# February 2025: Domain Activity Highlights

Posted on March 12, 2025

The WhoisXML API research team analyzed 7.5+ million domains registered between 1 and 28 February 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 62.1+ billion domains from our DNS database's A record full file dated 6 February 2025.

Next, we studied the top TLDs of 1.0+ million domains detected as indicators of compromise (IoCs) this February.

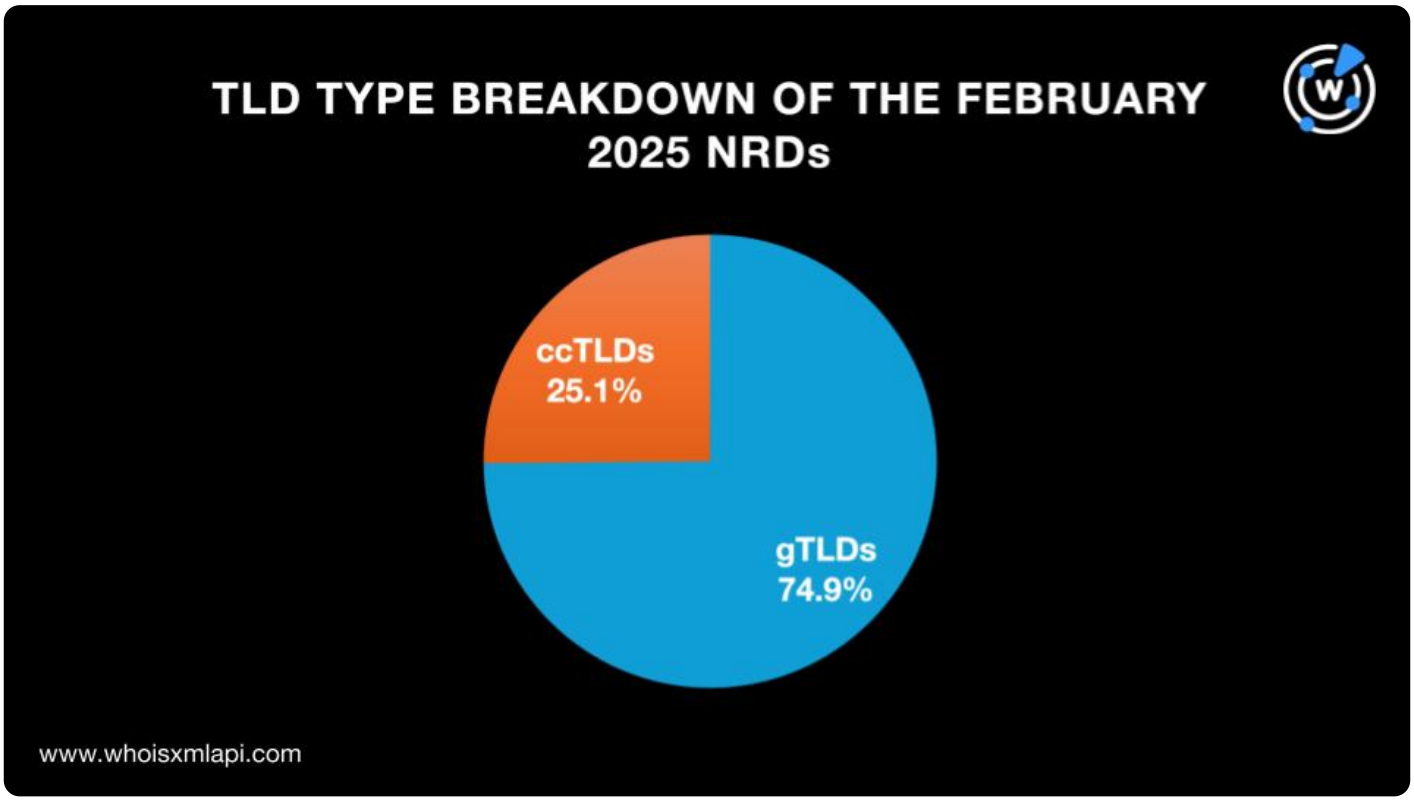
Finally, we summed up our findings and provided links to the threat reports produced using DNS, IP, and domain intelligence sources during the period.

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

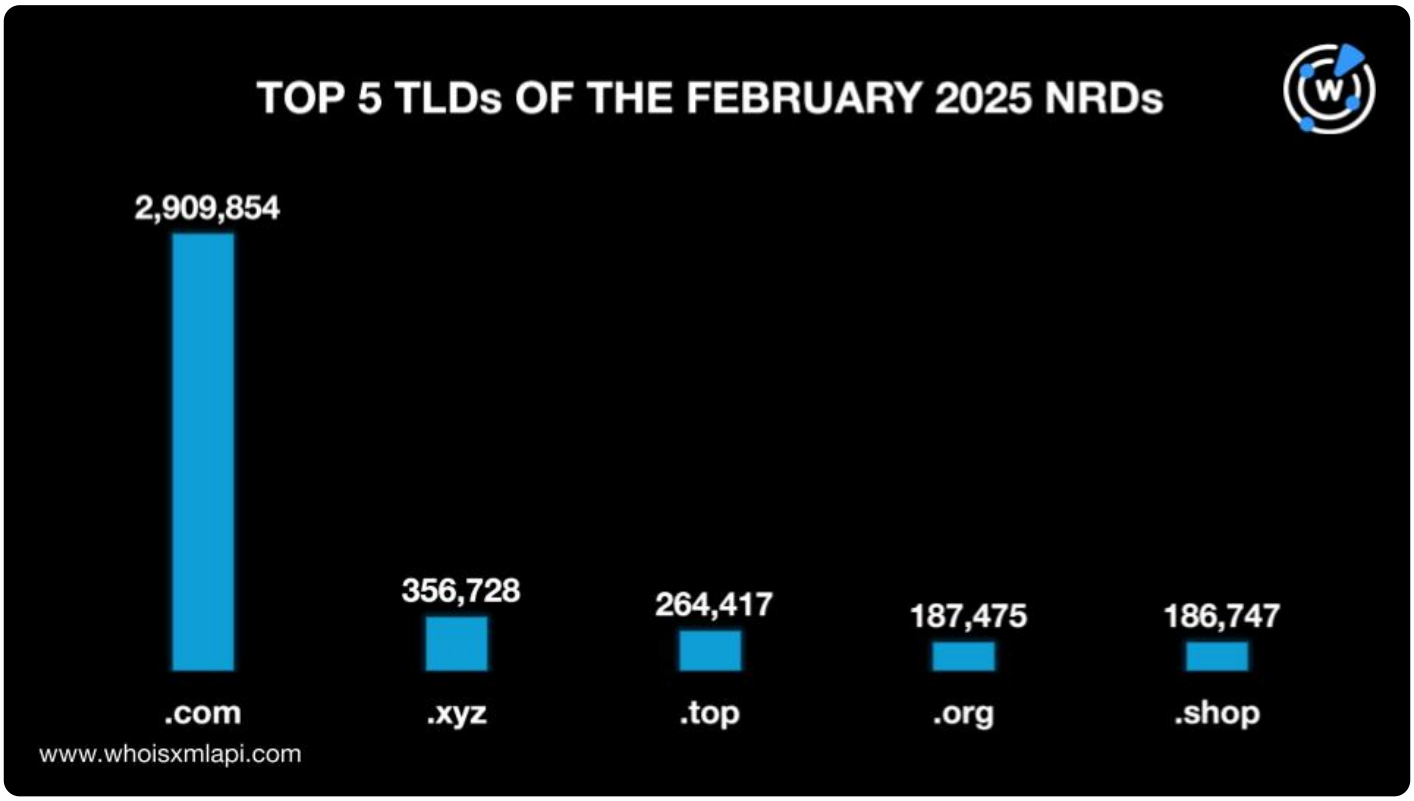
## Zooming in on the February 2025 NRDs

### TLD Distribution

A majority of the 7.5+ million domains registered in February 2025, 74.9% to be exact, used generic TLD (gTLD) extensions, while the remaining 25.1% used country-code TLD (ccTLD) extensions.

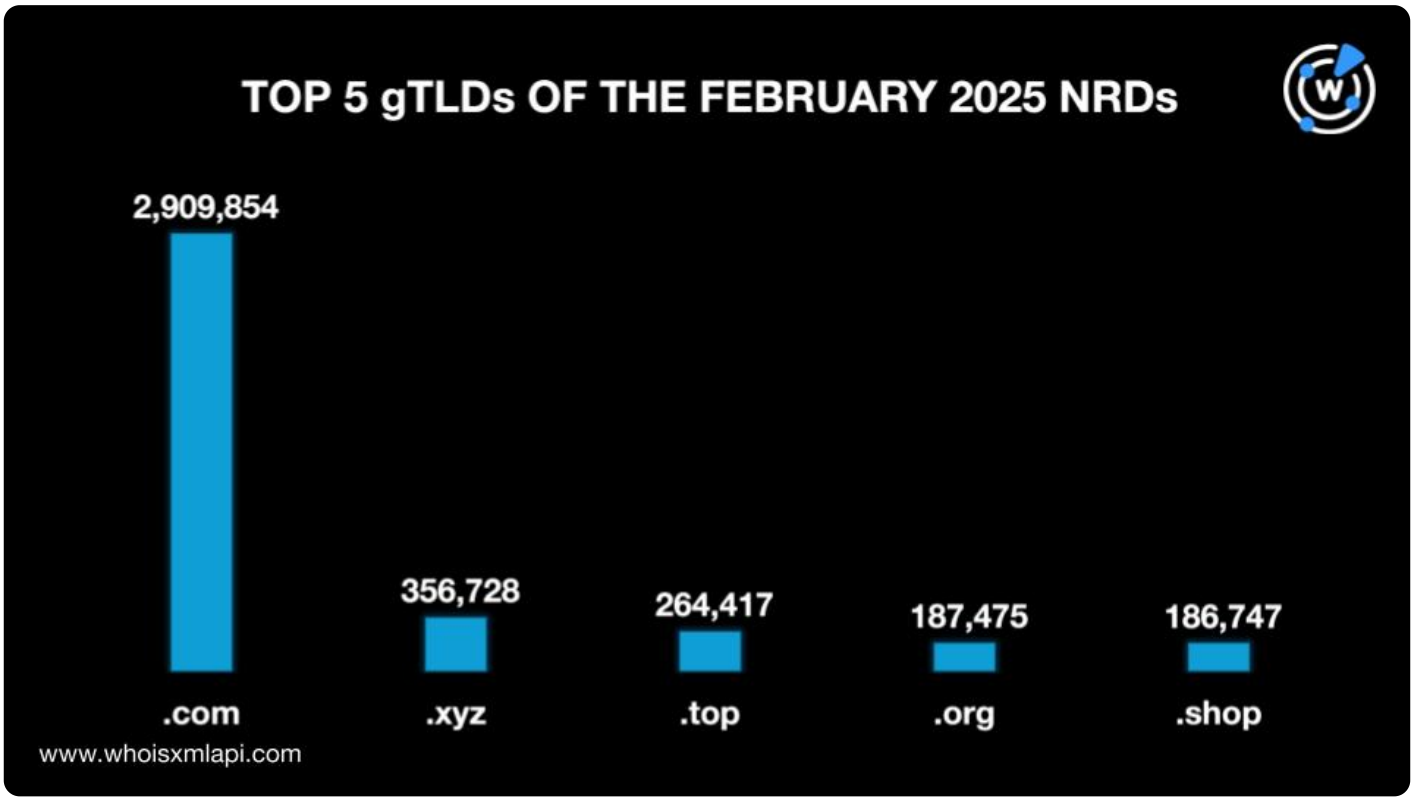



The .com TLD remained the most popular extension used by 38.4% of the total number of newly registered domains (NRDs), down slightly from 38.9% in January. The other most used TLDs on the top 5 followed with a significant gap as in the previous month. Four other gTLDs, namely, .xyz with a 4.7% share, .top with 3.5%, and .org and .shop with 2.5% each, completed the roster.

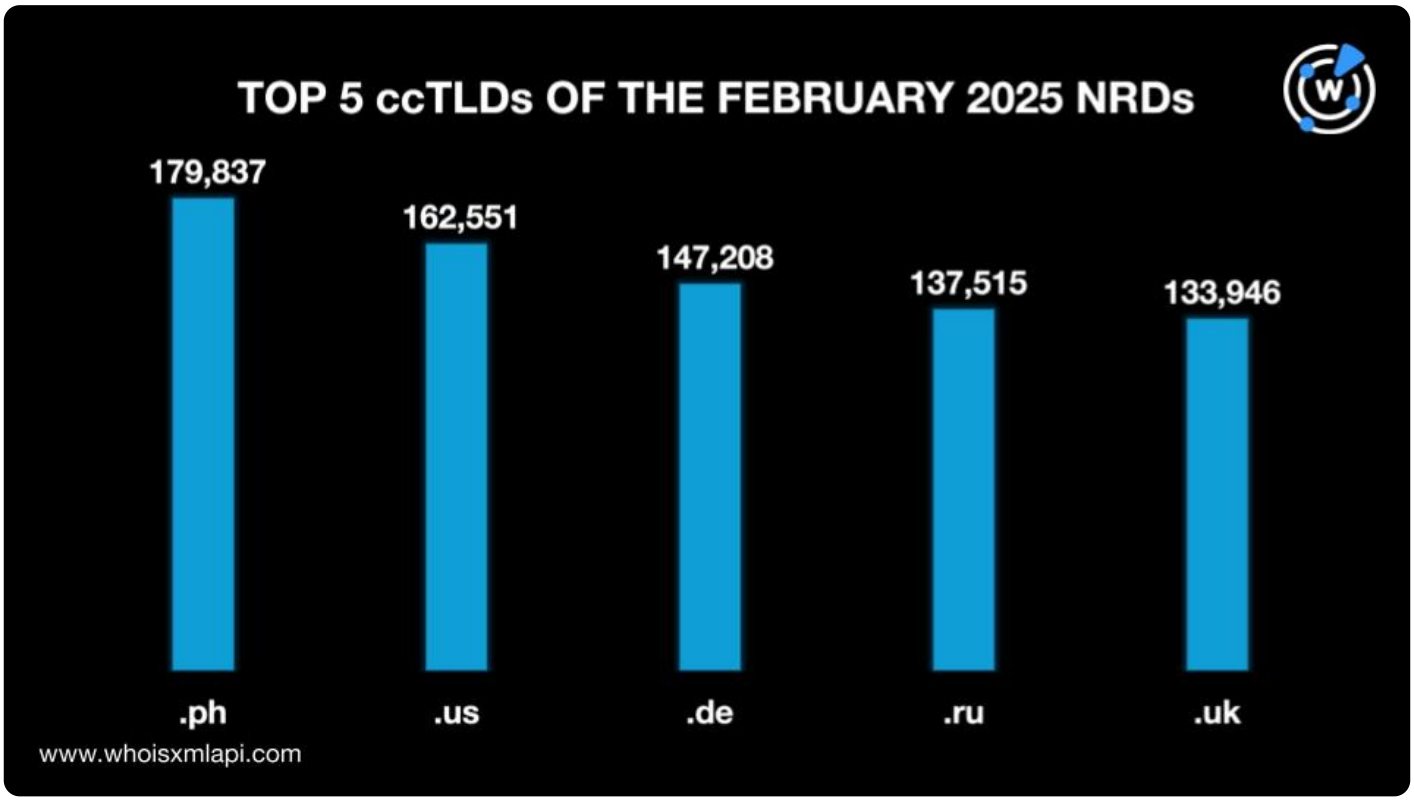



We then analyzed the February TLDs further to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 627 gTLDs, .com remained the most used, accounting for a 51.2% share, up from 50.5% in January. The rest of the top 5 lagged far behind. In fact, the four other gTLDs only clocked in a 17.5% share in total. The .xyz gTLD had a 6.3% share, .top had 4.7%, and .org and .shop had 3.3% each.

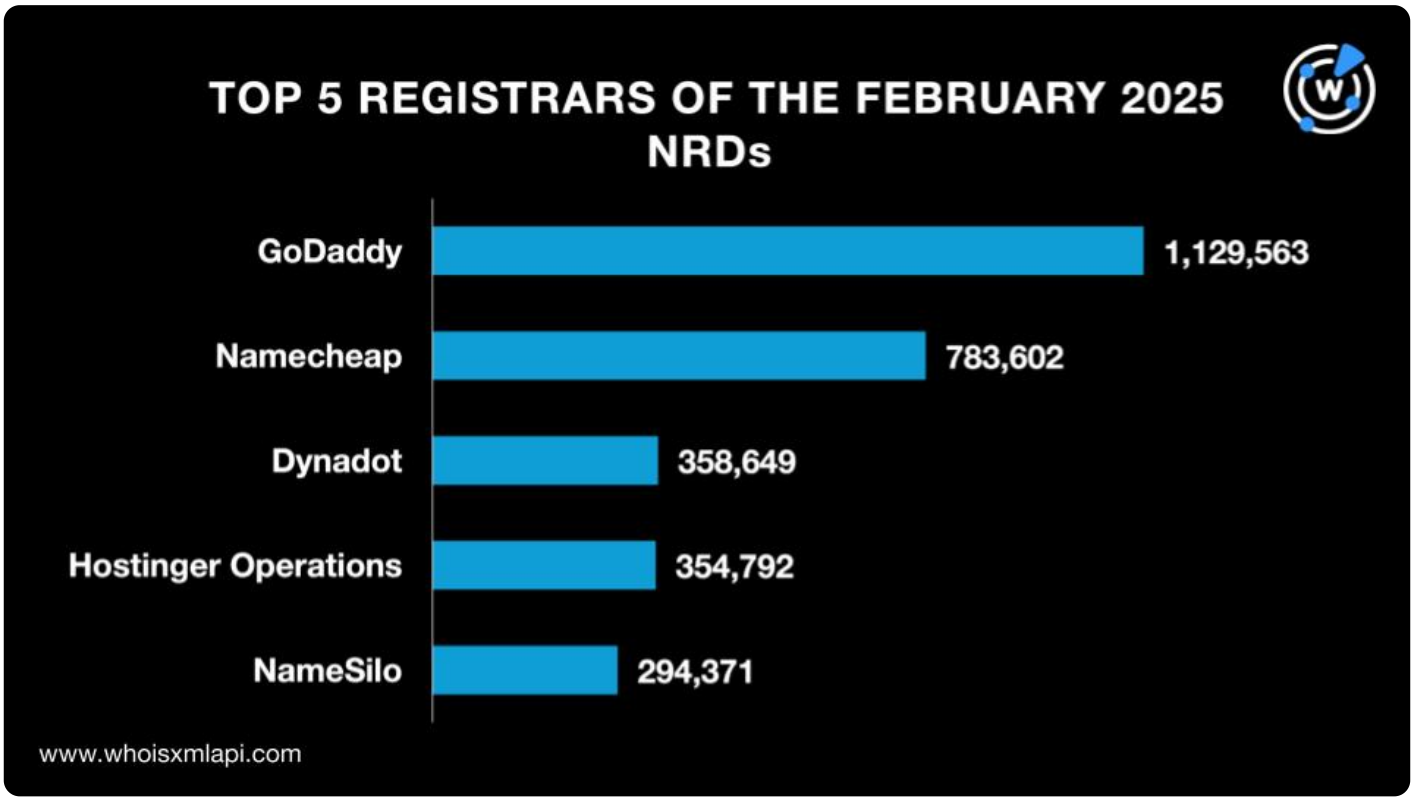



Meanwhile, .ph ousted last month's top ccTLD .de. Out of 250 ccTLD extensions, .ph came in with a 9.4% share. The remaining ccTLDs were .us with an 8.5% share, .de with 7.7%, .ru with 7.2%, and .uk with 7.0%.



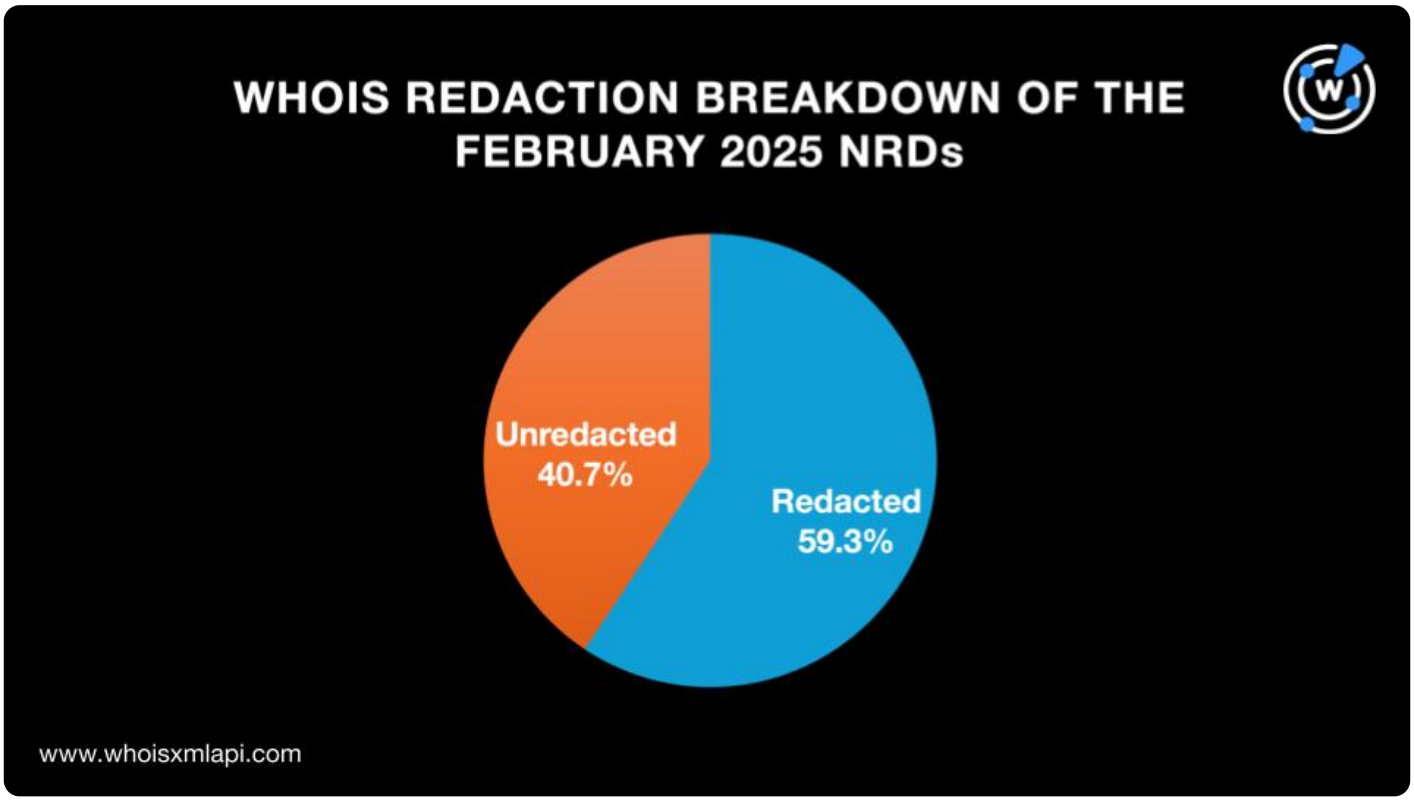

## Registrar Distribution

GoDaddy continued to reign supreme among the registrars with a 14.9% share, down from 15.4% in January. Namecheap took the second spot with a 10.3% share. The rest of the topnotchers were Dynadot and Hostinger Operations with a 4.7% share each and NameSilo with 3.9%.




## WHOIS Data Redaction

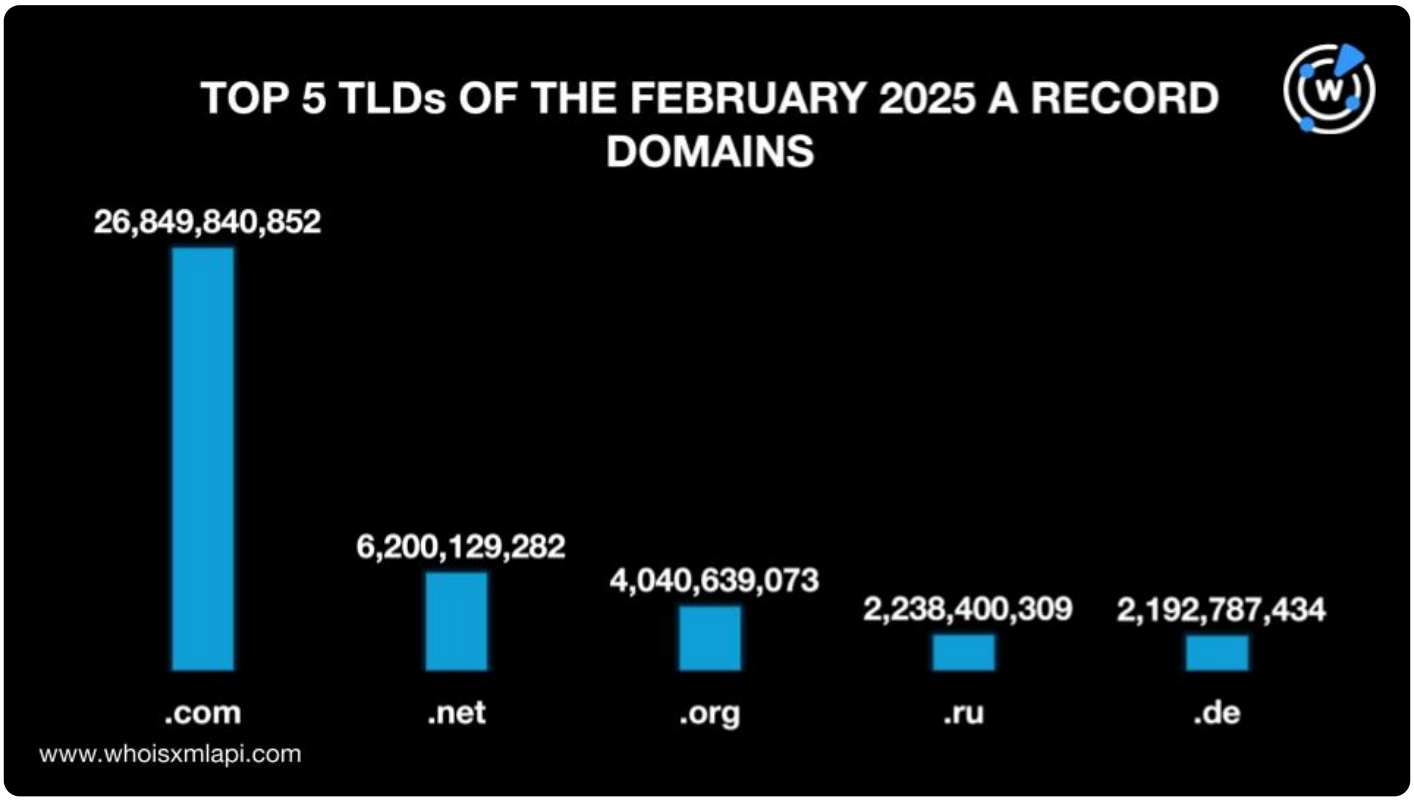
More NRDs had redacted WHOIS records in February, 59.3% to be exact, up from 58.8% in January. The remaining 40.7%, meanwhile, had public WHOIS records.




# A Closer Look at the February 2025 DNS Records

## Top TLDs of the A Record Domains

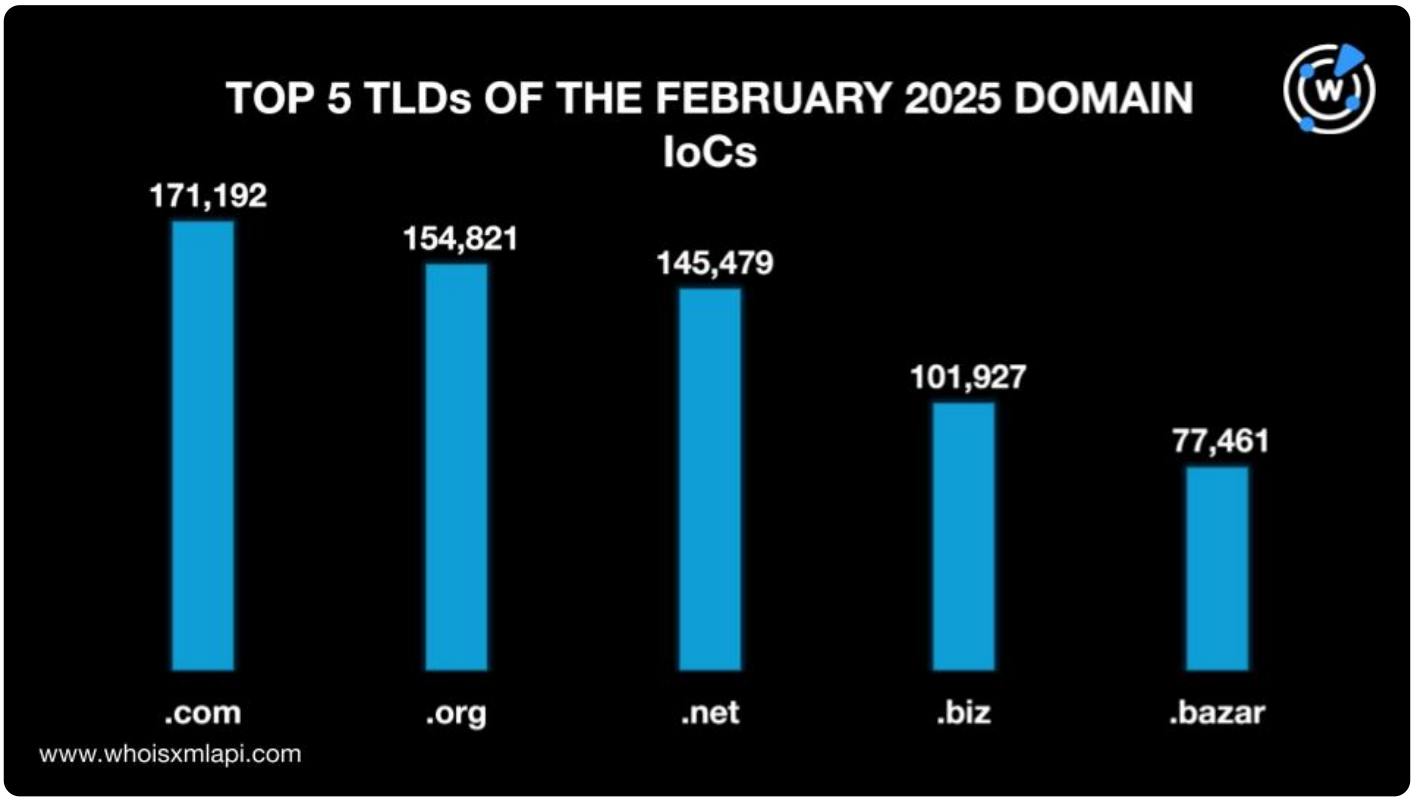
Next, we analyzed 62.1+ billion domains from our DNS database's A record full file dated 6 February 2025, which included DNS resolutions from the past 365 days. We found that 43.2% used the .com TLD, down from 44.4% in January. The rest of the top 5 comprised two other gTLDs (i.e., .net with a 10.0% share and .org with 6.5%) and two ccTLDs (i.e., .ru with a 3.6% share and .de with 3.5%).




## Cybersecurity through the DNS Lens

### Top TLDs of the February 2025 Domain IoCs

As usual, we analyzed 1.0+ million domains tagged as IoCs for various threats detected in February. Our analysis revealed that .com remained the most popular TLD with a 16.8% share. The remaining top TLDs were all gTLDs as well, namely, .org with a 15.2% share, .net with 14.3%, .biz with 10.0%, and .bazar with 7.6%.




## Threat Reports

Below are the threat reports we published in February 2025.

- **DNS Deep Dive: Peeking into Back Doors to Abandoned but Live Backdoors:** Backdoors let threat actors bypass a target organization's normal authentication mechanisms. Most steal sensitive information and send it to command-and-control (C&C) servers, typically domains under the attackers' control. And when former owners (i.e., threat actor) leave these C&C servers behind, they can remain operational and accessed by other threat actors. Security researchers identified 34 domains as IoCs for such a threat, which WhoisXML API expanded. We uncovered 1,360+ connected artifacts.

- **Illuminating Lumma Stealer DNS Facts and Findings:** Popular malware-as-a-service (MaaS) offering Lumma Stealer was employed to target victims in Argentina, Colombia, the U.S., the Philippines, and several other countries worldwide. The threat actors used fake

CAPTCHAs to deliver the malware. Cybersecurity researchers identified 34 IoCs, which WhoisXML API dove deeper into.

- **DNS Spotlight: Rockstar2FA Shuts Down, FlowerStorm Starts Up:** It's not unusual for threat actors to take over fellow criminals' existing infrastructure. ZeuS's original operator allegedly sold the malware's infrastructure to another actor who eventually turned it into SpyEye. Rockstar2FA followed the same fate—taking on a new life in FlowerStorm. WhoisXML API expanded a list of 190 FlowerStorm IoCs and uncovered other connected artifacts.

- **Unloading MintsLoader IoCs Using DNS Intelligence:** A sophisticated campaign leveraging MintsLoader targeted critical infrastructure and legal firms across the U.S. and Europe. Building on the 61 IoCs identified by threat researchers at eSentire, WhoisXML API WhoisXML API research team utilized our comprehensive DNS intelligence and uncovered additional artifacts.

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.***