December 2024: Domain Activity Highlights

Posted on January 10, 2025

The WhoisXML API research team analyzed 7.9+ million domains registered between 1 and 31 December 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 60.1+ billion domains from our DNS database's A record full file released in the same month.

Next, we studied the top TLDs of 1.3+ million domains detected as indicators of compromise (IoCs) in December.

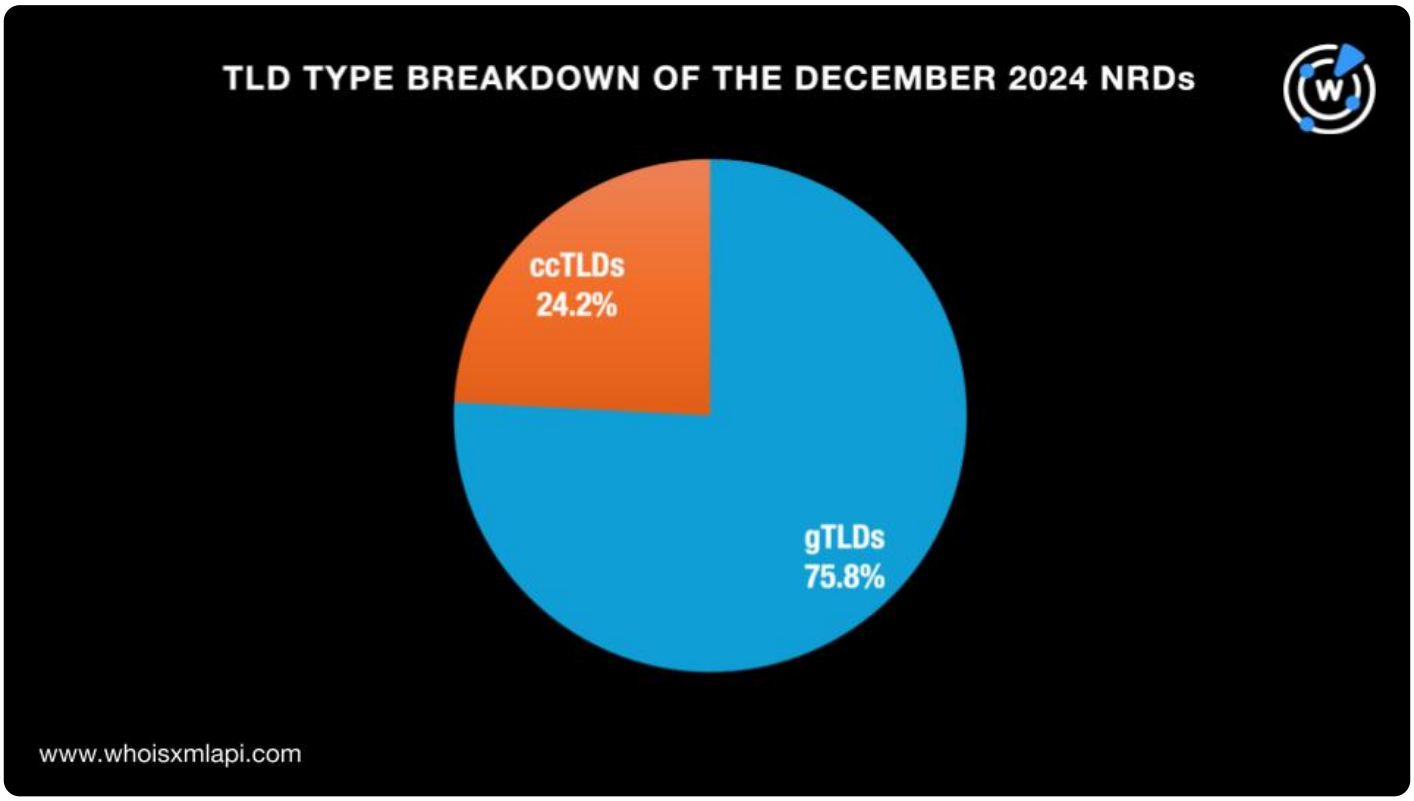
Finally, we summed up our findings and provided links to the threat reports produced using DNS, IP, and domain intelligence sources during the period.

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

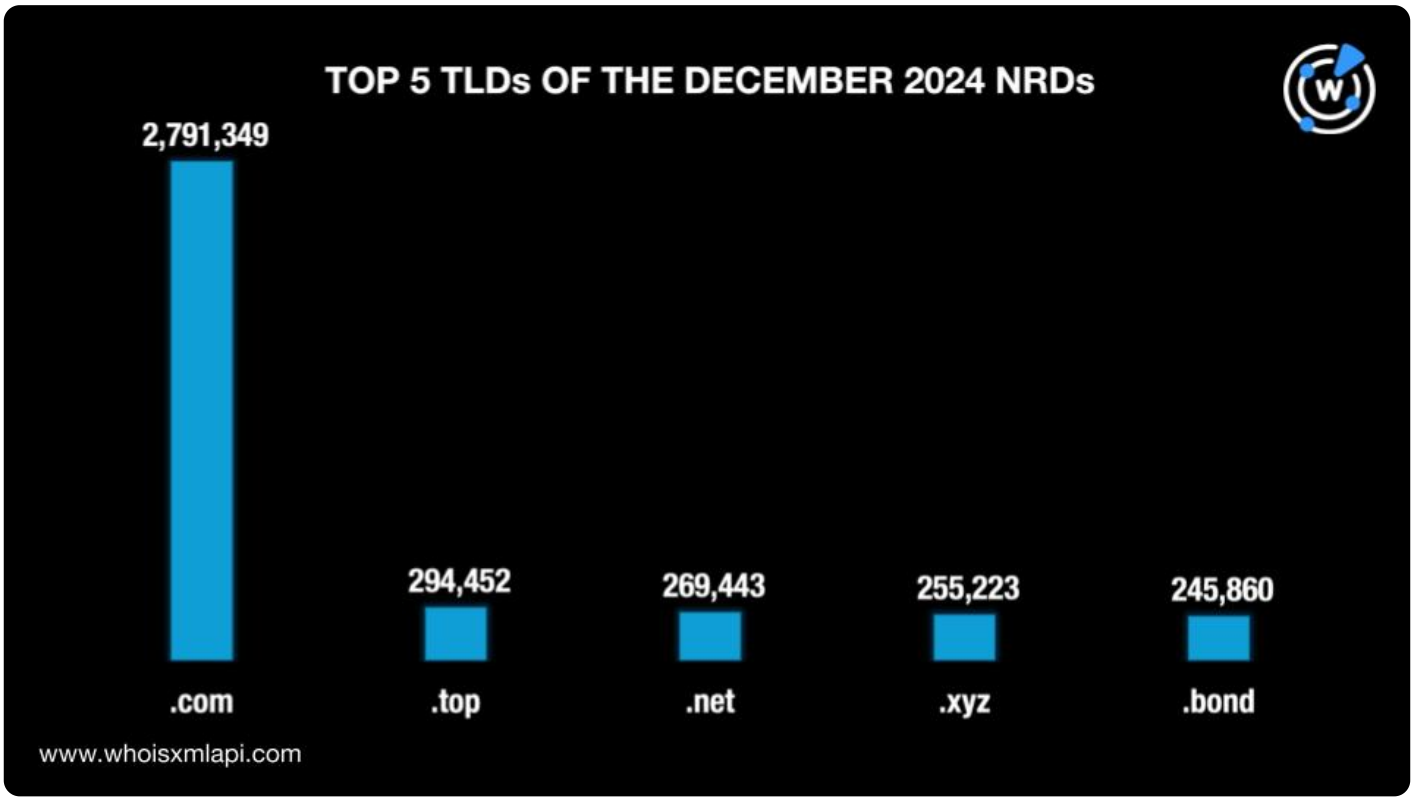
Zooming in on the December 2024 NRDs

TLD Distribution

A majority of the 7.9+ million domains registered in December 2024, 75.8% to be exact, used generic TLD (gTLD) extensions, while the remaining 24.2% used country-code TLD (ccTLD) extensions.

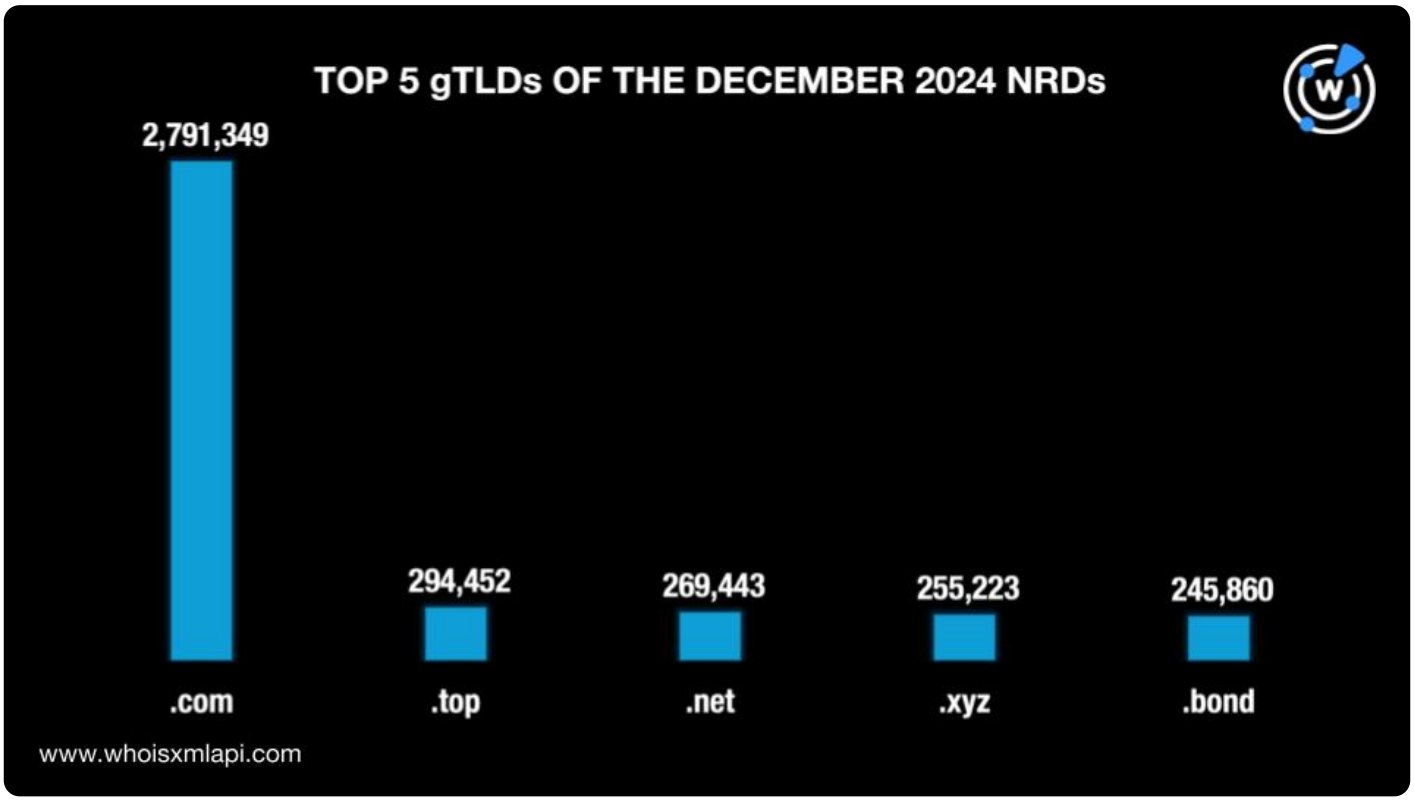


The .com TLD remained the most popular extension used by 34.9% of the total number of newly registered domains (NRDs), up from 34.3% in November. The other most used TLDs on the top 5 followed with a significant gap as in the previous month. Four other gTLDs—.top, .net, .xyz, and .bond—completed the roster with shares of 3.7%, 3.4%, 3.2%, and 3.1%, respectively.

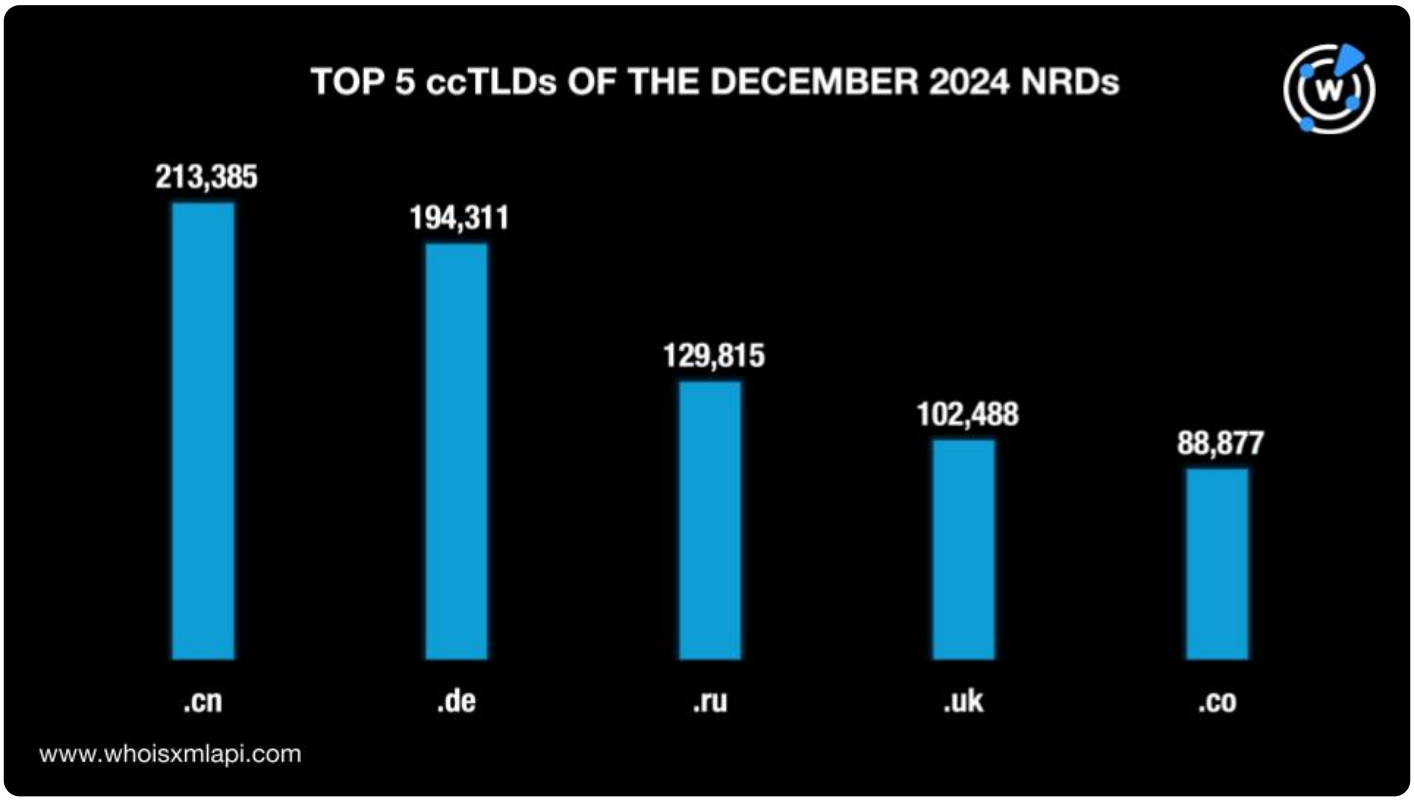


We then analyzed the December TLDs further to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 646 gTLDs, .com remained the most used, accounting for a 46.1% share, down from 47.4% in November. The rest of the top 5 lagged far behind. In fact, the four other gTLDs only clocked in about a 4.0% share each. The .top gTLD only had a 4.9% share, followed by .net with a 4.5% share, .xyz with 4.2%, and .bond with 4.1%.

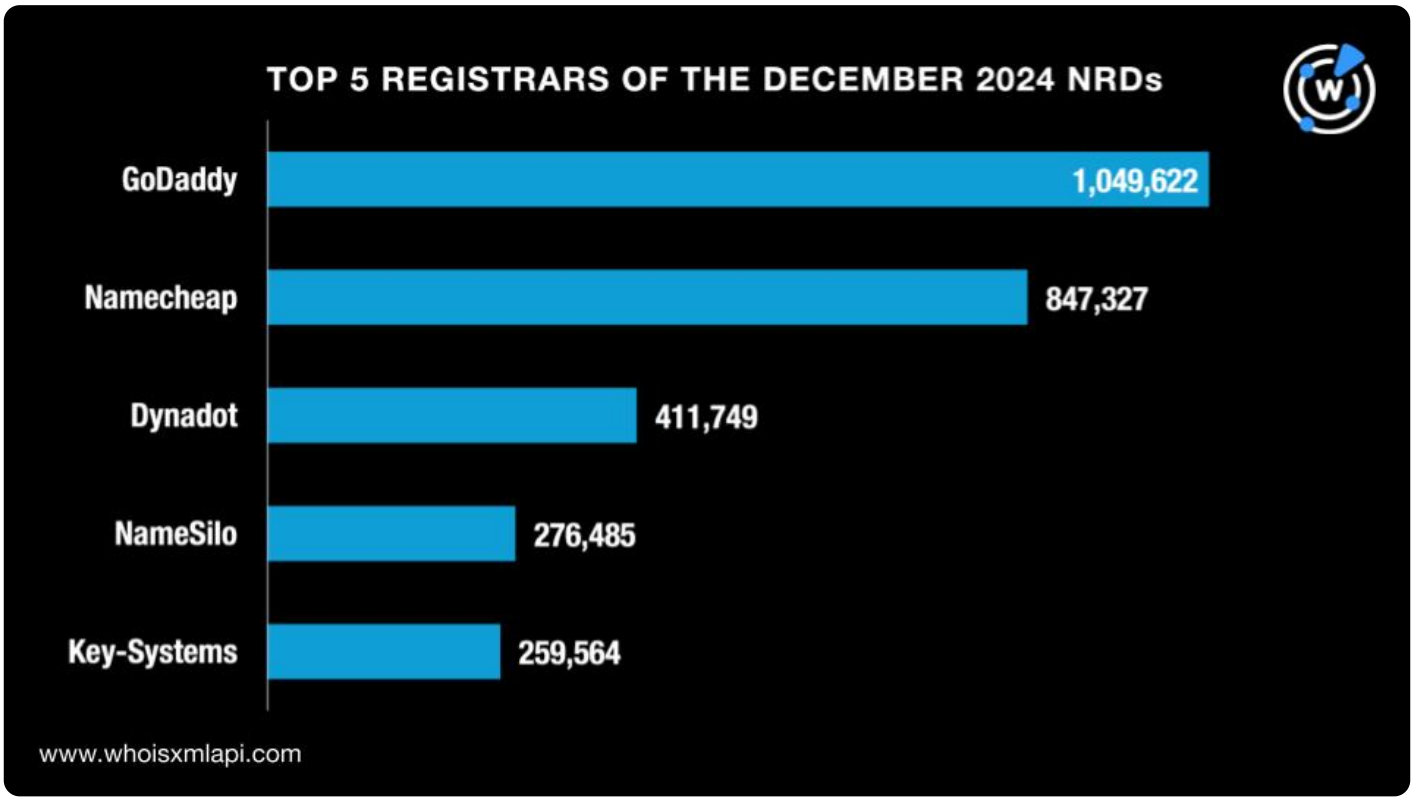


Meanwhile, .cn remained the top ccTLD out of 249 extensions with an 11.0% share, marking a significant decrease from 17.1% in November. The other commonly used ccTLDs were .de with a 10.1% share, followed by .ru with 6.7%, .uk with 5.3%, and .co with 4.6%.



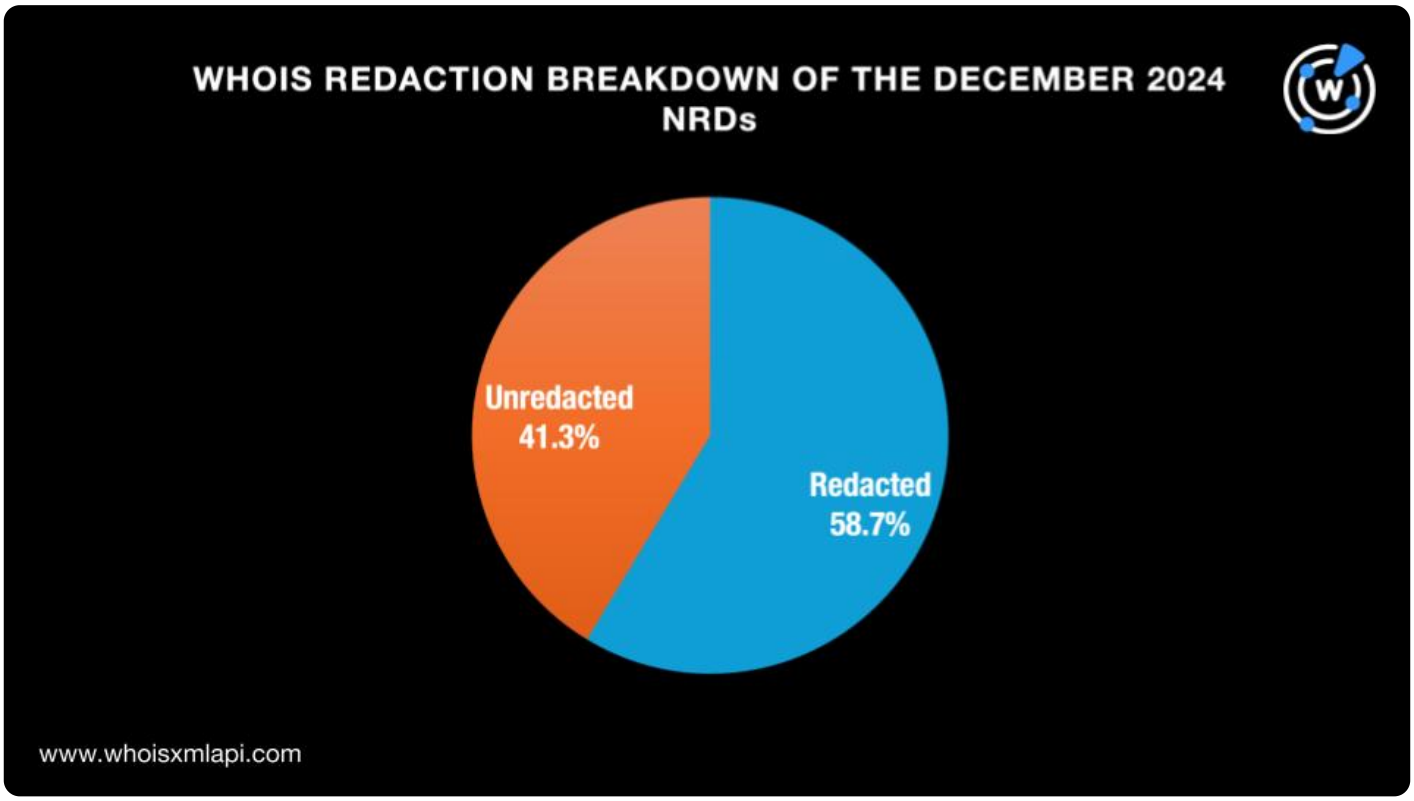
Registrar Distribution

GoDaddy continued to reign supreme among the registrars with a 13.1% share, slightly down from 13.2% in November. Namecheap took the second spot with a 10.6% share. The rest of the topnotchers were Dynadot with a 5.2% share, followed by NameSilo with 3.5% and Key-Systems with 3.2%.



WHOIS Data Redaction

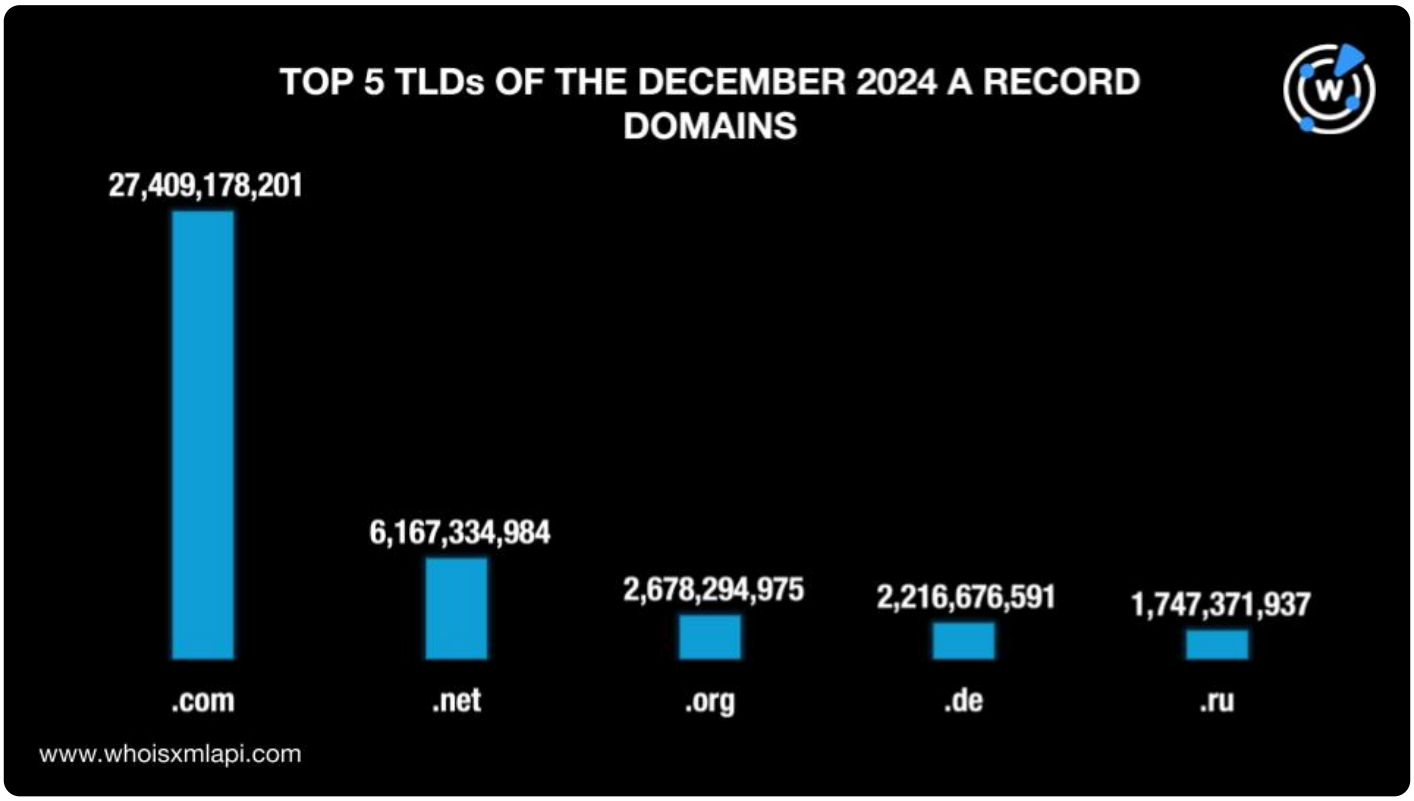
More NRDs in December, 58.7% compared with 54.5% in November, had redacted WHOIS records. The remaining 41.3%, meanwhile, had public WHOIS records.



A Closer Look at the December 2024 DNS Records

Top TLDs of the A Record Domains

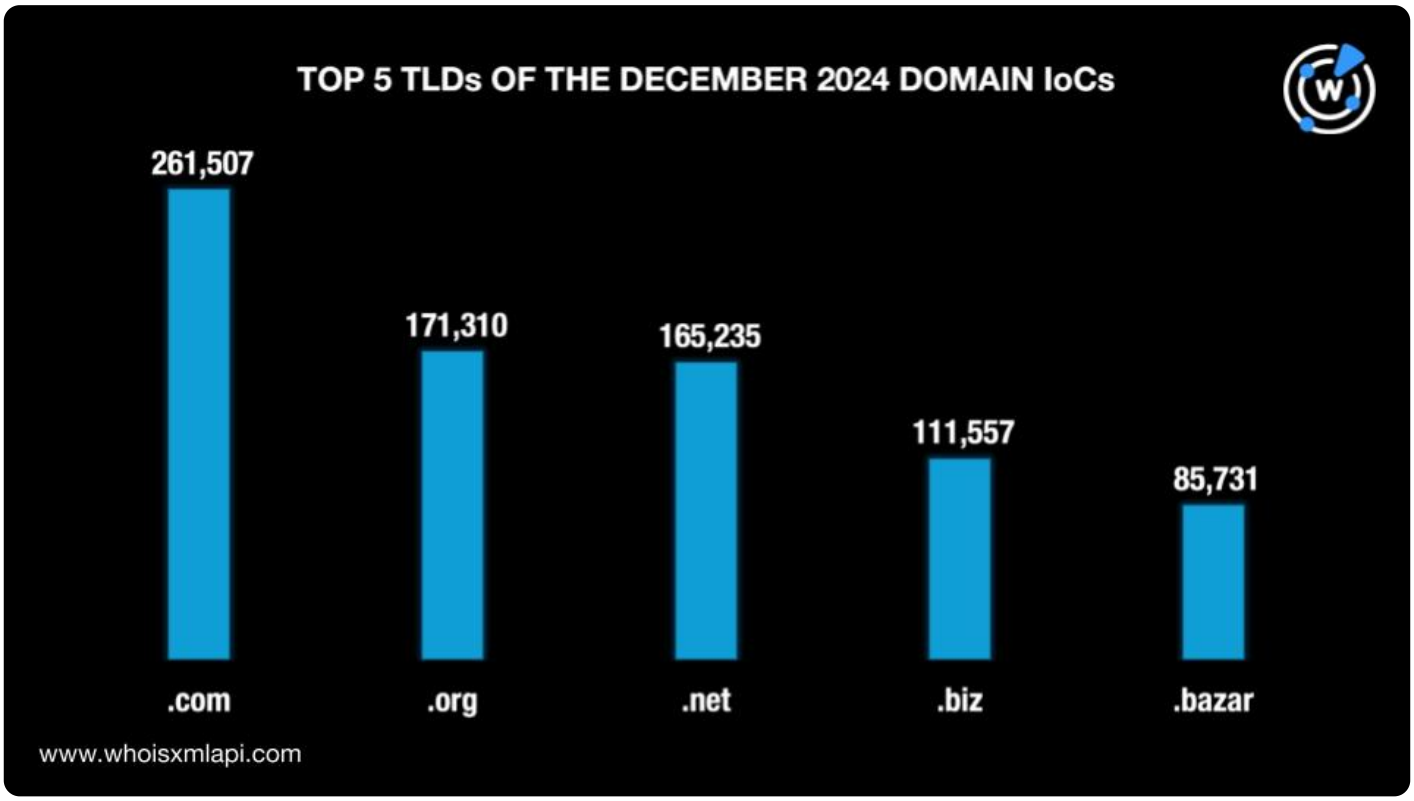
Next, we analyzed 60.1+ billion domains from our DNS database's A record full file for December 2024, which included DNS resolutions from the past 365 days. We found that 45.6% used the .com TLD, down from 46.7% in November. The rest of the top 5 comprised two other gTLDs (i.e., .net with a 10.3% share and .org with 4.5%) and two ccTLDs (i.e., .de with a 3.7% share and .ru with 2.9%).



Cybersecurity through the DNS Lens

Top TLDs of the December 2024 Domain IoCs

As usual, we analyzed 1.3+ million domains tagged as IoCs for various threats detected in December. Our analysis revealed that .com remained the most popular TLD with a 19.7% share, increasing from 17.1% in November. The remaining top TLDs were all gTLDs as well, namely, .org with a 12.9% share, .net with 12.4%, .biz with 8.4%, and .bazar with 6.5%.



Threat Reports

Below are the threat reports we published in December 2024.

- **A DNS Deep Dive into New Crypto Threat "Hidden Risk":** The WhoisXML API research team compiled 81 IoCs related to crypto threat Hidden Risk and expanded it aided by DNS intelligence. The actors launched a malicious campaign using fake crypto news to distribute the RustBucket malware.

- **Silent Night, Deadly Sites: How Christmas Cyber Threats Lurk in the DNS:** WhoisXML API collated 22,923 domains containing the string **christmas** from First Watch Malicious Domains Data Feed and analyzed their DNS footprint. We uncovered 27,000+ potentially connected artifacts.

- **Unraveling the DNS Connections of ToxicPanda:** Banking Trojan ToxicPanda was

specifically designed to affect Android devices. The WhoisXML API research team expanded a list of 21 domains tagged as IoCs related to the threat. Take a look at our findings.

- **Tracking Down APT Group WIRTE's DNS Movements:** Advanced persistent threat (APT) group WIRTE has been active since at least August 2018. It remains active despite upping its tactic ante. The latest attack used custom loaders like IronWind to infiltrate target networks. Read all about the attack.

- **Peering into Midnight Blizzard's DNS Footprint:** Midnight Blizzard, active since 2008, is still up to no good. The threat actor recently leveraged signed Remote Desktop Protocol (RDP) configuration files to gain access to victims' devices. WhoisXML API expanded a list of 39 domains tagged as 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.