WhoisXMLAPI

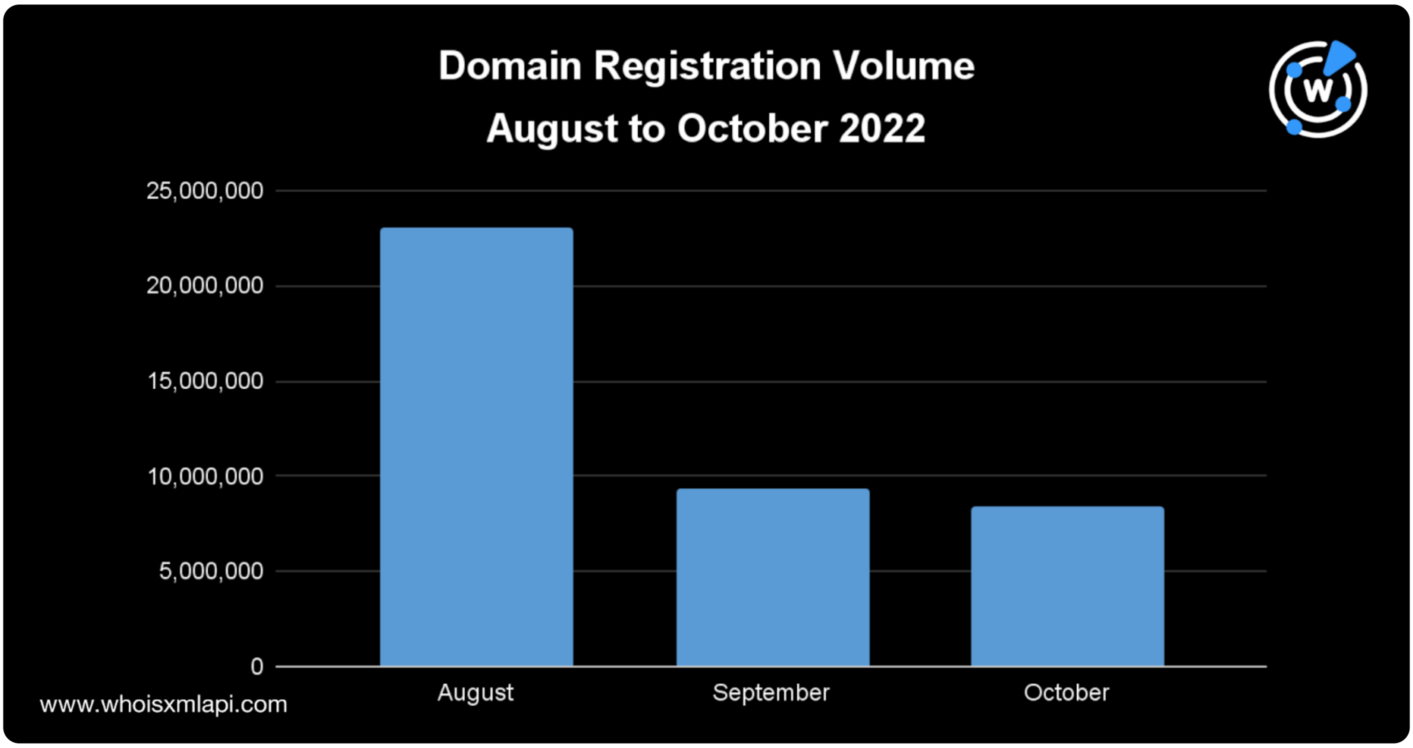
# October 2022: DNS Highlights

Posted on November 9, 2022

WhoisXML API analyzed more than 8.4 million newly registered domains (NRDs) added during 1–31 October 2022 to detect trends, such as top-level domain (TLD) and text string usage. Check out our findings below, along with threat reports our researchers put together, to provide the Internet community with domain, DNS, and IP intelligence.

## Domain Registration Volume in the Past Three Months

The number of domain registrations sharply decreased from August to September and continued to decline in October. From 9.3 million NRDs in September, the volume went down to 8.4 million in October. The chart below shows the monthly registration volume in the past three months.

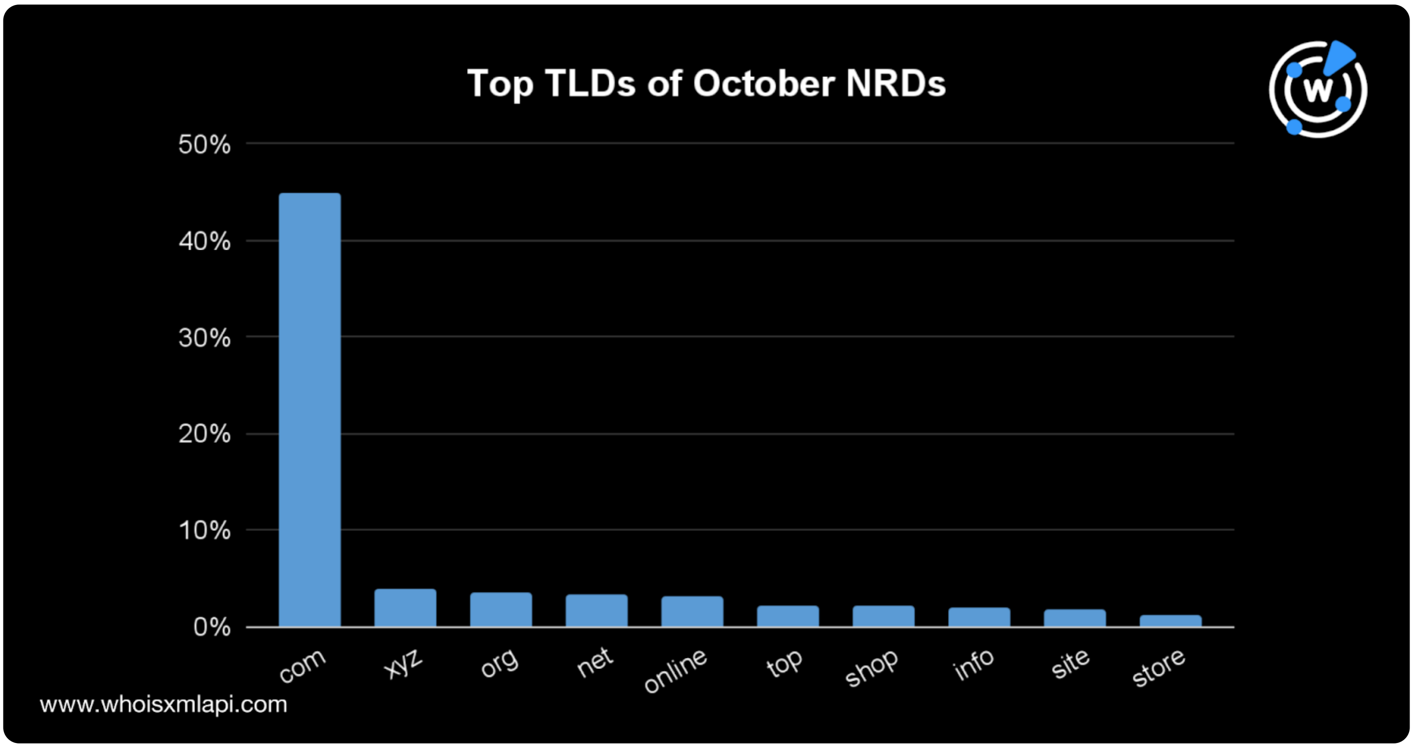


## Zooming in on October NRDs

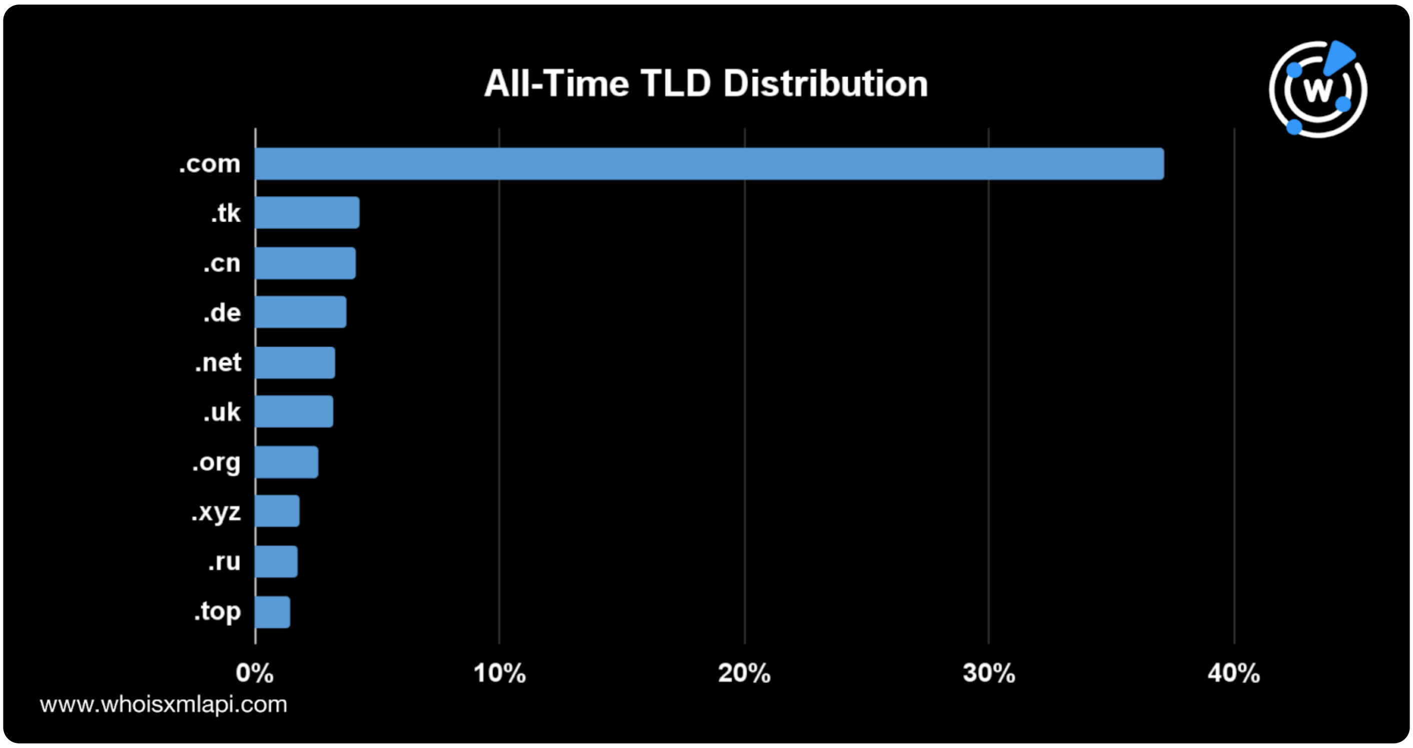
Using a sample comprising 3.4 million NRDs, we sought to determine the top TLDs and most commonly used text strings among the October NRDs.

### TLD Distribution

About 45% of the NRDs fell under the .com TLD space. The number dropped from the previous month, where TLDs accounted for 60% of the total domain registration volume. Other generic TLDs (gTLDs) in the top 10 were .org and .net, while the rest were new gTLDs, such as .xyz, .online, .top, .shop, and .site.



The top TLDs were the same as those in September. However, when we looked at the overall registration distribution per TLD, the top 10 TLDs differed, except for .com, which continued to account for the majority share of 37.16%. Country-code TLDs (ccTLDs) .tk and .cn followed suit with 4.29% and 4.16% shares, respectively. The chart below shows the TLD distribution as of 7 November 2022.



## Common Strings Appearance in SLDs

Internationalized domain names (IDNs) continued to trend, with “xn” most recurring among the NRDs. Generic tech terms, such as “app,” “web,” “www,” and “URL” were also prevalent, along with e-commerce-related strings, such as “shop” and “market.”

We will continue monitoring the DNS for registration trends that could be relevant to organizations making critical business decisions.

## This Month's Cybersecurity through the DNS Lens

WhoisXML API is always on the lookout for opportunities to enrich cyberthreat intelligence with IP, DNS, and other Internet-related data to hasten threat detection and prevention. This October, our researchers took deep dives into different types of threats, including domain shadowing, spamming, and malware-as-a-service (MaaS) campaigns. Below are some of the threat reports we published. You can find more here.

- **Domain Shadowing IoC Expansion Led to Thousands of Possible Connections:** Our researchers built on a Palo Alto Networks report that enumerated indicators of compromise (IoCs) associated with domain shadowing. We found thousands of connected domains added in September and October 2022, several of which hosted questionable content.

- **Insights into an Active Malicious Spam Domain Portfolio:** We analyzed an active malicious spam domain portfolio and found hundreds of domains associated with the network through their registrant email and IP addresses.

- **Eternity's LilithBot, Soon Available to Regular Internet Users?:** MaaS products like LilithBot may extend their reach beyond the Dark Web and seep into the Surface Web. Our research revealed dozens of domains that could serve as MaaS vehicles.

- **Uncovering a Large Footprint of Fake NordVPN Sites:** Scammers targeted NordVPN users by creating fake domains and websites. We analyzed the campaign IoCs and found more than 10,000 connected domains registered using the same email addresses as the IoCs.

We will continue investigating cyberthreats, expanding IoCs, and enriching cyber intelligence through our threat reports.

***Please do not hesitate to contact us for more information about the domain registration events and analyses mentioned above or any inquiries about enterprise commercial solutions***.