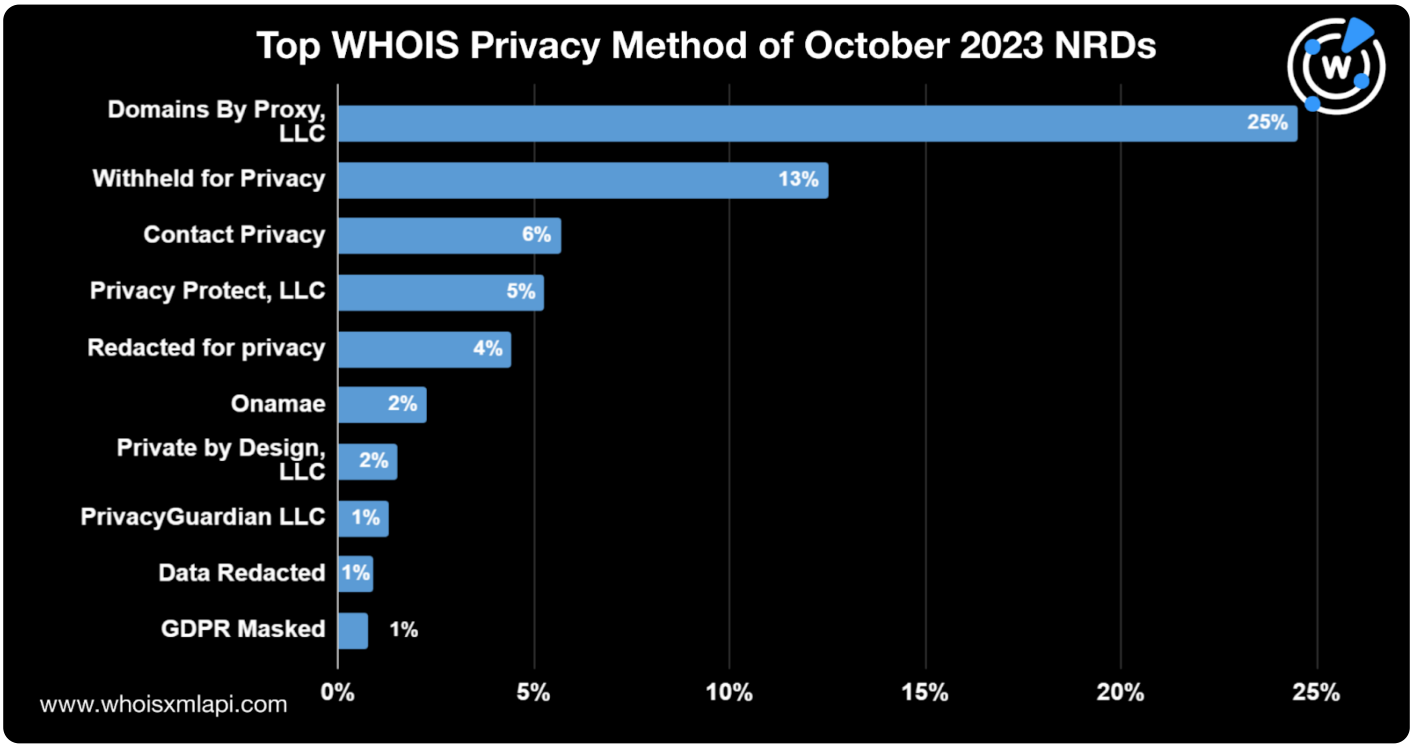


WHOIS Data Redaction

Approximately 70% of the NRDs had redacted WHOIS records, which means their registrants' identities were hidden. Only around 11% of the new domains made their registrant information public, while the remaining 19% had blank fields.



The most popular privacy redaction service provider was Domains By Proxy, which accounted for a quarter of the new domain registrations. The other popular providers included Withheld for Privacy (13%), Contact Privacy (6%), Privacy Protect (5%), Onamae (2%), Private by Design (2%), and Privacy Guardian (1%).

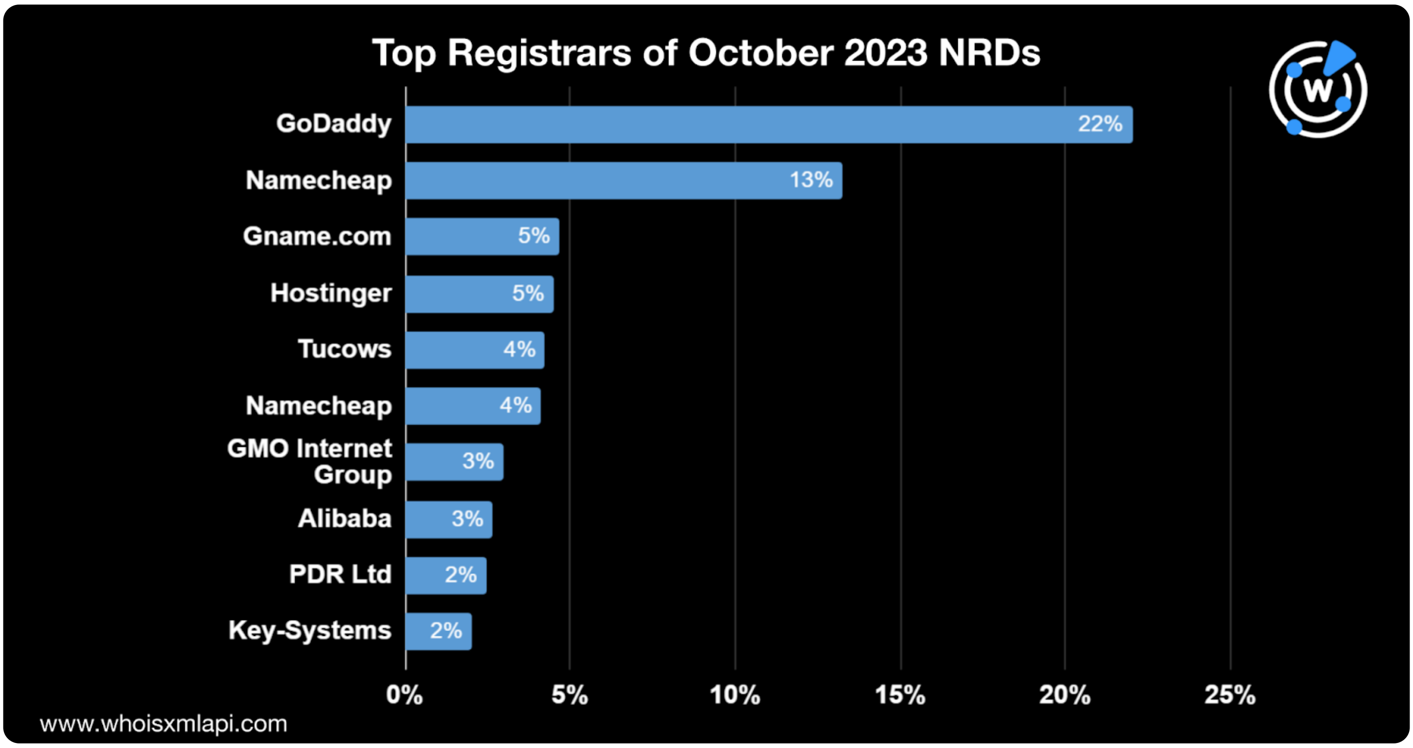


Several registrants labeled their registrant organization fields with strings like **Redacted for privacy**, **Data Redacted**, and **GDPR Masked**.

Registrar Distribution

GoDaddy was the most popular domain registrar, with a 22% share. Namecheap came in second with a 13% share. Gname and Hostinger followed with a 5% share each.

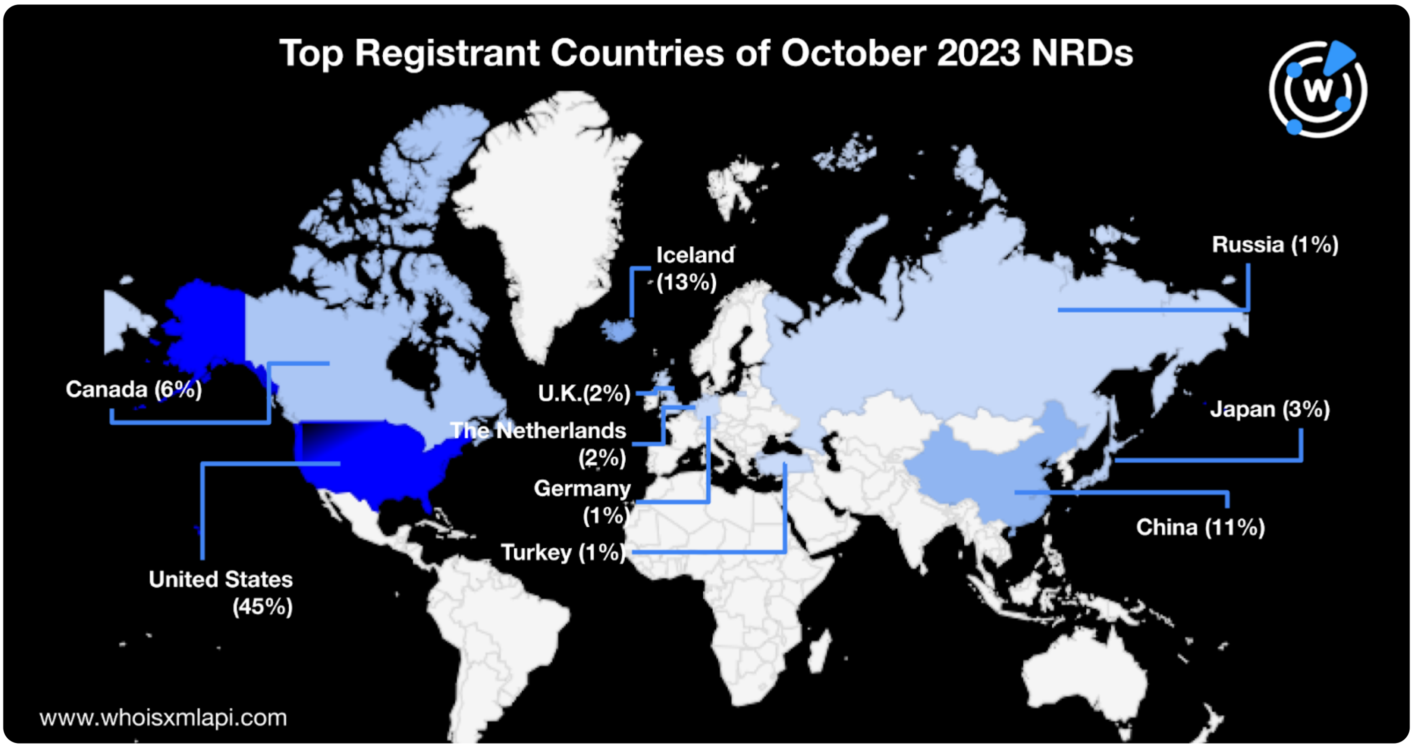
The rest of the top 10 registrars included Tucows and Namecheap with 4% of the NRDs each, GMO Internet Group and Alibaba with a 3% share each, and PDR Ltd. and Key-Systems with a 2% share each.



The top 10 domain registrars controlled 63% of the new domain registrations. The remaining 37% of the NRDs was divided among more than 350 other registrars.

Top Registrant Countries

The U.S. accounted for the largest number of domain registrations, with a 45% share. Iceland and China were the second and third top registrant countries, with 13% and 11% shares, respectively. Canada (6%), Japan (3%), the U.K. (2%), the Netherlands (2%), Russia (1%), Turkey (1%), and Germany (1%) rounded out the top 10 registrant countries for October.

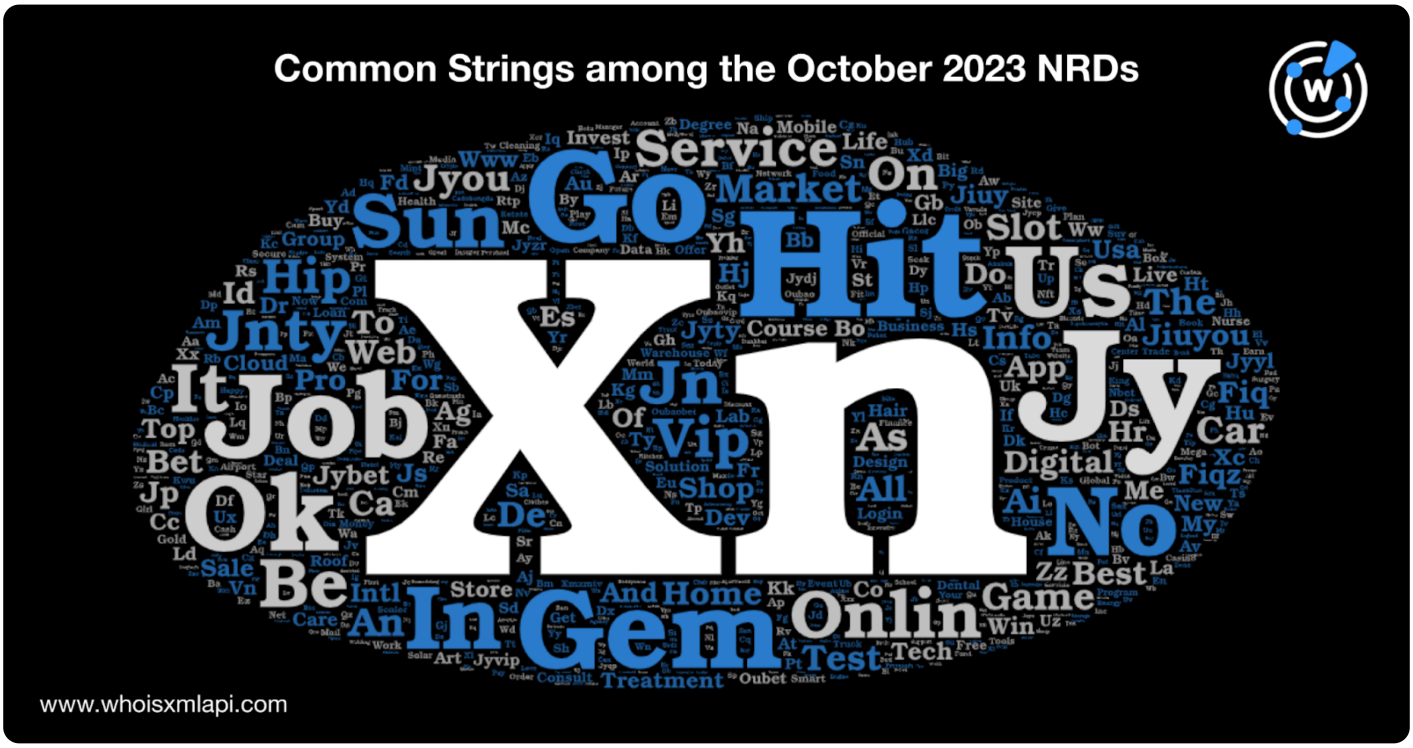


The top 10 registrant countries accounted for a massive 85% of all the domain registrations. The remaining 15% were distributed among more than 130 other countries.

Appearance of Common Strings among the SLDs

Some of the most commonly seen strings among the October NRDs were Internet-related, such as **service**, **online**, **test**, and **shop**. The repeated appearances of **go**, **hit**, **job**, **market**, **gem**, and **game** were also noteworthy.

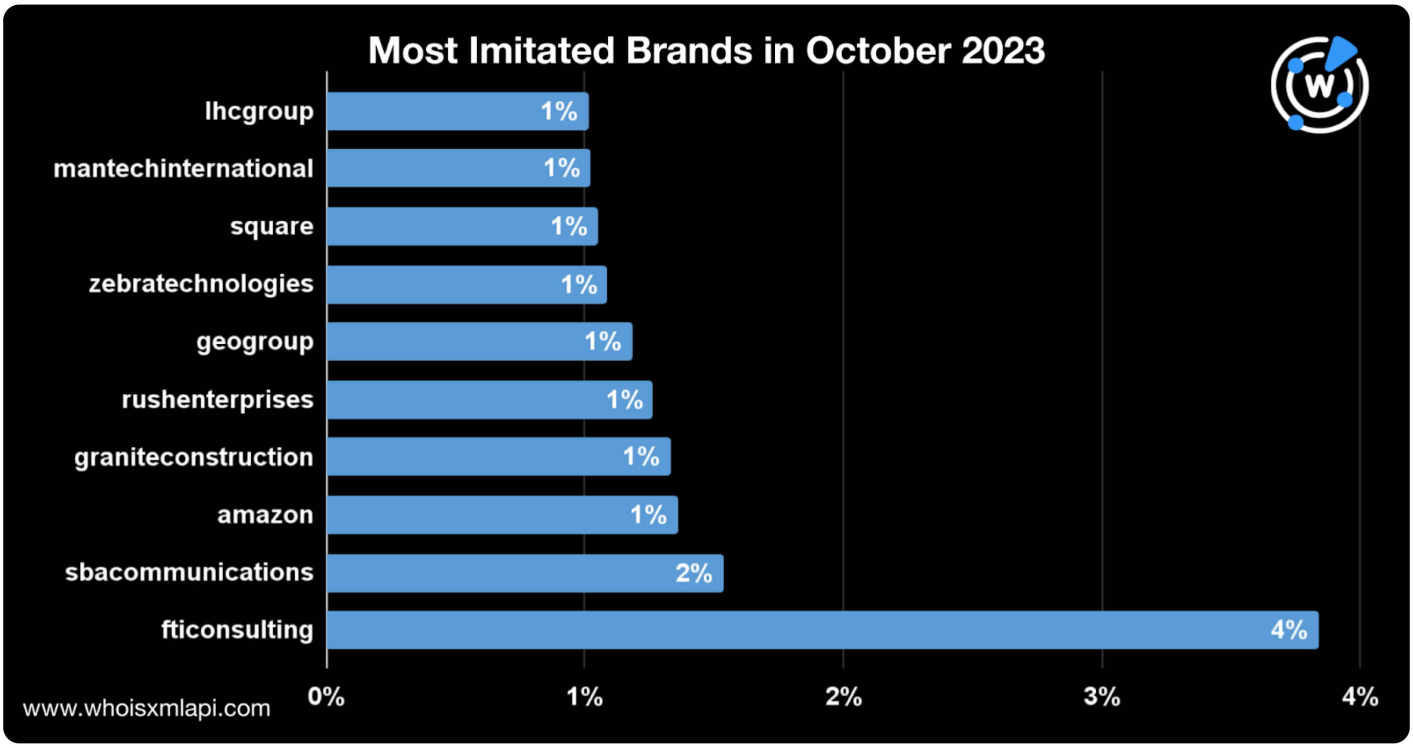
The continued popularity of **xn** suggests that registrants continued to register internationalized domain names (IDNs).


Common Strings among the October 2023 NRDs

www.whoisxmlapi.com

Early Warning Phishing Detection

We also analyzed a sample of the Early Warning Phishing Feed comprising thousands of domains, revealing that the most frequently appearing string was still **fticonsulting**, which was found in nearly 4% of the suspicious domains. Other popular strings were **sbacommunications**, **amazon**, **graniteconstruction**, **rushenterprises**, **geogroup**, **zebratechnologies**, **square**, **mantechinternational**, and **lhcgroup**.



Cybersecurity through the DNS Lens

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

- **Phishing Group Found Abusing .top Domains:** WhoisXML API threat researcher Dancho Danchev discovered a phishing operation weaponizing .top domains, leading our research team to more than 4,000 additional connected artifacts.

- **Fishing for QR Code Phishing Traces in the DNS:** Aided with WHOIS and DNS intelligence, WhoisXML API researchers expanded 18 URLs tagged as indicators of compromise (IoCs) related to a QR phishing code campaign to 10,000+ connected artifacts.

- **Catching Messenger Phishing Footprints Using a DNS Net:** We recently looked into MrTonyScam, a phishing campaign targeting Facebook business accounts that aim to infect victim devices with password-stealing malware. The attackers left behind DNS traces, leading us to over a dozen public email addresses and 1,000+ artifacts sharing the same email address and strings as the threat IoCs.

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.