January 2025: Domain Activity Highlights

Posted on February 17, 2025

The WhoisXML API research team analyzed 7.6+ million domains registered between 1 and 31 January 2025 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 61.2+ billion domains from our DNS database's A record full file released in the same month.

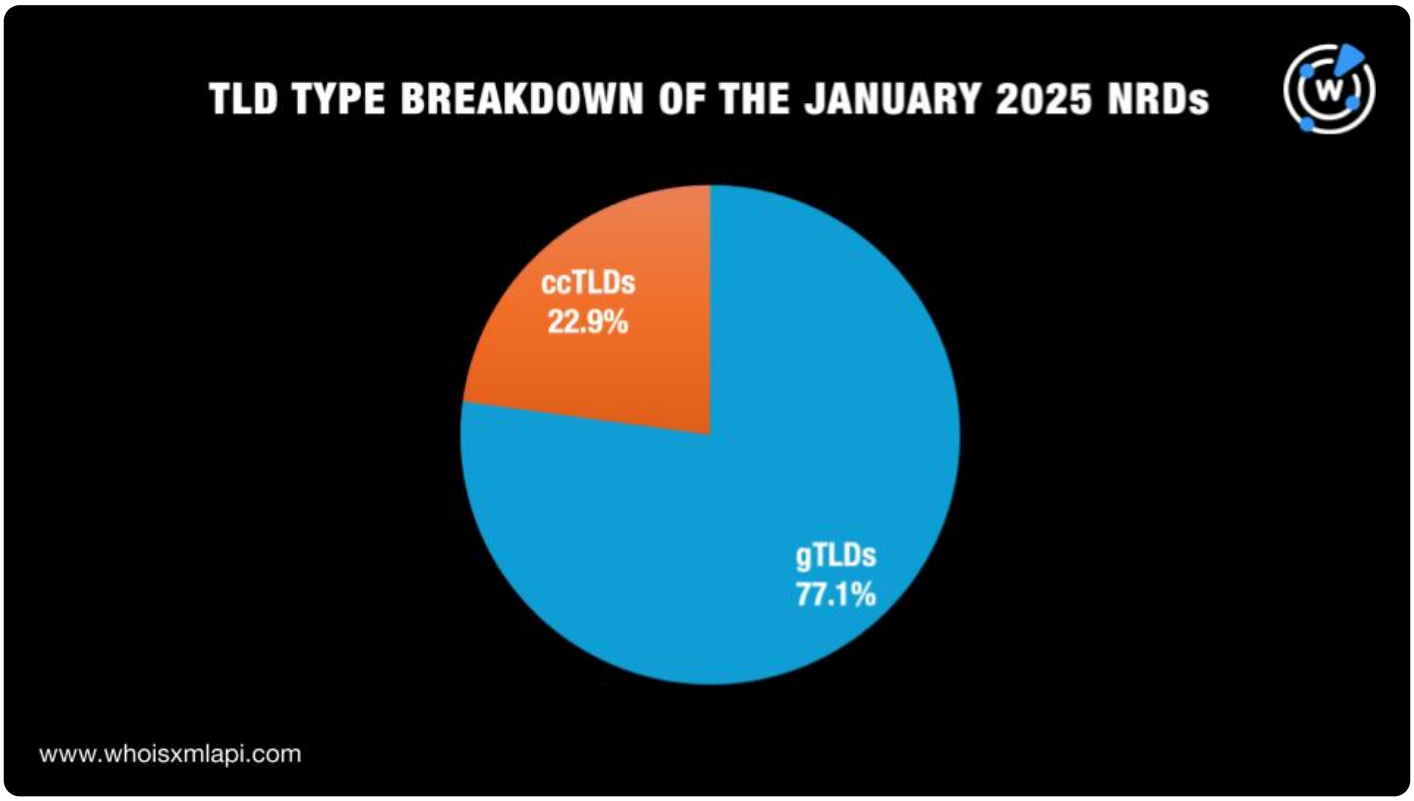
Finally, we summed up our findings and provided links to the threat reports produced using DNS, IP, and domain intelligence sources during the period.

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

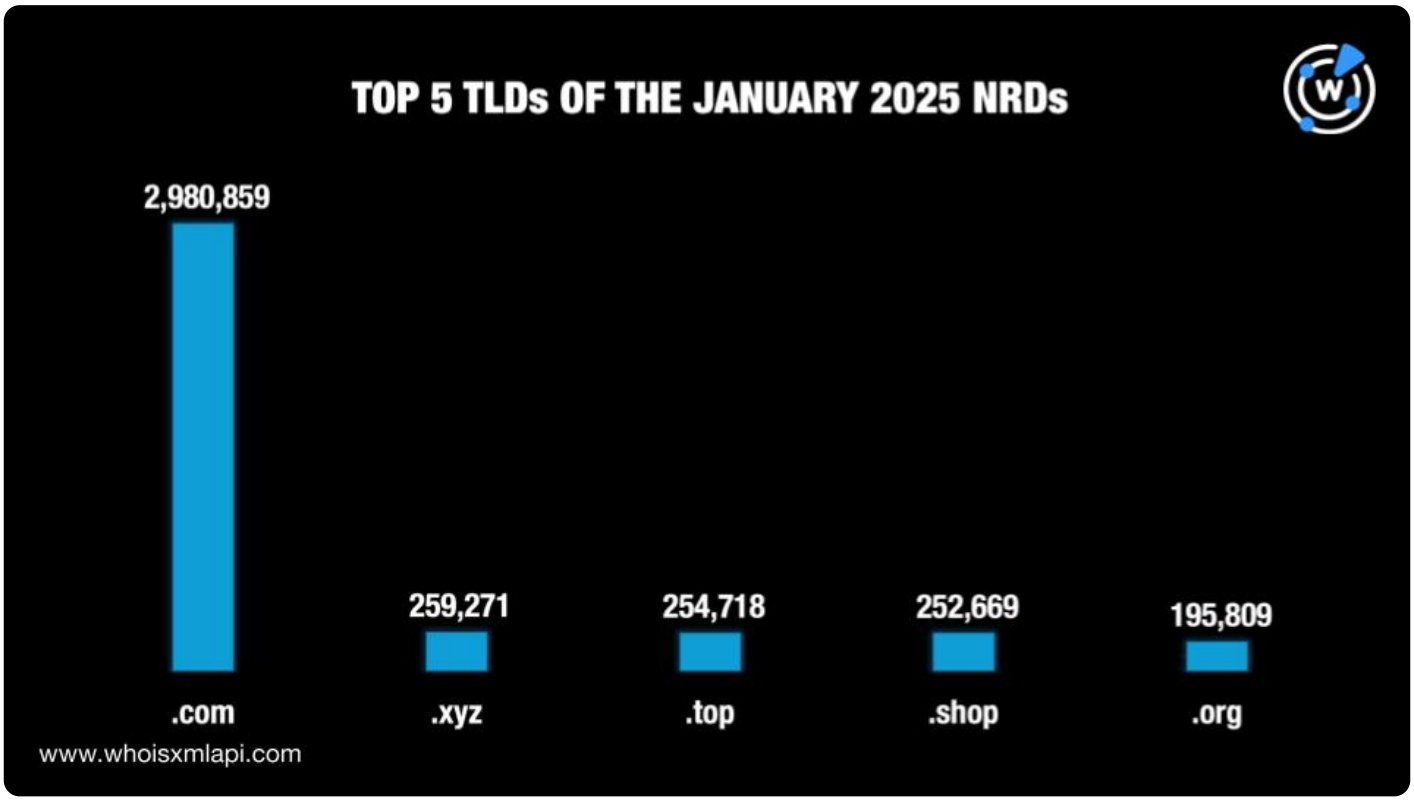
Zooming in on the January 2025 NRDs

TLD Distribution

A majority of the 7.6+ million domains registered in January 2025, 77.1% to be exact, used generic TLD (gTLD) extensions, while the remaining 22.9% used country-code TLD (ccTLD) extensions.

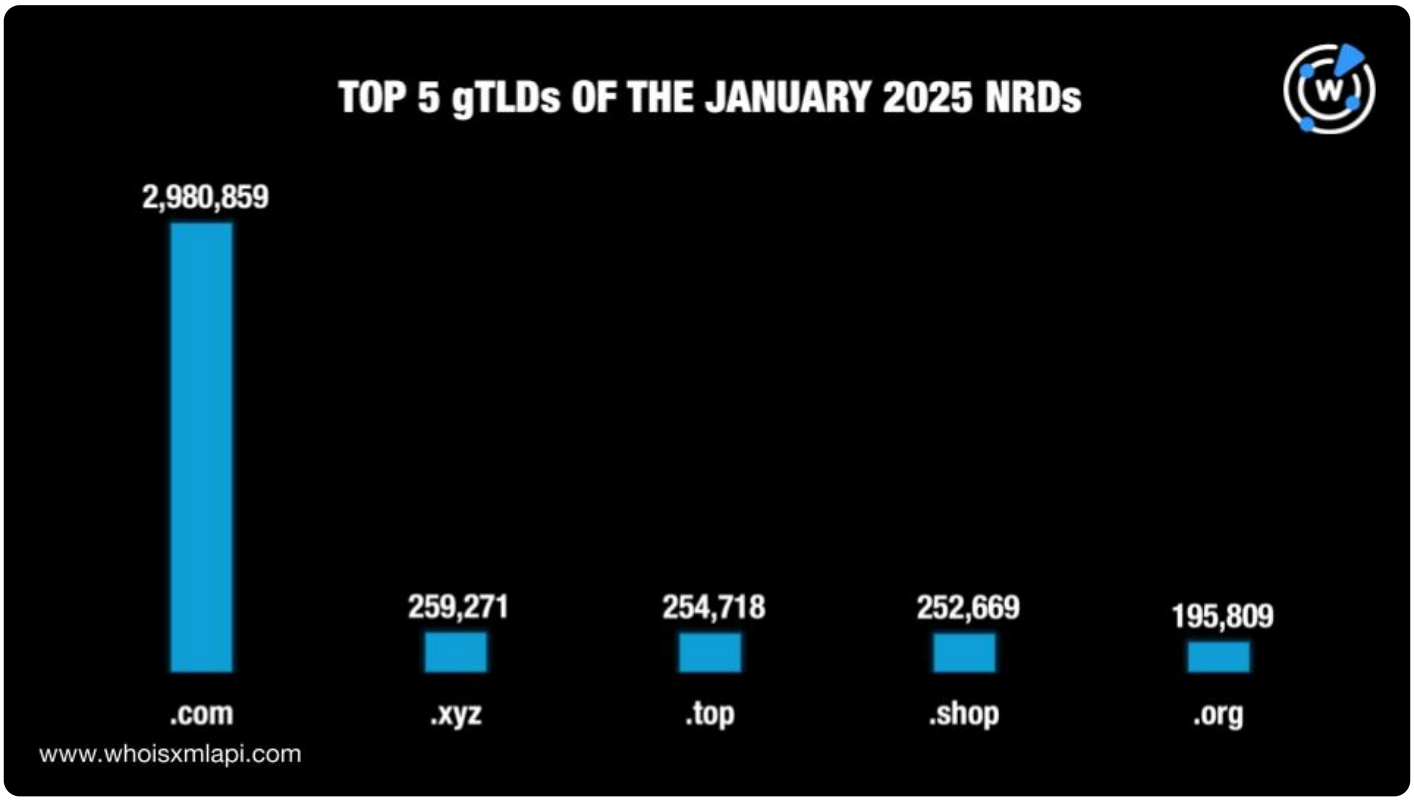


The .com TLD remained the most popular extension used by 38.9% of the total number of newly registered domains (NRDs), up from 34.9% in December. The other most used TLDs on the top 5 followed with a significant gap as in the previous month. Four other gTLDs, namely, .xyz (3.4%), .top and .shop (3.3% each), and .org (2.6%), completed the roster.

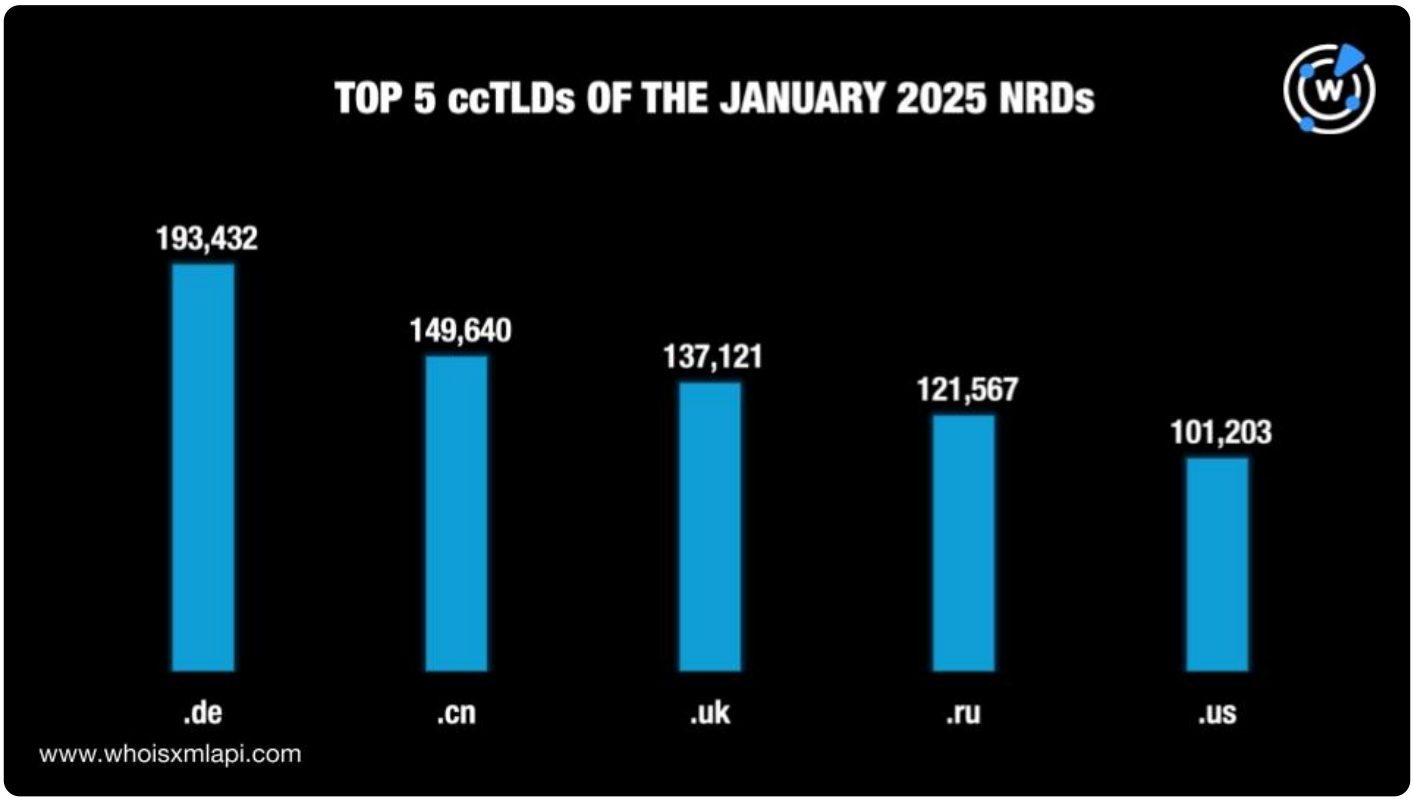


We then analyzed the January TLDs further to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 676 gTLDs, .com remained the most used, accounting for a 50.5% share, up from 46.1% in December. The rest of the top 5 lagged far behind. In fact, the four other gTLDs only clocked in a 16.3% share in total. The .xyz TLD had a 4.4% share, .top and .shop had 4.3% each, and .org had 3.3%.

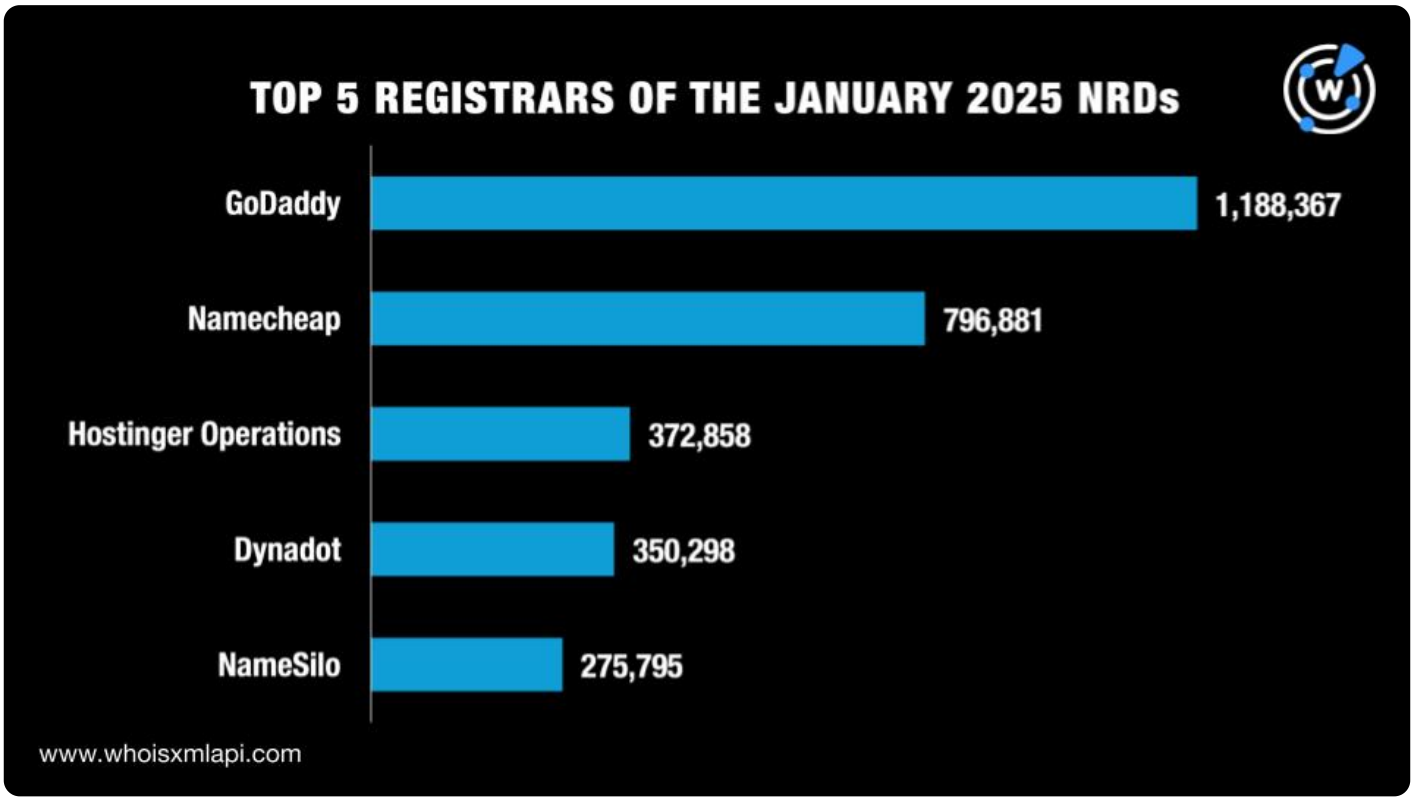


Meanwhile, .de has ousted .cn from the top ccTLD spot, replacing last month's leader. Out of 252 ccTLD extensions, .de accounted for an 11.0% share as in December. The other commonly used ccTLDs were .cn with an 8.5% share, .uk with 7.8%, .ru with 6.9%, and .us with 5.8%.



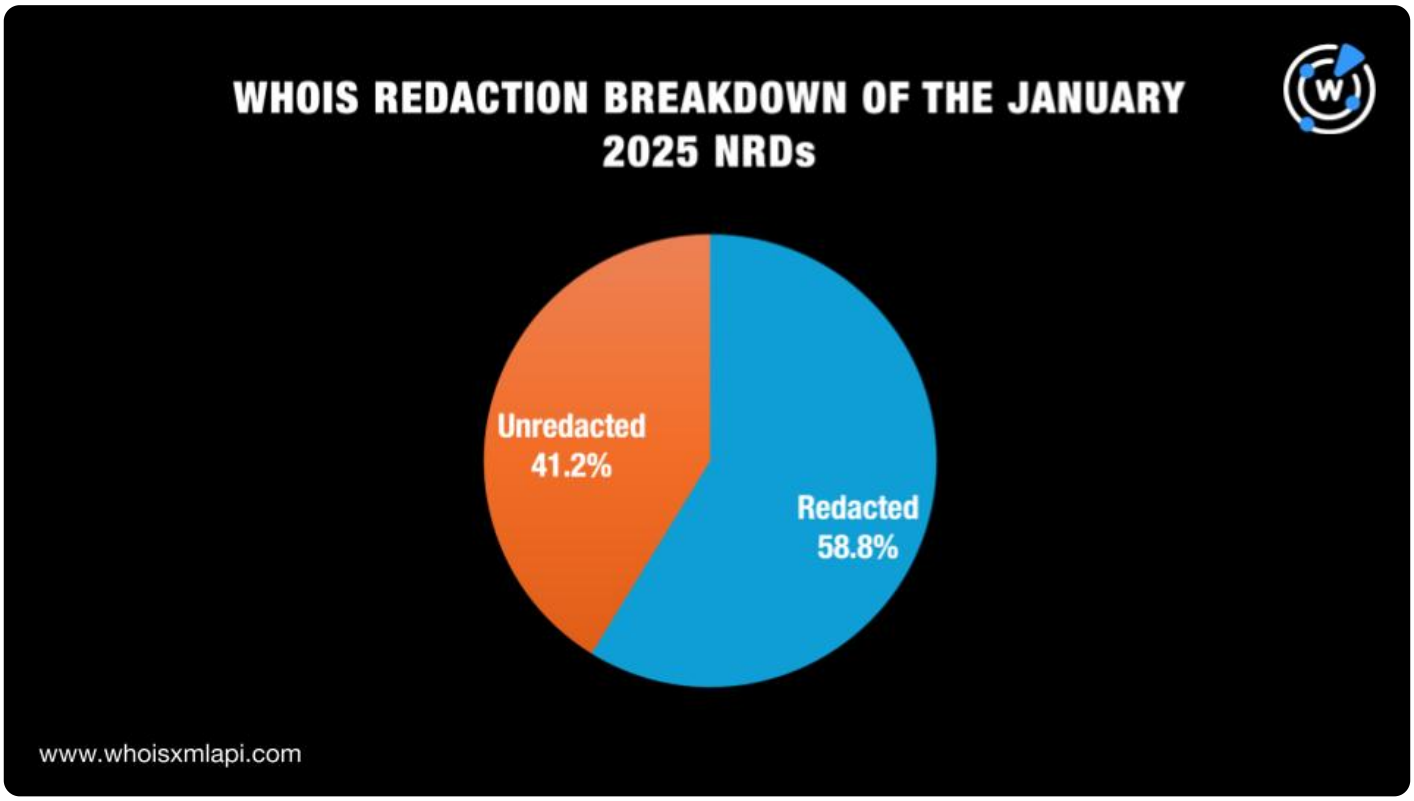
Registrar Distribution

GoDaddy continued to reign supreme among the registrars with a 15.4% share, up from 13.1% in December. Namecheap took the second spot with a 10.3% share. The rest of the topnotchers were Hostinger Operations with a 4.8% share, Dynadot with 4.5%, and NameSilo with 3.6%.



WHOIS Data Redaction

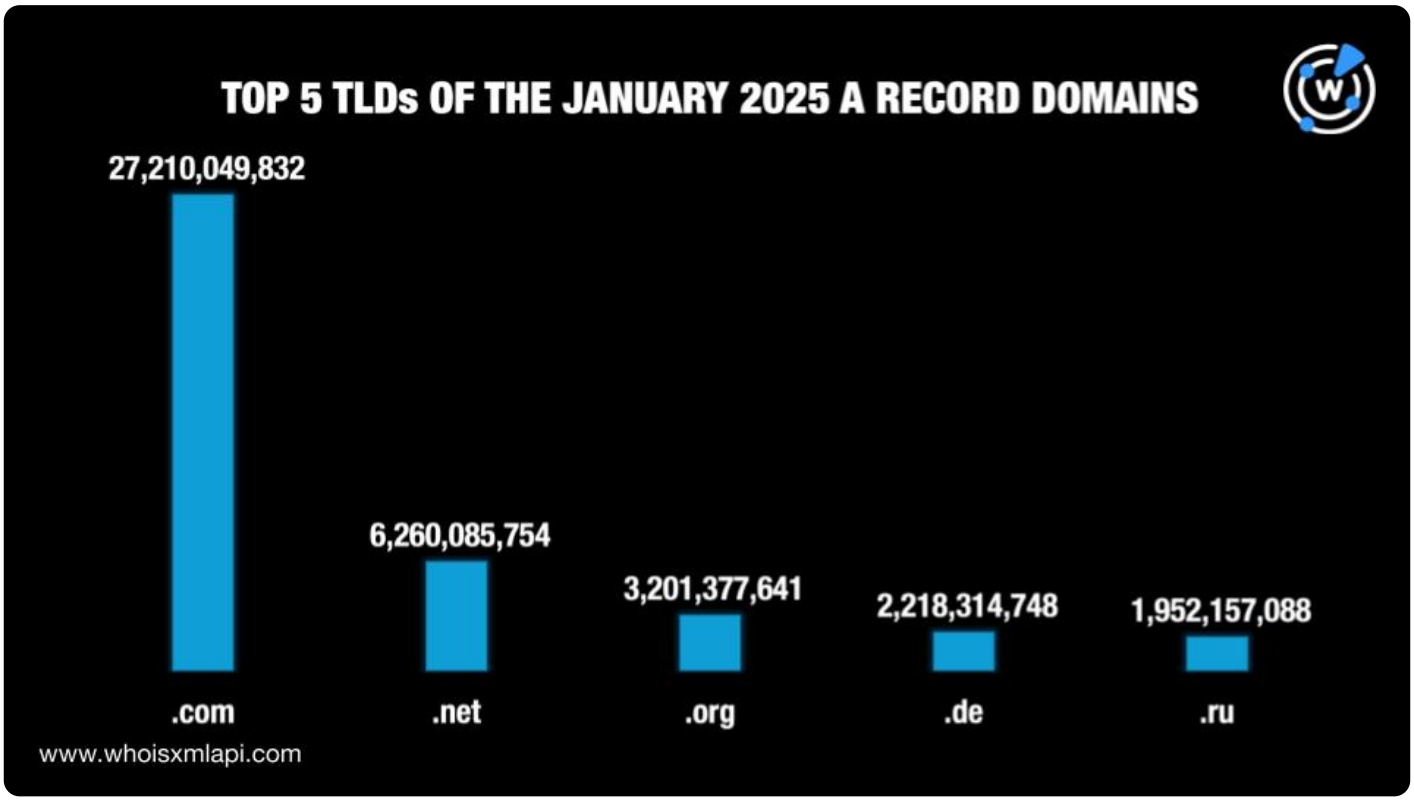
The same number of NRDs had redacted WHOIS records in January, 58.8% to be exact, compared with December. The remaining 41.2%, meanwhile, had public WHOIS records.



A Closer Look at the January 2025 DNS Records

Top TLDs of the A Record Domains

Next, we analyzed 61.2+ billion domains from our DNS database's A record full file for January 2025, which included DNS resolutions from the past 365 days. We found that 44.4% used the .com TLD, down from 45.6% in December. The rest of the top 5 comprised two other gTLDs (i.e., .net with a 10.2% share and .org with 5.2%) and two ccTLDs (i.e., .de with a 3.6% share and .ru with 3.2%).



Threat Reports

Below are the threat reports we published in January 2025.

- **More Signs of the more_eggs Backdoor Found in the DNS:** Threat actor TA4557 utilized a weaponized resume to drop a backdoor called “more_eggs” to steal victims’ credentials. WhoisXML API expanded a list of indicators of compromise (IoCs) and uncovered 768 potentially connected artifacts.

- **New Year, Old Threats: What Does the DNS Reveal about 2025?:** A WhoisXML API investigation of new year-themed threats led to the discovery of 16,086 artifacts. The researchers analyzed a sample comprising 1,000 domains that contained the text string **2025** from First Watch Malicious Domains Data Feed.

- **The MOONSHINE Exploit Kit and the DarkNimbus Backdoor in the DNS Spotlight:** The

Earth Minotaur attackers used the MOONSHINE and DarkNimbus combo to launch attacks. WhoisXML API found 463 possibly connected artifacts after expanding a list of 53 IoCs.

- **DNS Insights on a Free Form Builder Service Phishing Campaign:** Phishers harvested victims' credentials and took over their organizations' Microsoft Azure cloud infrastructure by leveraging the HubSpot Free Form Builder service. WhoisXML API expanded a list of 33 IoCs and uncovered 494 new artifacts.

- **Early Discovery and Prediction of Meduza Stealer IoCs with First Watch:** WhoisXML API selected a handful of Meduza Stealer IoCs and expanded the list using First Watch Malicious Domains Data Feed. We discovered that the malicious infrastructure could indeed be broader.

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.