# November 2024: Domain Activity Highlights

Posted on December 17, 2024

The WhoisXML API research team analyzed 8.2 million domains registered between 1 and 30 November 2024 to identify the most popular registrars, top-level domain (TLD) extensions, and other global domain registration trends.

We also determined the top TLD extensions used by 59.6 billion domains from our DNS database's A record full file released in the same month.

Next, we studied the top TLDs of 1.1 million domains detected as indicators of compromise (IoCs) in November.

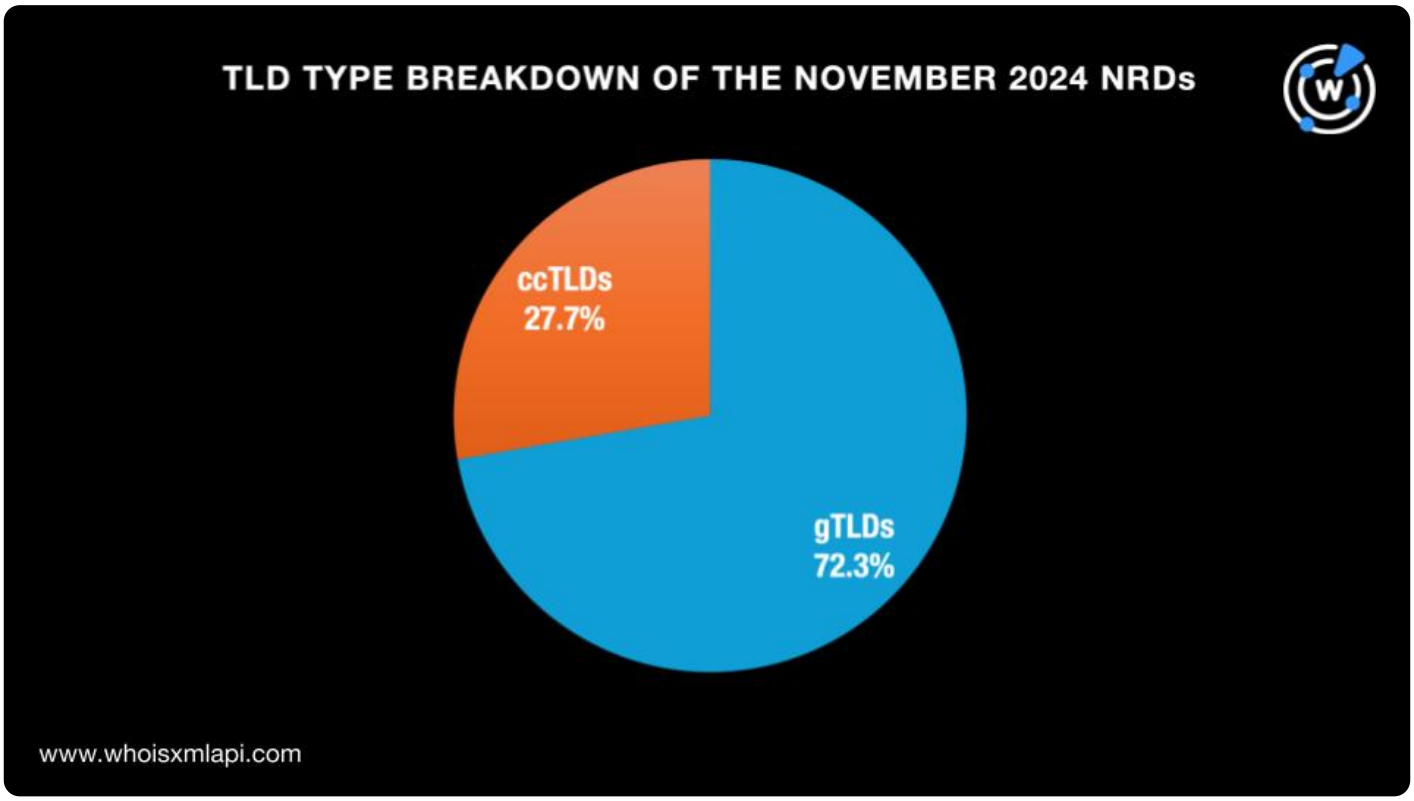
Finally, we summed up our findings and provided links to the threat reports produced using DNS, IP, and domain intelligence sources during the period.

***You can download an extended sample of the data obtained from this analysis from our website.***

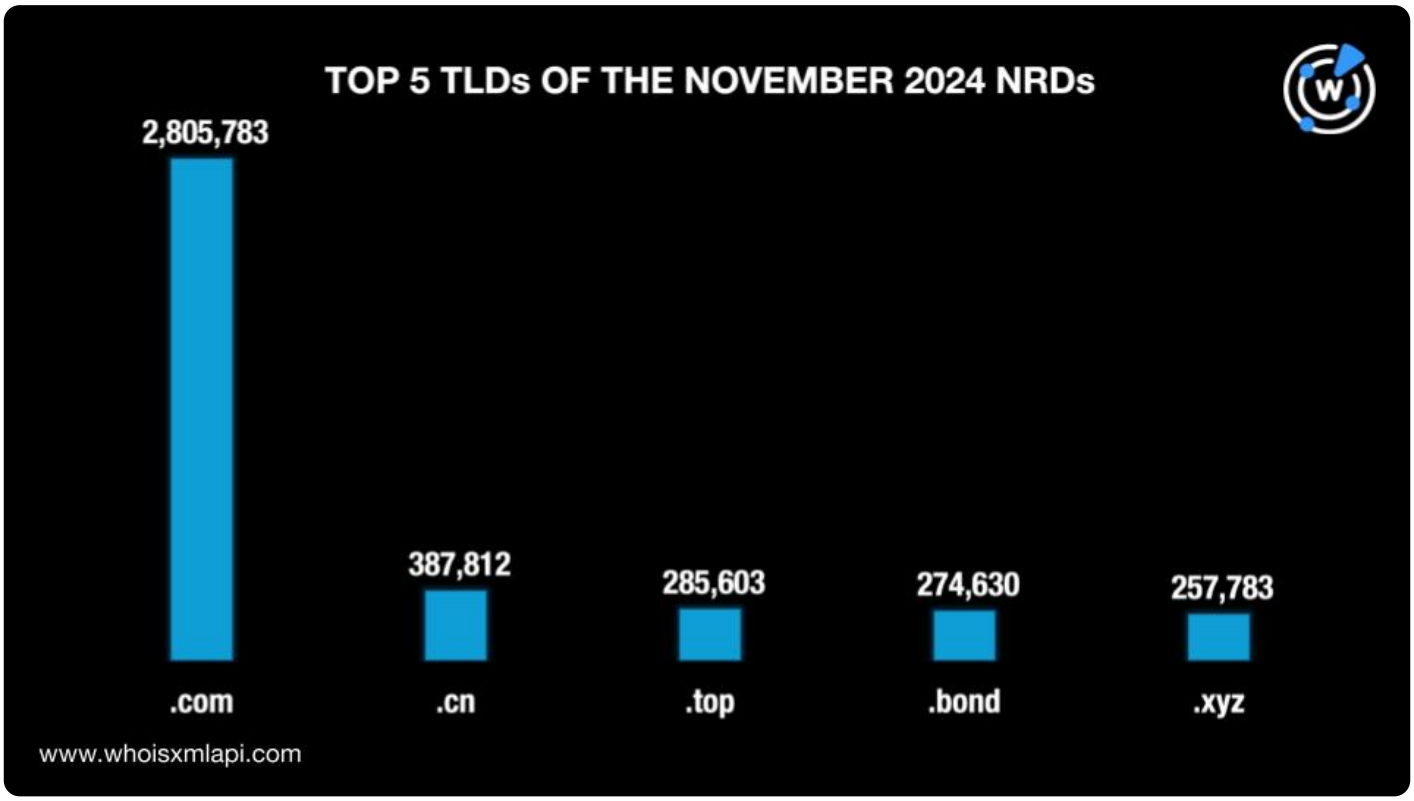
## Zooming in on the November 2024 NRDs

### TLD Distribution

A majority of the 8.2 million domains registered in November 2024, 72.3% to be exact, used generic TLD (gTLD) extensions, while the remaining 27.7% used country-code TLD (ccTLD) extensions.

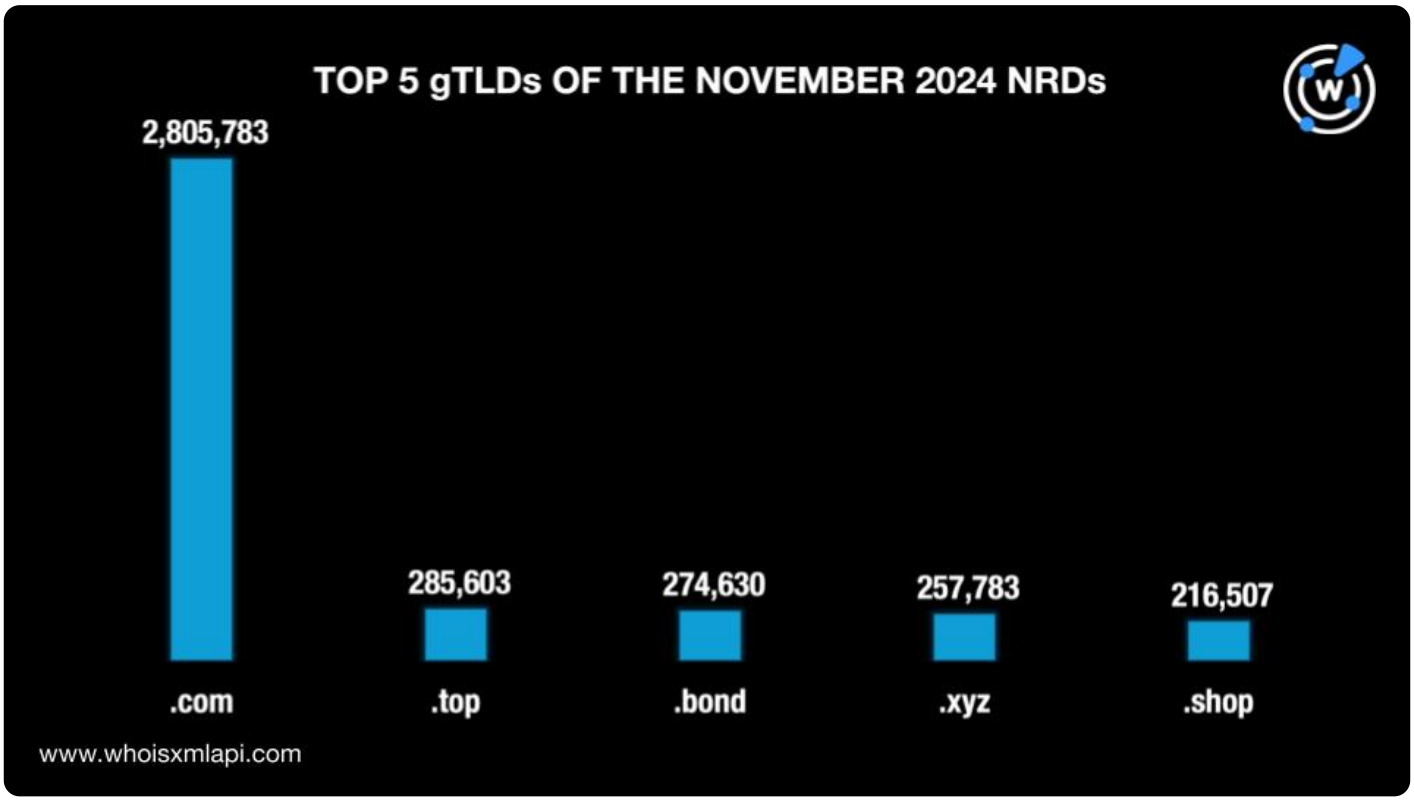



The .com TLD remained the most popular extension used by 34.3% of the total number of newly registered domains (NRDs), down from 37.2% in October. The other most used TLDs on the top 5 followed with a significant gap as in the previous month. One ccTLD made the cut in second place—.cn with a 4.7% share. Three other gTLDs—.top, .bond, and .xyz—completed the roster with shares of 3.5%, 3.4%, and 3.1%, respectively.

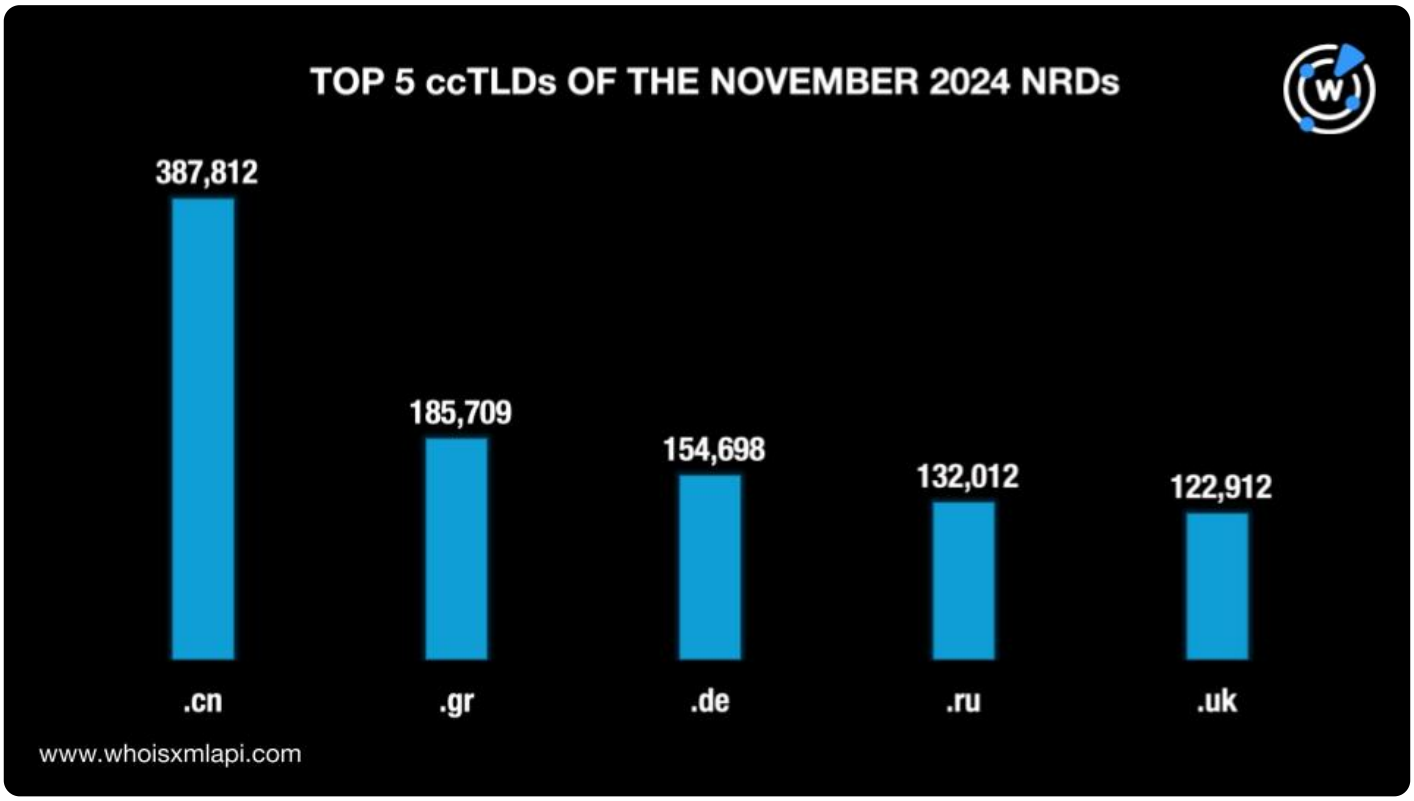



We then analyzed the November TLDs further to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 643 gTLDs, .com remained the most used, accounting for a 47.4% share, down from 49.1% in October. The rest of the top 5 lagged far behind. In fact, second placer .top only had a 4.8% share. The other gTLDs were .bond with a 4.6% share, .xyz with 4.4%, and .shop with 3.7%.

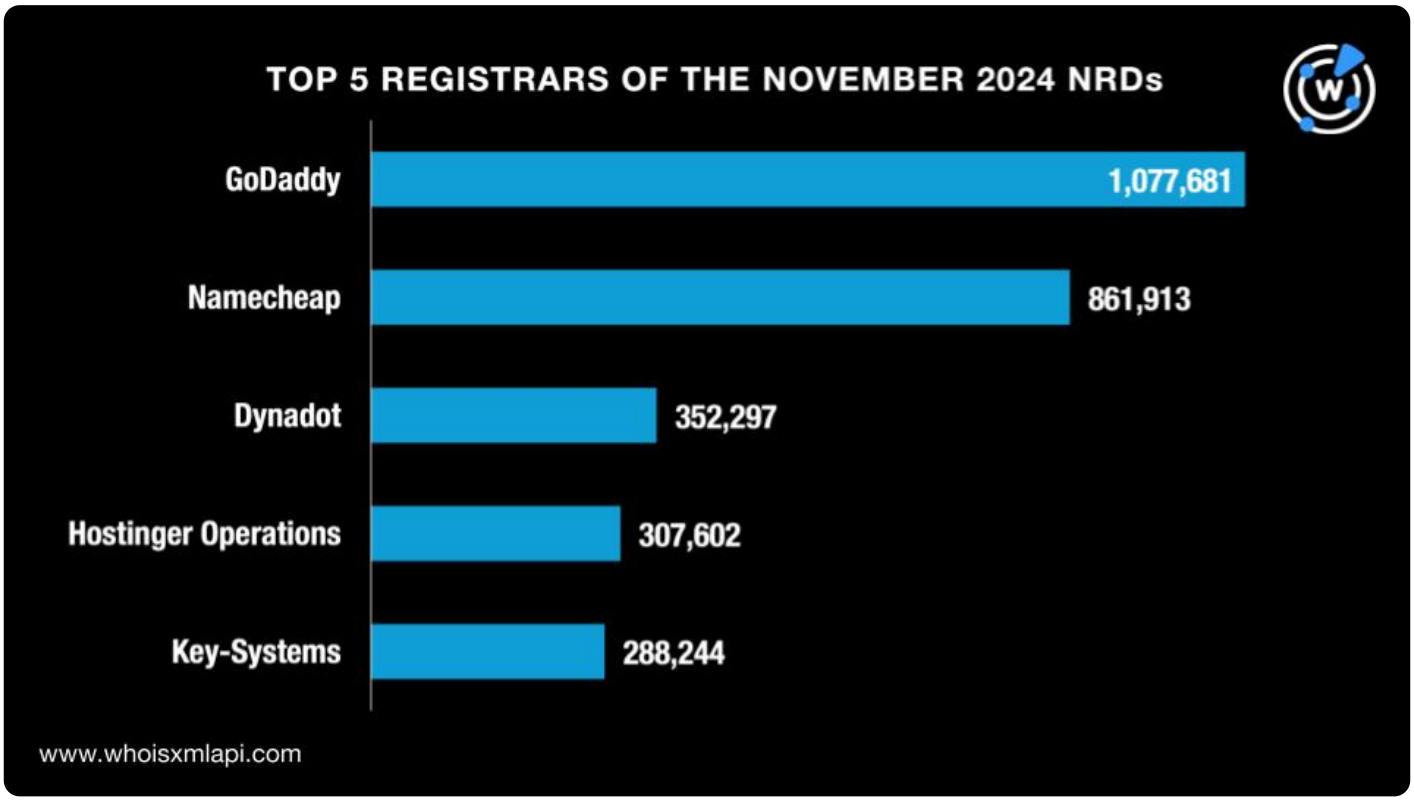



Meanwhile, .cn remained the top ccTLD out of 252 extensions with a 17.1% ccTLD share, marking a huge increase from 8.5% in October. The other commonly used ccTLDs were .gr with an 8.2% share, .de with 6.8%, .ru with 5.8%, and .uk with 5.4%.



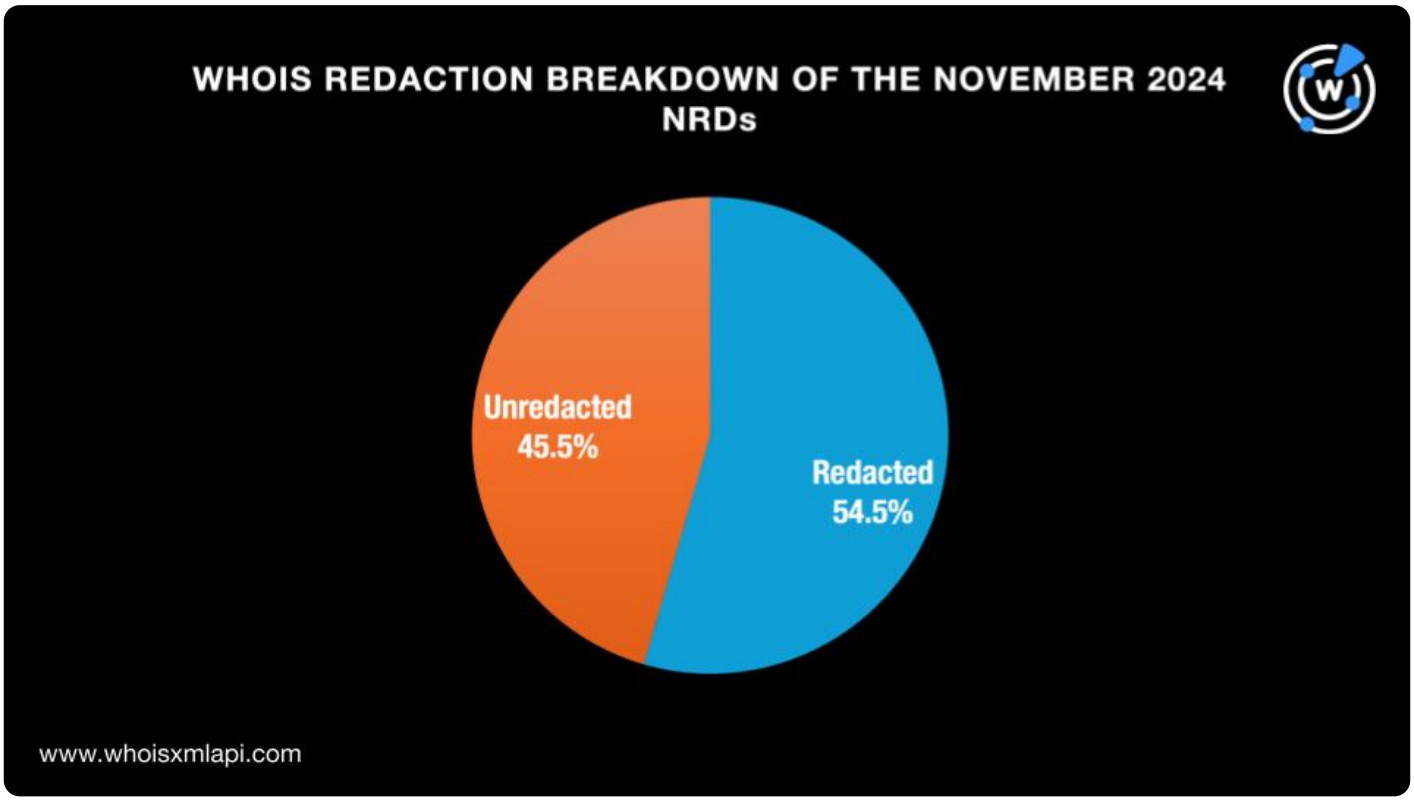

## Registrar Distribution

GoDaddy continued to reign supreme among the registrars with a 13.2% share, down from 14.6% in October. Namecheap came in second place with a 10.5% share. The rest of the top 5 were Dynadot with a 4.3% share, Hostinger Operations with 3.8%, and Key-Systems with 3.5%.




## WHOIS Data Redaction

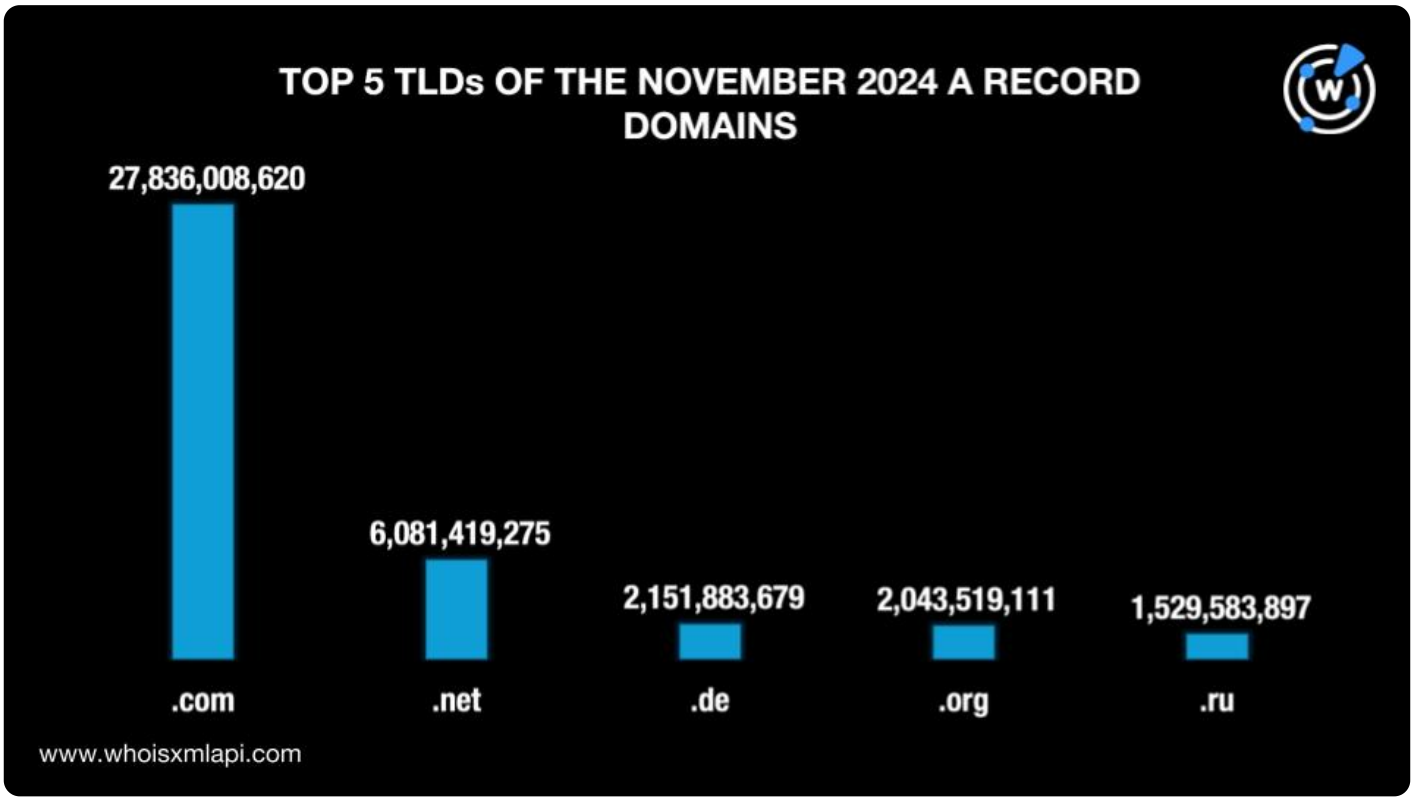
As usual, a majority of the NRDs, 54.5% to be exact, down from 55.4% in October, had redacted WHOIS records. The remaining 45.5%, up from 44.6% last month, meanwhile, had public WHOIS records.




# A Closer Look at the November 2024 DNS Records

## Top TLDs of the A Record Domains

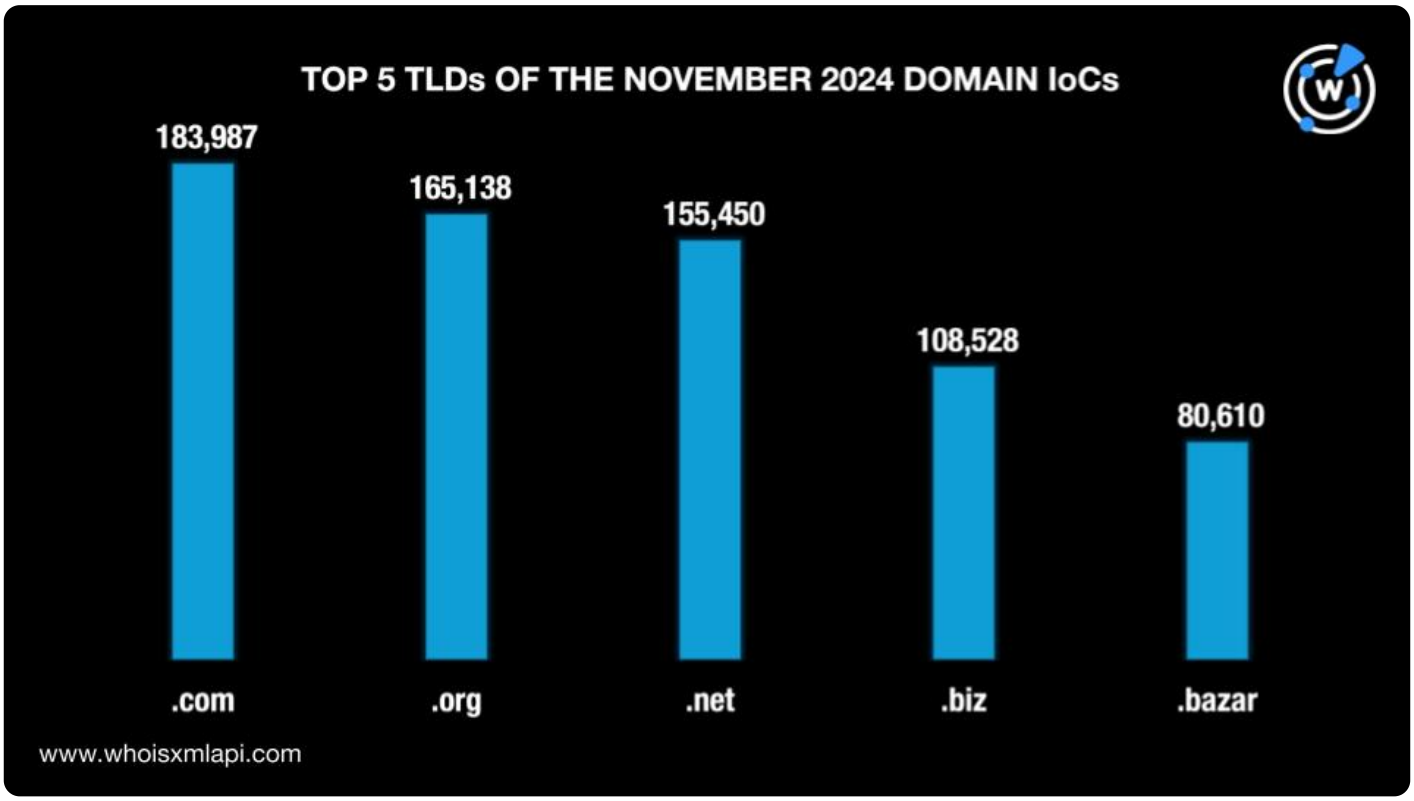
Next, we analyzed 59.6 billion domains from our DNS database's A record full file for November 2024, which included DNS resolutions from the past 365 days. We found that 46.7% used the .com TLD, down from 48.7% in October. The rest of the top 5 comprised two other gTLDs (i.e., .net with a 10.2% share and .org with 3.4%) and two ccTLDs (i.e., .de with a 3.6% share and .ru with 2.6%).




## Cybersecurity through the DNS Lens

### Top TLDs of the November 2024 Domain IoCs

As usual, we analyzed 1.1 million domains tagged as IoCs for various threats detected in November. Our analysis revealed that .com remained the most popular TLD with a 17.1% share. The remaining top TLDs were all gTLDs as well, namely, .org with a 15.4% share, .net with 14.5%, .biz with 10.1%, and .bazar with 7.5%.




## Threat Reports

Below are the threat reports we published in November 2024.

- **A DNS Deep Dive into FUNULL's Triad Nexus:** FUNNULL, the threat actors behind the Polyfill supply chain attack, as it turns out, were also responsible for investment scams, fake trading app distribution, and suspect gambling networks in a massive campaign dubbed "Triad Nexus." WhoisXML API expanded a list of 63 suspicious indicators and uncovered 11,900+ connected artifacts.

- **Exploring the SideWinder APT Group's DNS Footprint:** The SideWinder advanced persistent threat (APT) group has been around for more than a decade now. It is not surprising, therefore, for its network to have grown over time. We expanded a list of 100 domains identified as IoCs and unveiled 500+ connected artifacts.

- **Uncovering Potential Black Friday and Thanksgiving Threats with DNS Data:** WhoisXML API's First Watch Malicious Domains Data Feed provided our researchers 2,324 domains containing the text strings **blackfriday** and **thanksgiving**. Our DNS deep dive into these domains likely to turn malicious led to the discovery of 6,600 other web properties worth being wary of.

- **A DNS Investigation of the GootLoader Campaign:** We investigated GootLoader, a malware that paved the way for ransomware infection or enabled further network compromise, and found that apart from the 12 domains tagged as IoCs, organizations and individuals alike should be aware of 1,000+ other potential threat vectors as well.

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.***