March 2025: Domain Activity Highlights

Posted on April 9, 2025

The WhoisXML API research team analyzed 8.2+ million domains registered between 1 and 31 March 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 59.2+ billion domains from our DNS database's A record full file dated 6 March 2025.

Next, we studied the top TLDs of 1.1+ million domains detected as indicators of compromise (IoCs) this March.

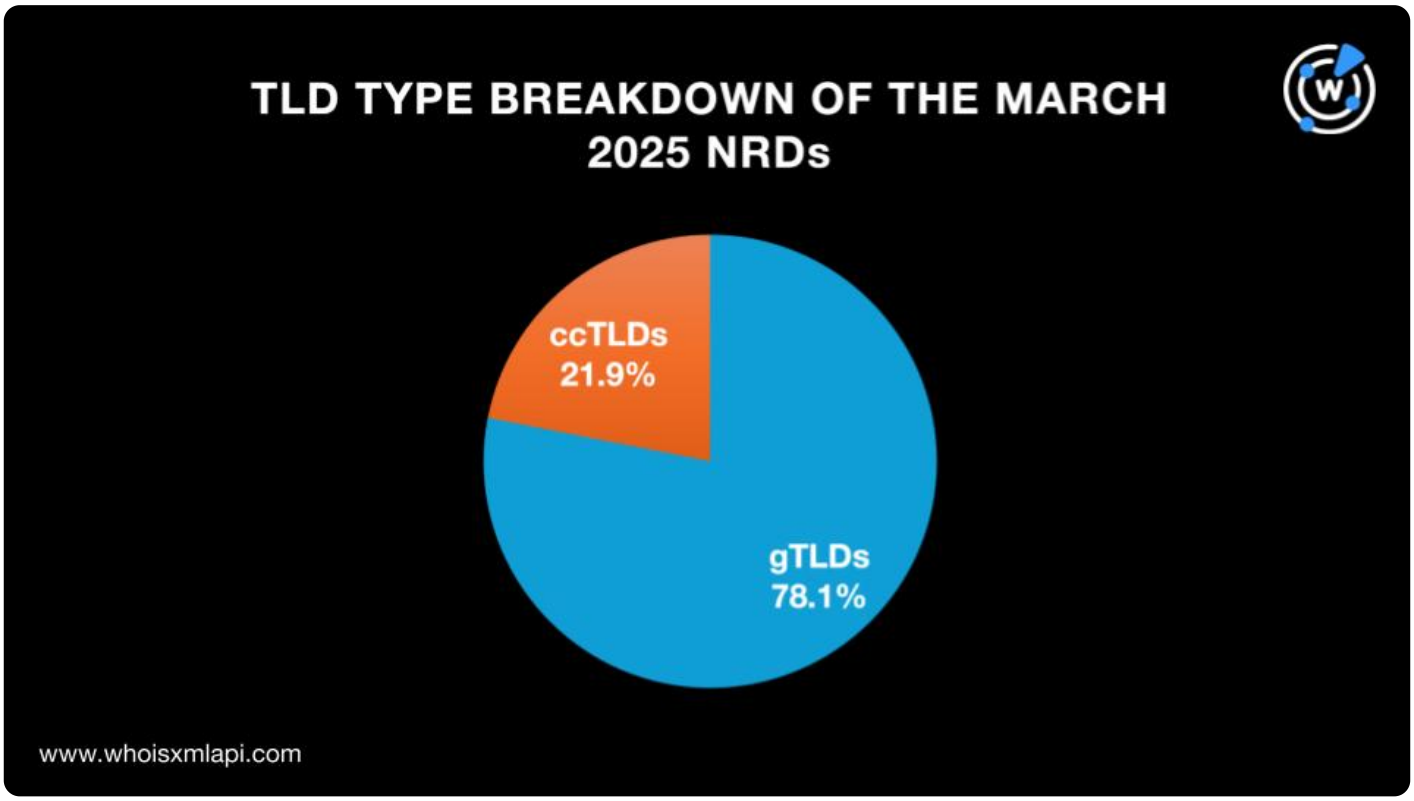
Finally, we summed up our findings and provided links to the threat reports produced using DNS, IP, and domain intelligence sources during the period.

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

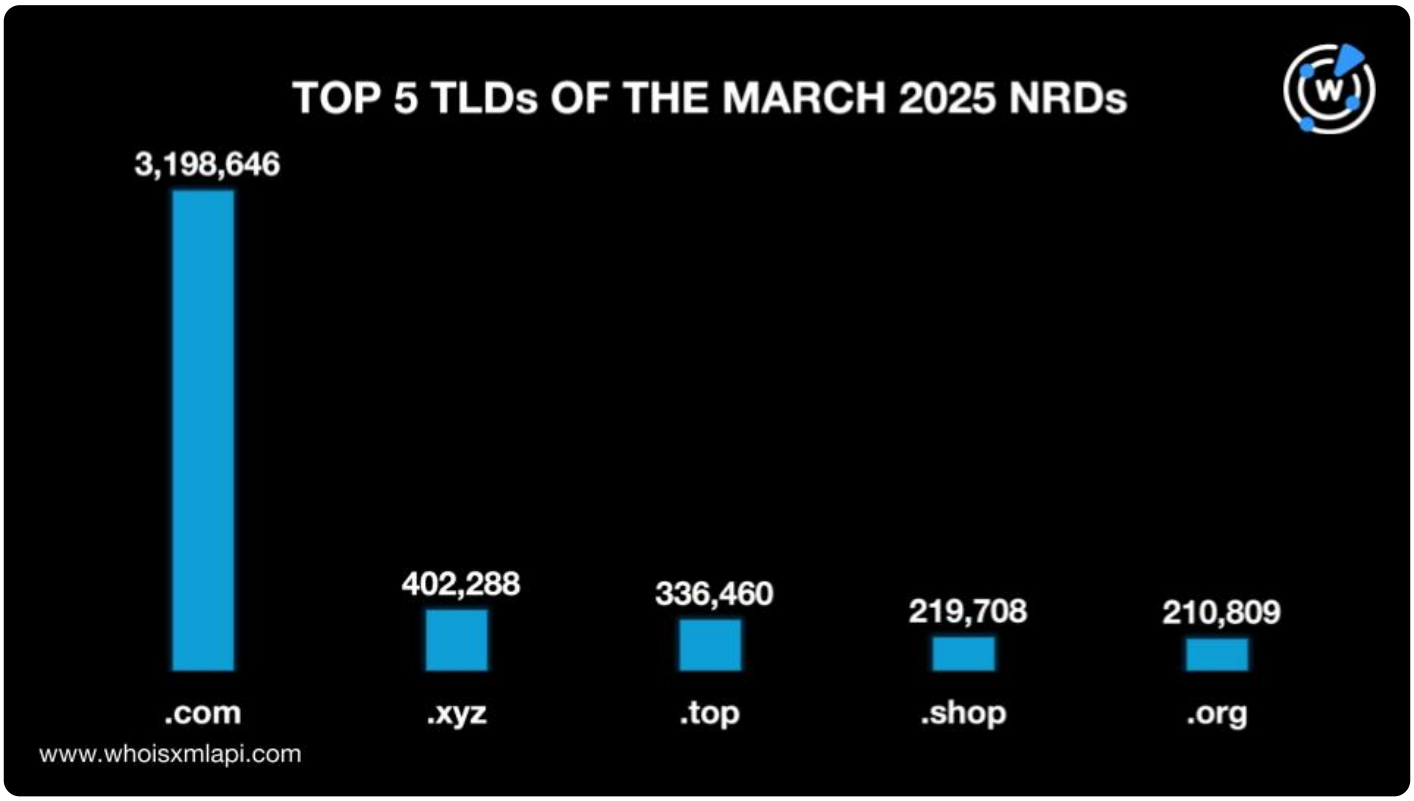
Zooming in on the March 2025 NRDs

TLD Distribution

A majority of the 8.2+ million domains registered in March 2025, 78.1% to be exact, used generic TLD (gTLD) extensions, while the remaining 21.9% used country-code TLD (ccTLD) extensions.

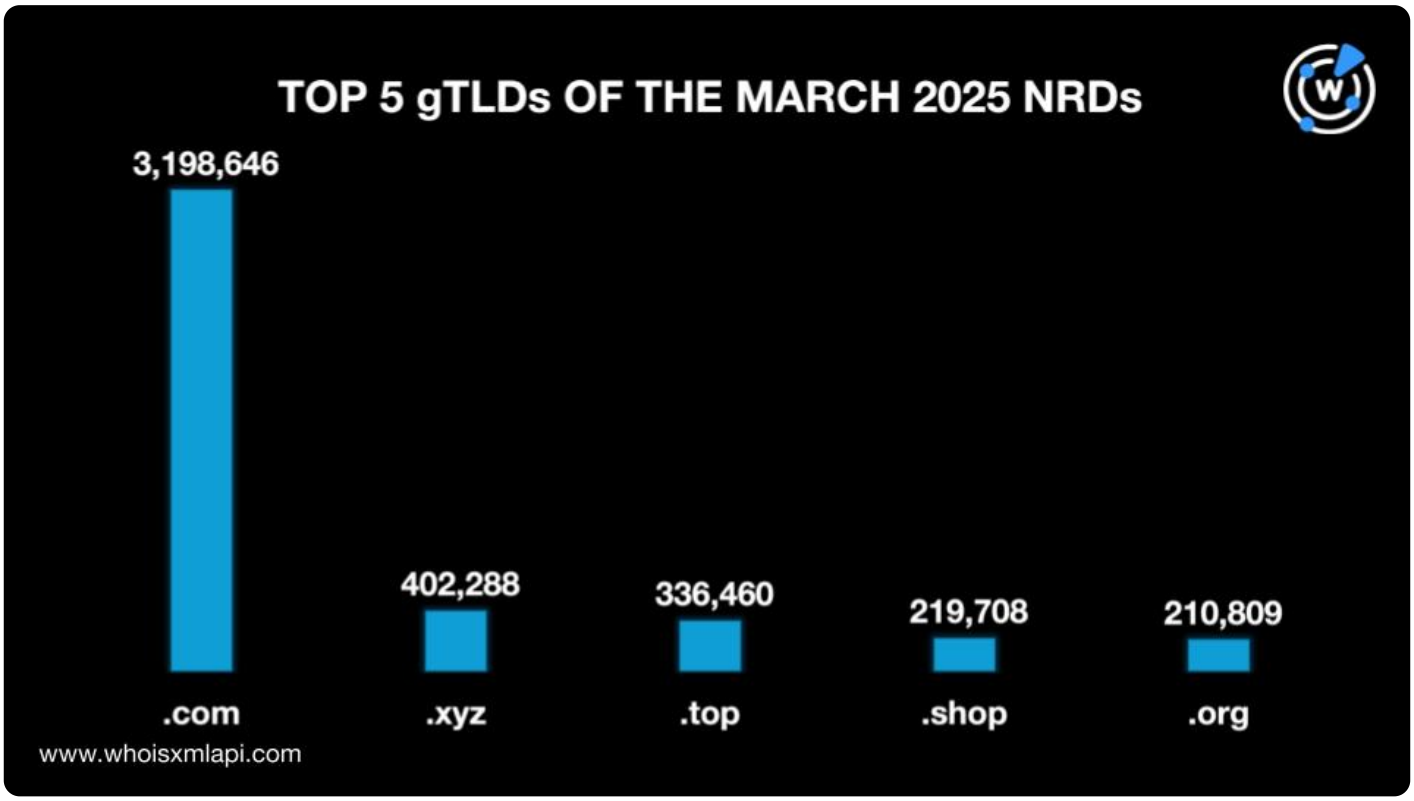


The .com TLD remained the most popular extension used by 38.9% of the total number of newly registered domains (NRDs), up very slightly from 38.4% in February. The other most used TLDs on the top 5 followed with a significant gap as in the previous month. Four other gTLDs, namely, .xyz with a 4.9% share, .top with 4.1%, .shop with 2.7%, and .org with 2.6%, completed the roster.

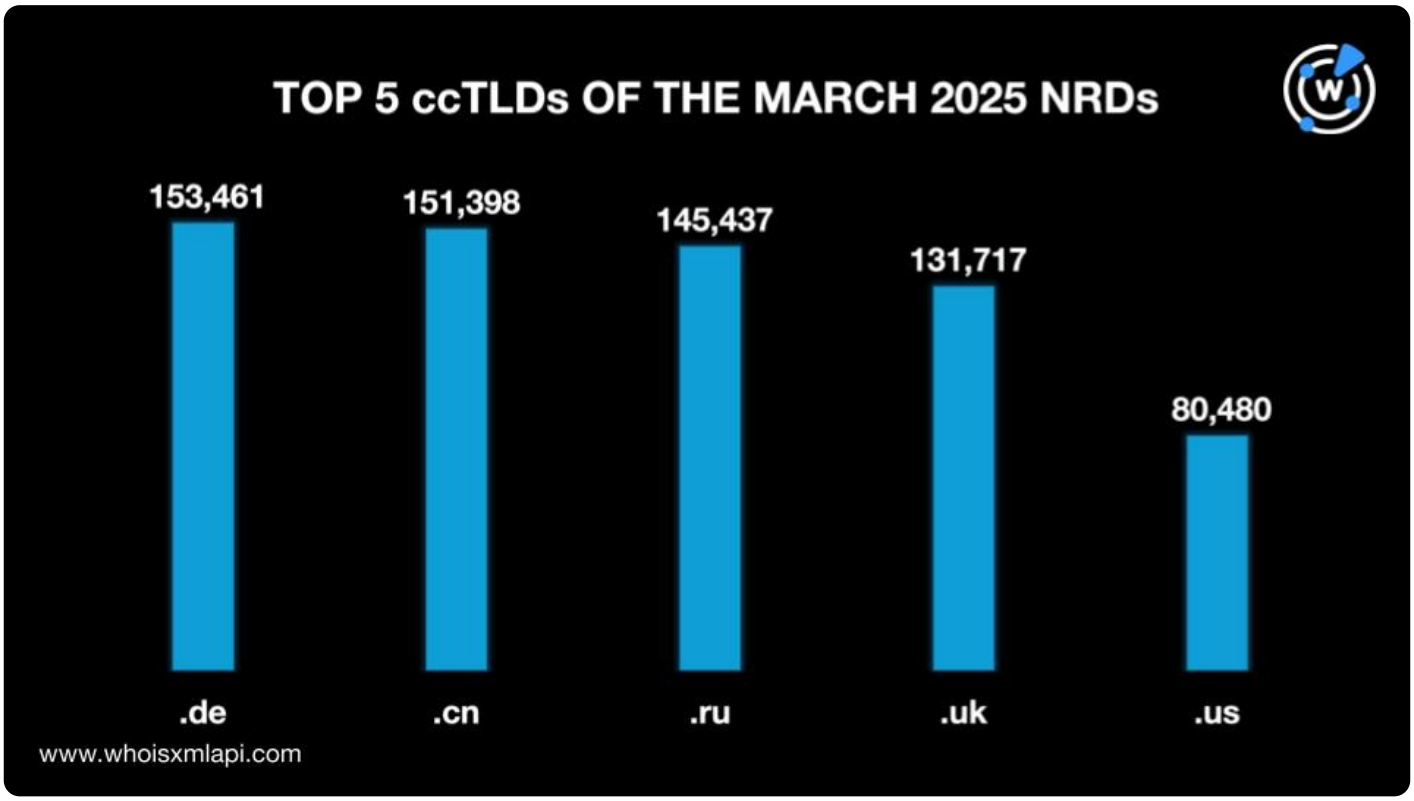


We then analyzed the March TLDs further to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 617 gTLDs, .com remained the most used, accounting for a 49.9% share, down from 51.2% in February. The rest of the top 5 lagged far behind. In fact, the four other gTLDs only clocked in an 18.2% share in total. The four remaining gTLDs were .xyz with a 6.3% share, .top with 5.2%, .shop with 3.4%, and .org with 3.3%.

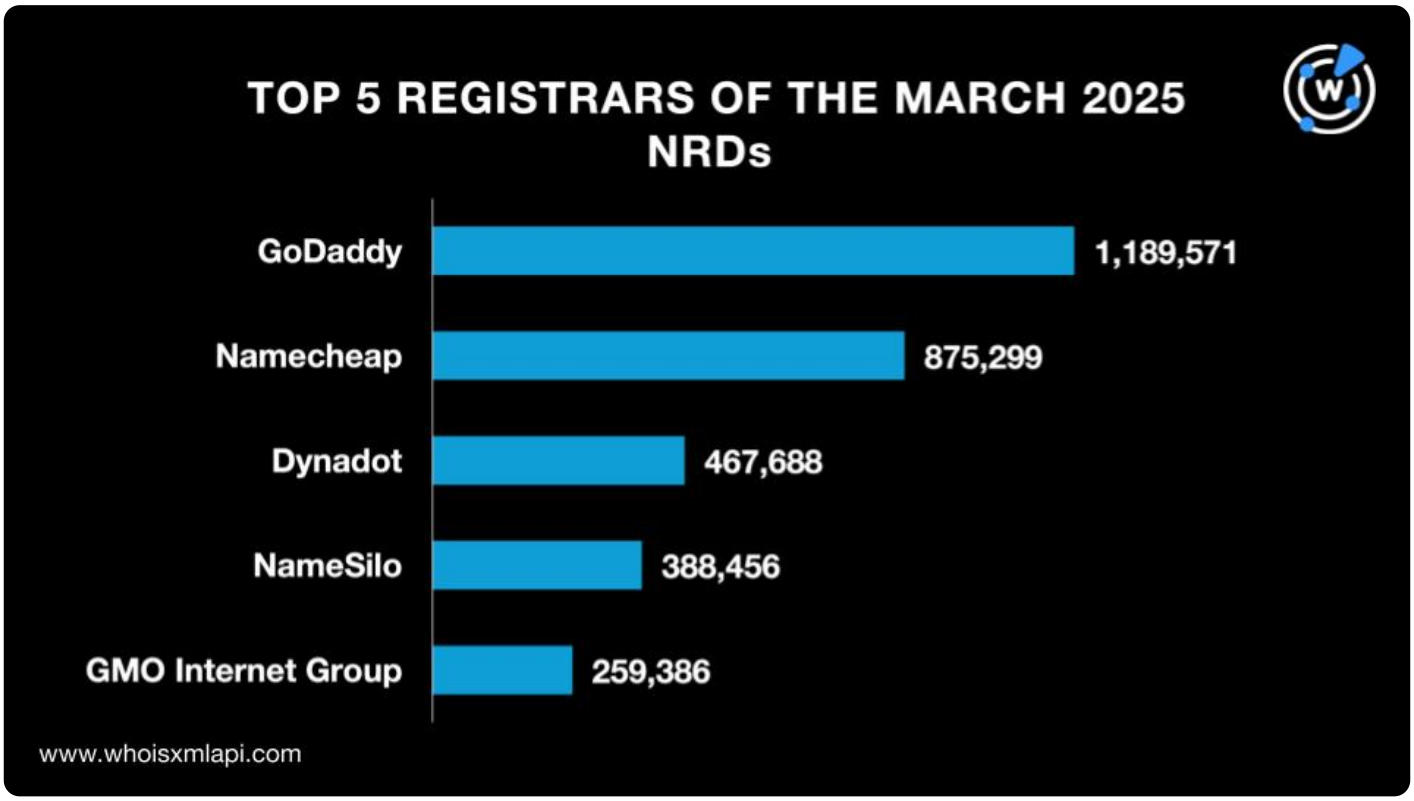


Meanwhile, .ph dropped out of the top 5 roster compared with February 2025. Out of 250 ccTLD extensions, .de took the top spot with an 8.5% share. The .cn ccTLD followed with an 8.4% share. Then came .ru with an 8.1% share, .uk with 7.3%, and .us with 4.5%.



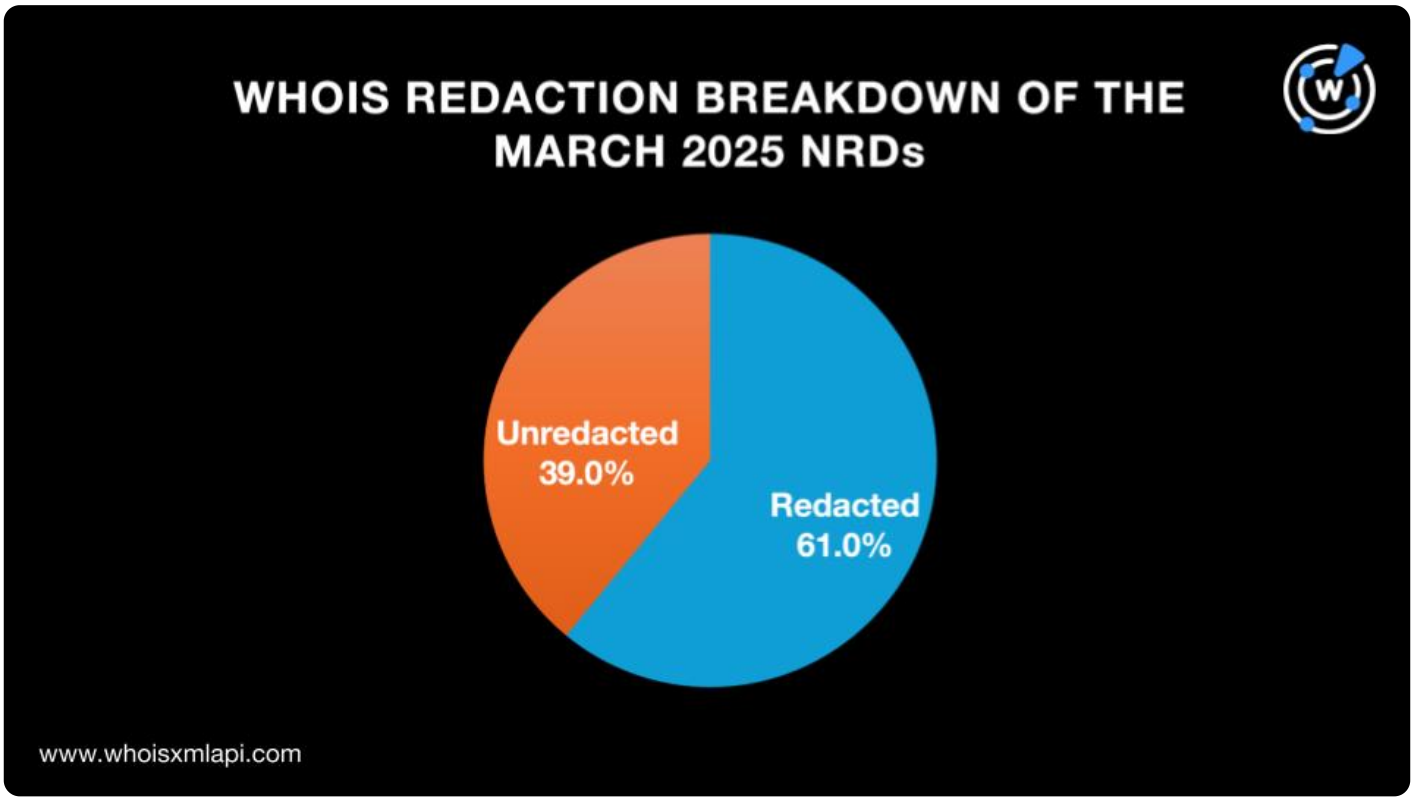
Registrar Distribution

GoDaddy continued to reign supreme among the registrars with a 14.5% share, down slightly from 14.9% in February. Namecheap took the second spot with a 10.7% share. The rest of the topnotchers were Dynadot with a 5.7% share, NameSilo with 4.7%, and GMO Internet Group with 3.2%.



WHOIS Data Redaction

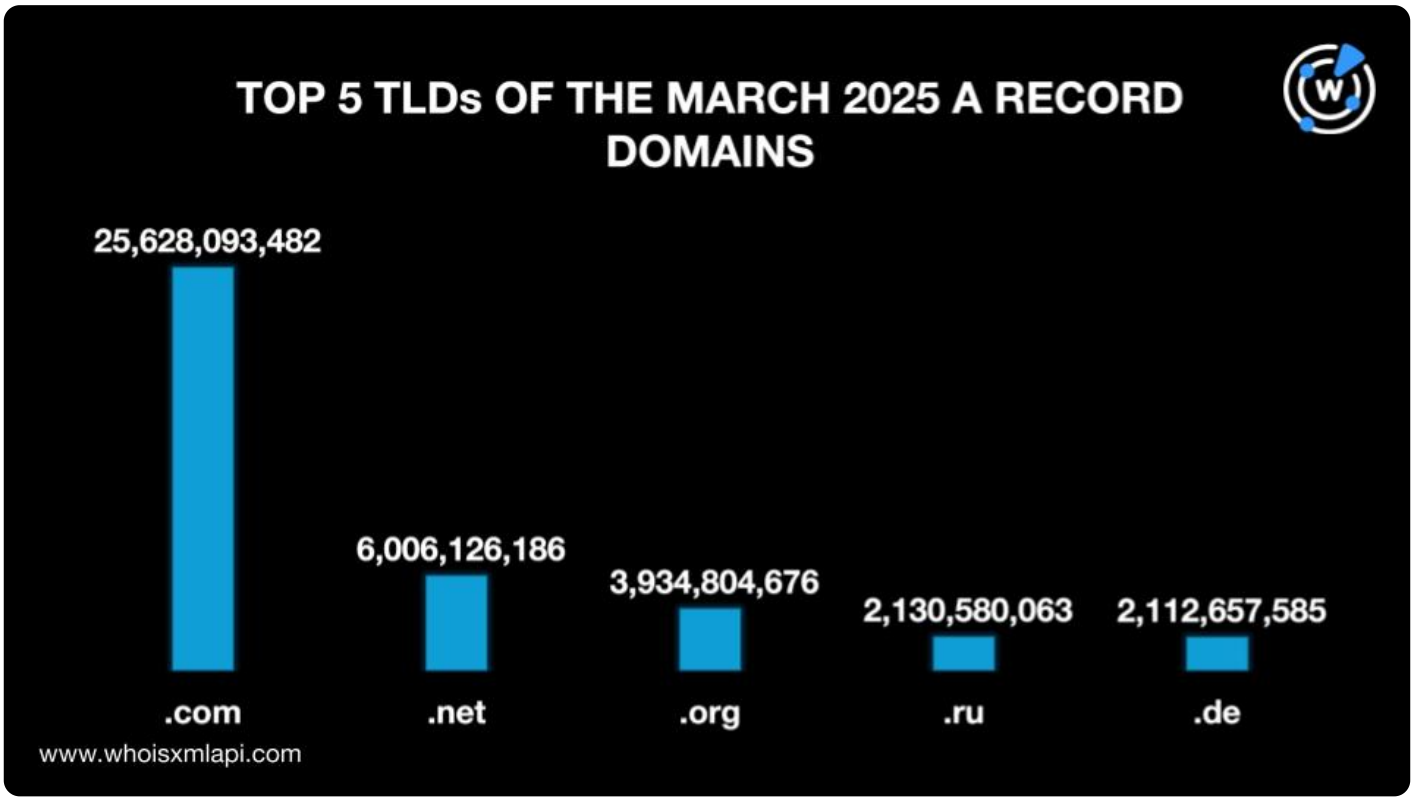
More NRDs had redacted WHOIS records in March, 61.0% to be exact, up from 59.3% in February. The remaining 39.0%, meanwhile, had public WHOIS records.



A Closer Look at the March 2025 DNS Records

Top TLDs of the A Record Domains

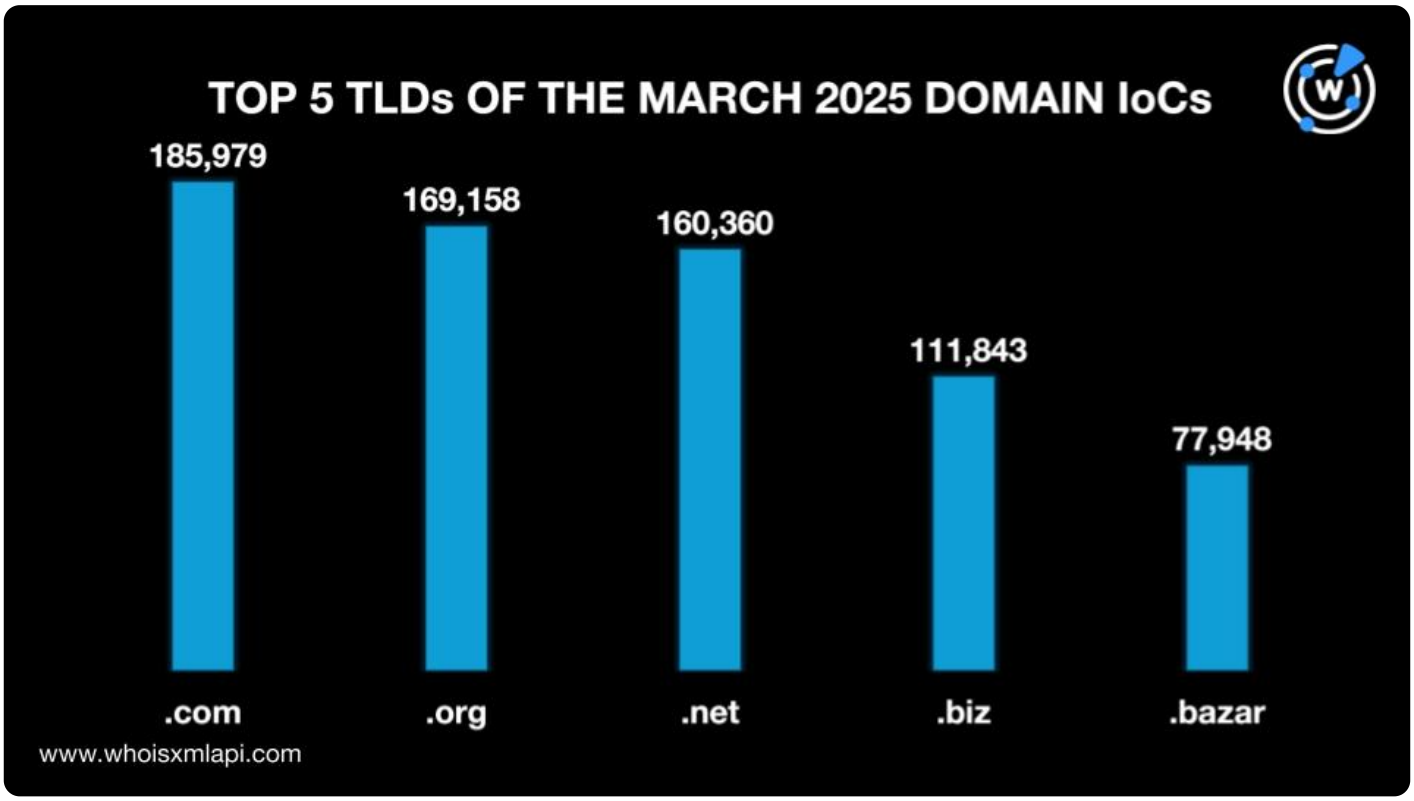
Next, we analyzed 59.2+ billion domains from our DNS database's A record full file dated 6 March 2025, which included DNS resolutions from the past 365 days. We found that 43.3% used the .com TLD, up very slightly from 43.2% in February. The rest of the top 5 comprised two other gTLDs (i.e., .net with a 10.1% share and .org with 6.6%) and two ccTLDs (i.e., .ru and .de with a 3.6% share each).



Cybersecurity through the DNS Lens

Top TLDs of the March 2025 Domain IoCs

As usual, we analyzed 1.1+ million domains tagged as IoCs for various threats detected in March. 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 14.5%, .biz with 10.1%, and .bazar with 7.0%.



Threat Reports

Below are the threat reports we published in March 2025.

- **Sneaking a Peek into the Inner DNS Workings of Sneaky 2FA:** Phishing-as-a-service (PhaaS) offering Sneaky 2FA figured in an adversary-in-the-middle (AitM) attack targeting Microsoft 365 users. Jumping off 61 IoCs, we uncovered 890+ possibly connected artifacts.
- **A DNS Investigation of SEO Manipulation via Bad Seed BadIIS:** A search engine optimization (SEO) manipulation campaign dubbed "BadIIS" trailed its sights on Internet Information Services (IIS) users. A report identified 51 IoCs, which we further analyzed, leading to the discovery of 2,280 other artifacts.
- **Malicious Ads Targeting Advertisers in the DNS Spotlight:** Researchers identified 97 domains as IoCs related to a new attack targeting Microsoft advertisers. The threat actors

used malicious Google ads to steal the login information of users of Microsoft's advertising platform. We unearthed 1,120+ potentially connected artifacts.

- **Igniting a DNS Spark to Investigate the Inner Workings of SparkCat:** A recent investigation led to the discovery of Android and iOS apps laced with a malicious software development kit (SDK) dubbed "SparkCat." Five IoCs were named, to which we added 790 other artifacts.

- **DNS Deep Diving into 2025's Up and Coming Ransomware Families:** A report named 10 of the most active ransomware families in 2024 that are likely to make it big in 2025. We expanded the IoC lists for RansomHub, LockBit 3.0, Play, Akira, Hunters, Medusa, BlackBasta, Qilin, BianLian, and INC. Ransom (aka Lynx) and discovered 2,380+ new 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.