April 2025: Domain Activity Highlights

Posted on May 12, 2025

The WhoisXML API research team analyzed 7.6+ million domains registered between 1 and 30 April 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 55.8+ billion domains from our DNS database's A record full file dated 3 April 2025.

Next, we studied the top TLDs of 1.5+ million domains detected as indicators of compromise (IoCs) this April.

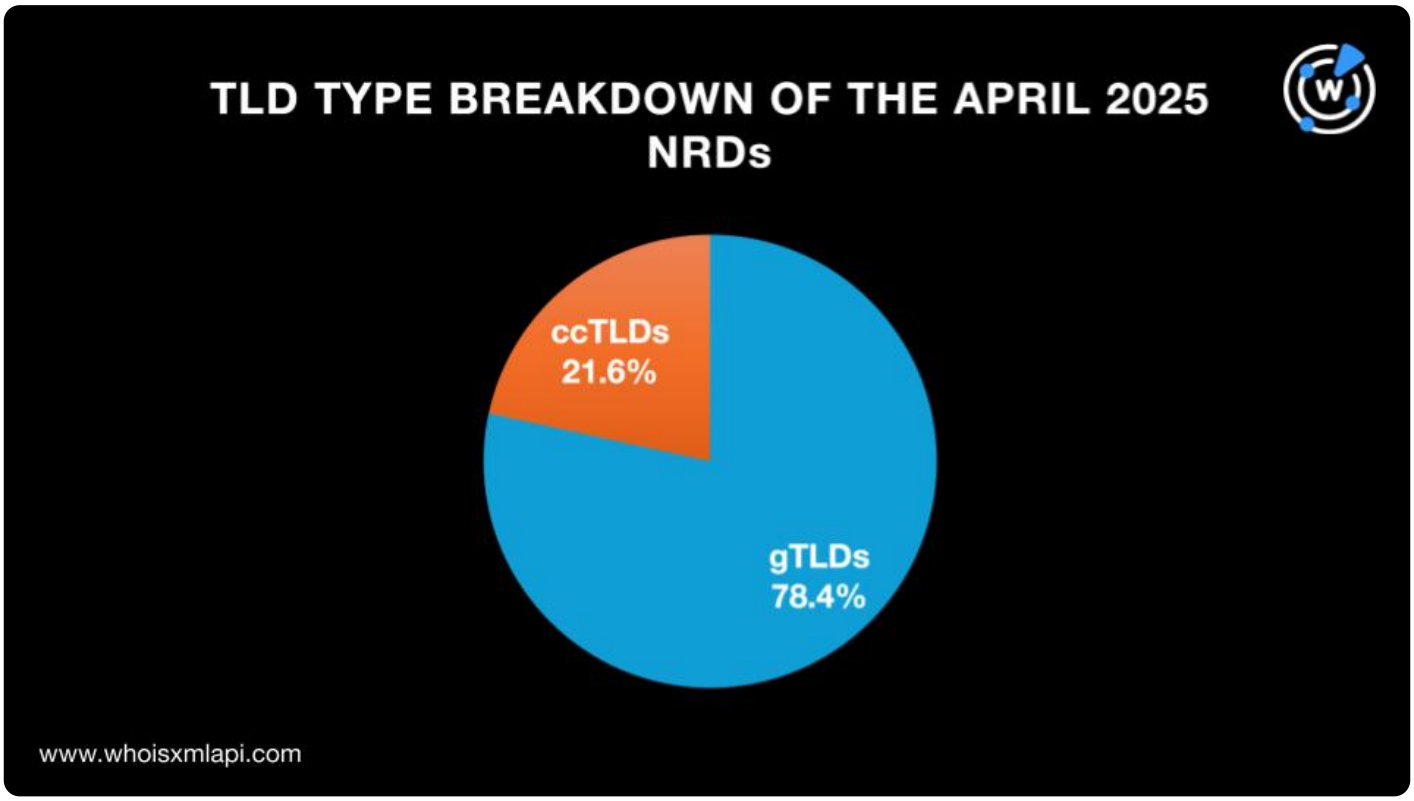
Finally, we summed up our findings and provided links to the threat reports produced using DNS, IP, and domain intelligence sources during the period.

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

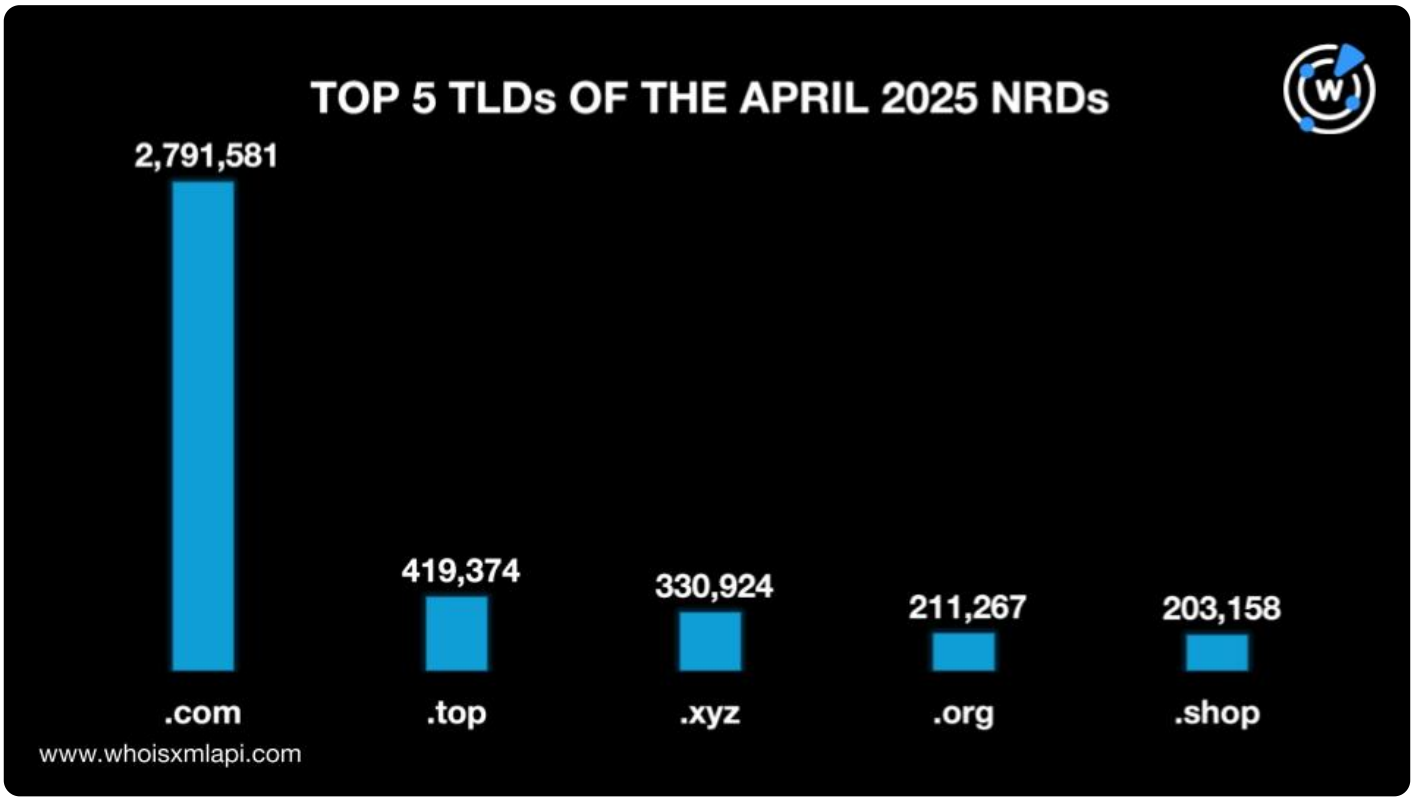
Zooming in on the April 2025 NRDs

TLD Distribution

A majority of the 7.6+ million domains registered in April 2025, 78.4% to be exact, used generic TLD (gTLD) extensions, while the remaining 21.6% used country-code TLD (ccTLD) extensions.

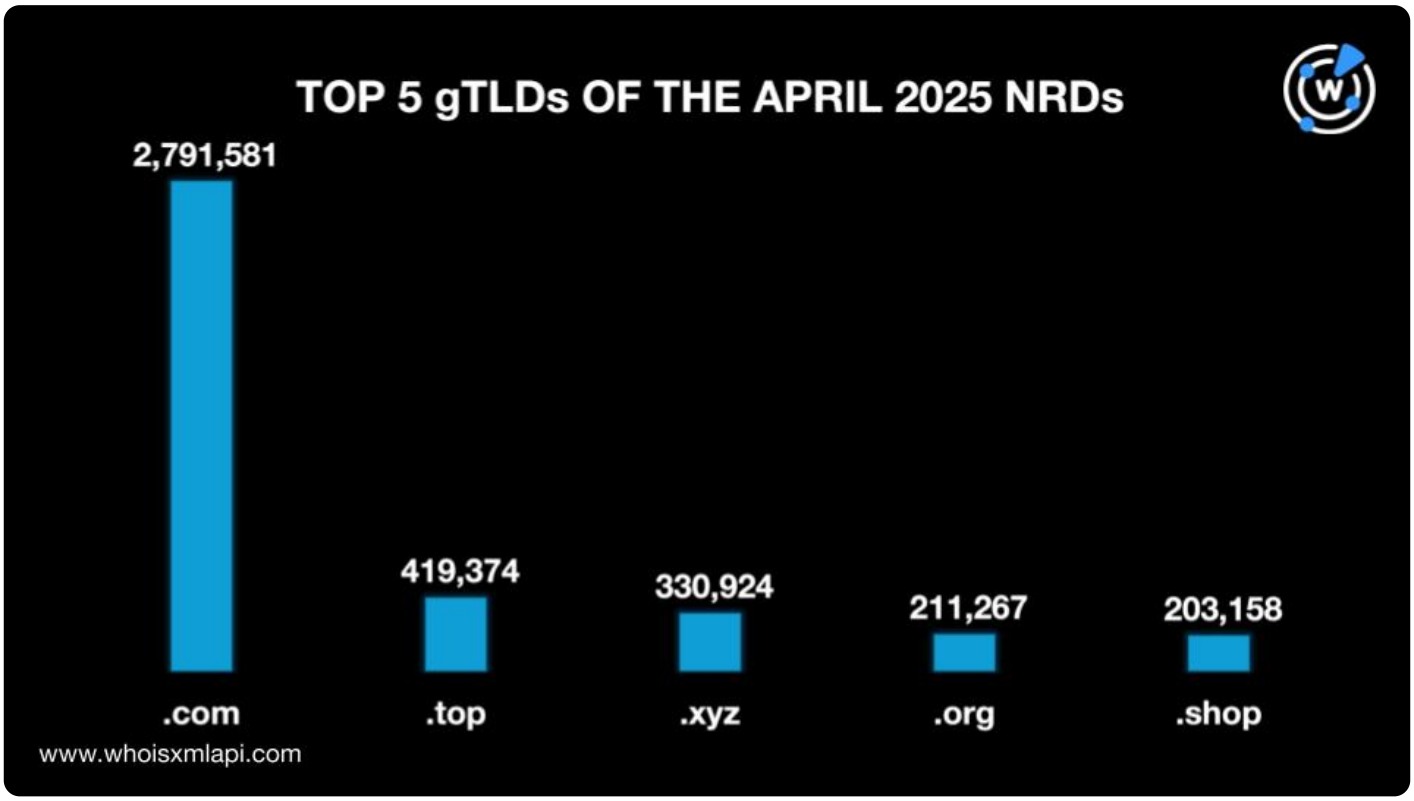


The .com TLD remained the most popular extension used by 36.5% of the total number of newly registered domains (NRDs), down from 38.9% in March. The other most used TLDs on the top 5 followed with a significant gap as in the previous month. Four other gTLDs, namely, .top with a 5.5% share, .xyz with 4.3%, .org with 2.8%, and .shop with 2.7%, completed the roster.

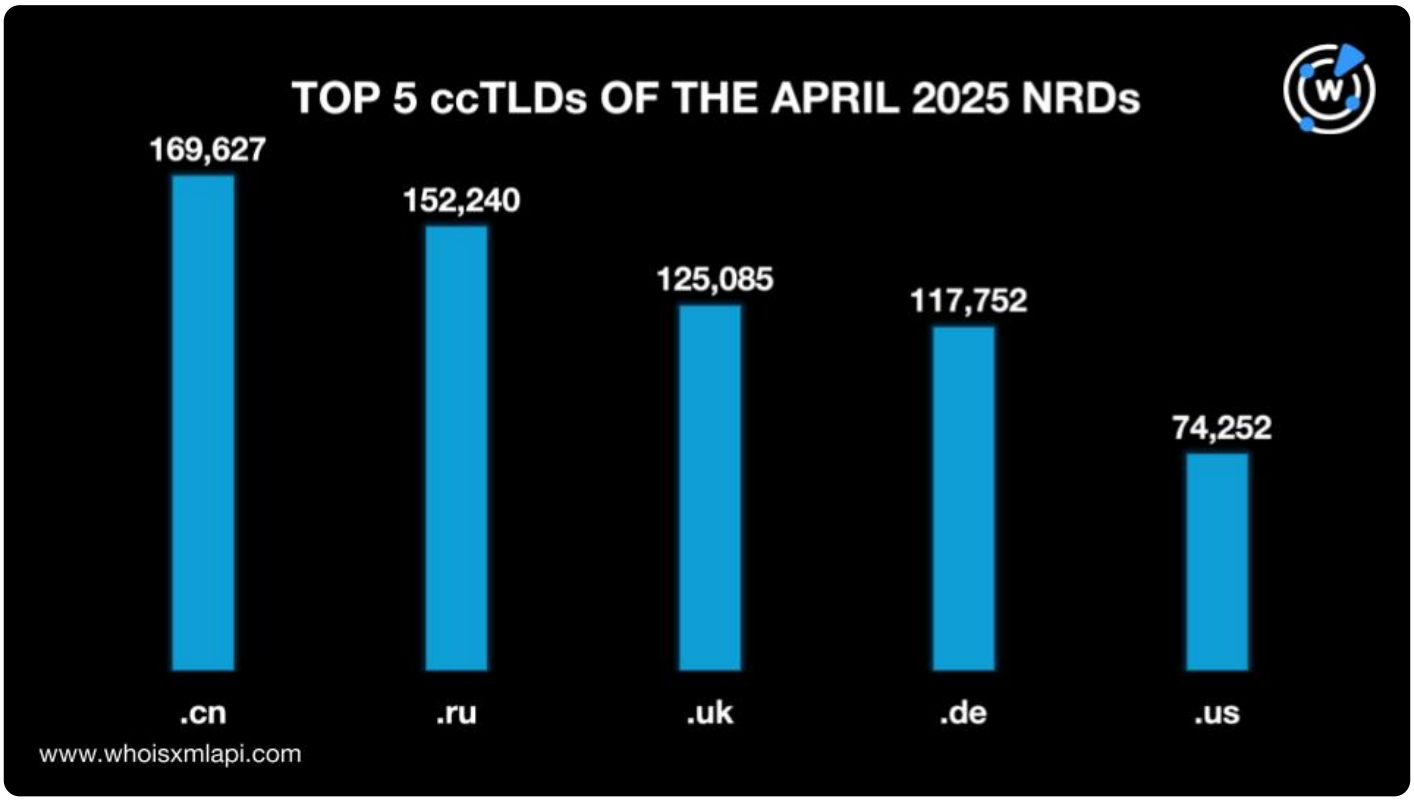


We then analyzed the April TLDs further to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 623 gTLDs, .com remained the most used, accounting for a 46.6% share, down from 49.9% in March. The rest of the top 5 lagged far behind. In fact, the four other gTLDs only clocked in a 19.4% share in total. The four remaining gTLDs were .top with a 7.0% share, .xyz with 5.5%, .org with 3.5%, and .shop with 3.4%.

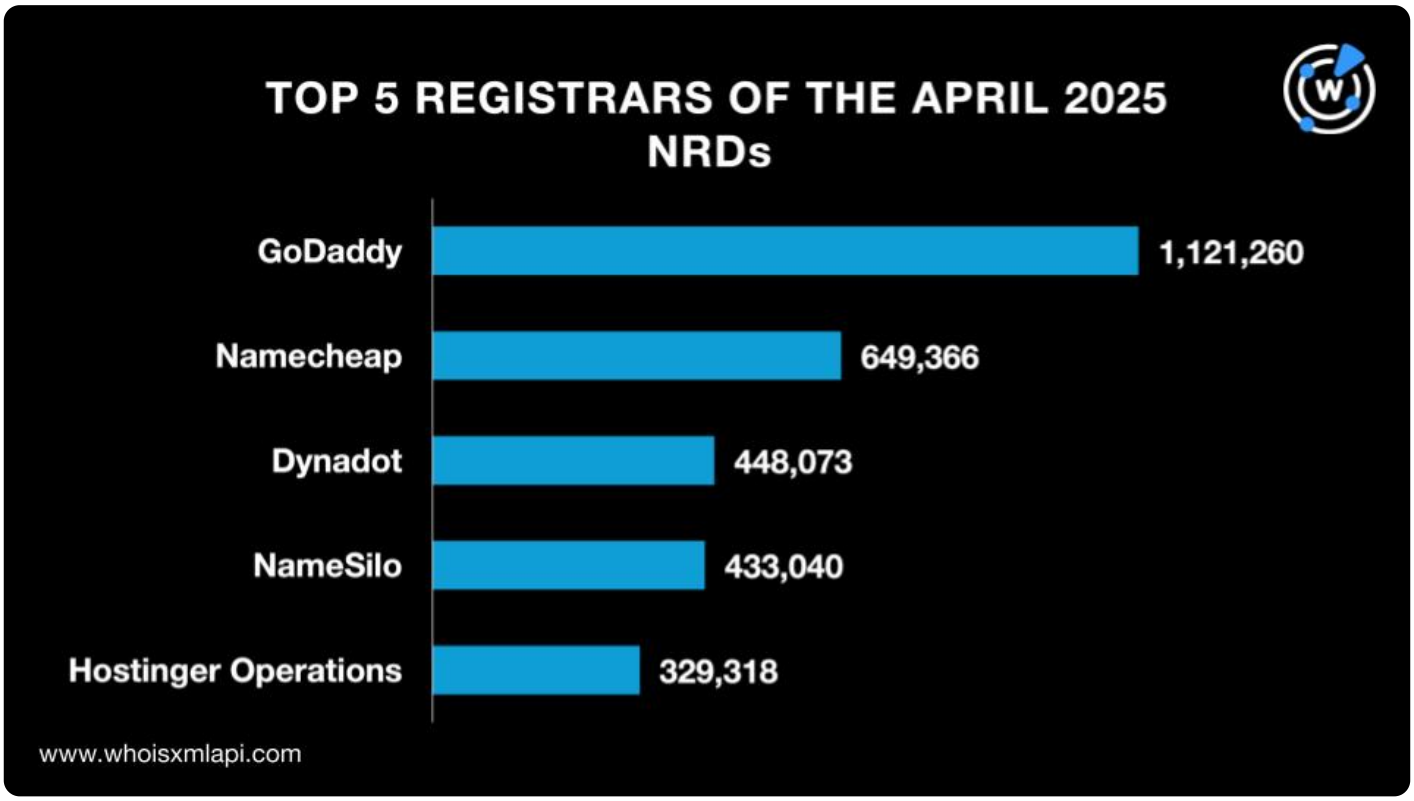


Meanwhile, .cn topped the list of 251 ccTLD extensions with a 10.3% share. The .ru ccTLD followed with a 9.2% share. Then came .uk with a 7.6% share, .de with 7.1%, and .us with 1.2%.



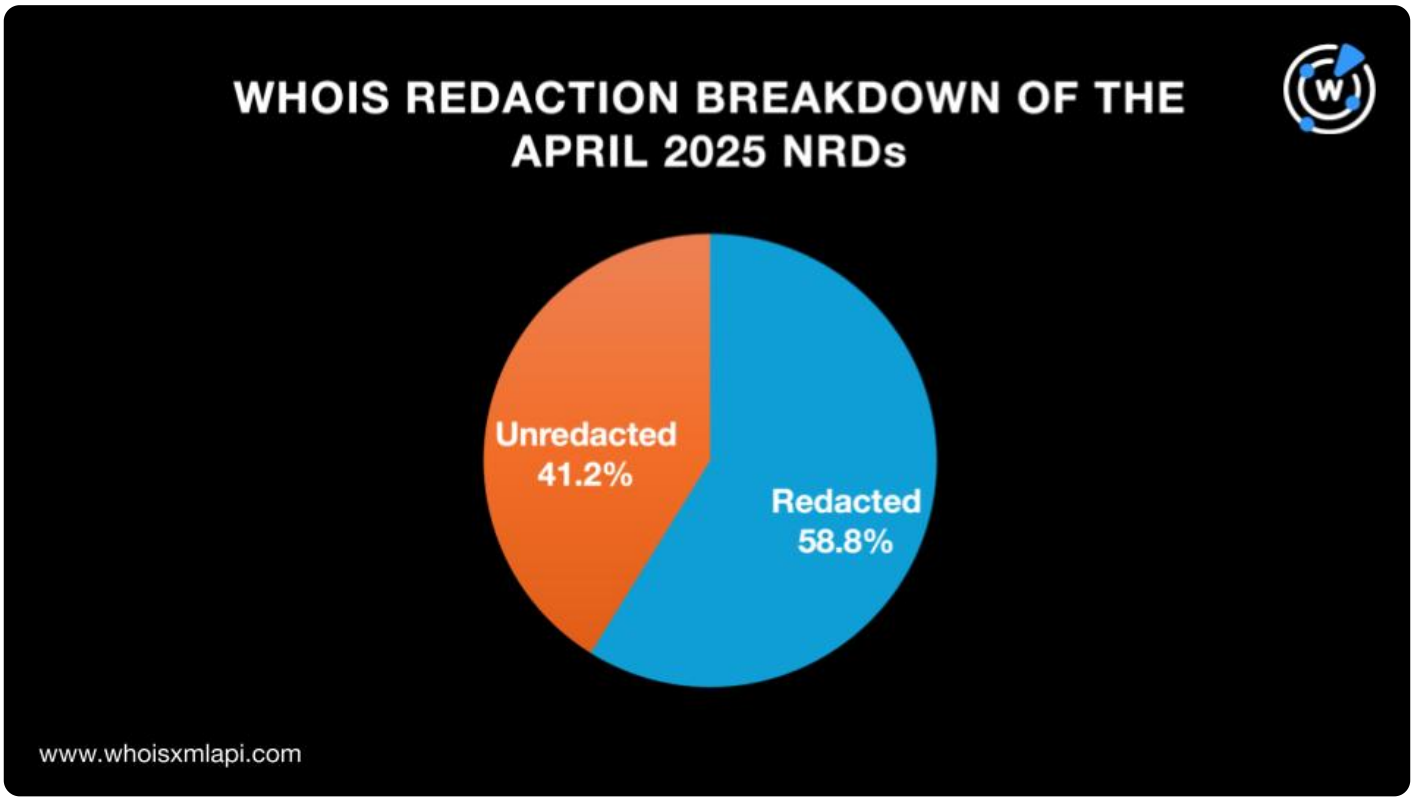
Registrar Distribution

GoDaddy continued to reign supreme among the registrars with a 14.7%, up slightly from 14.5% in March. Namecheap took the second spot with an 8.5% share. The rest of the topnotchers were Dynadot with a 5.9% share, NameSilo with 5.7%, and Hostinger Operations with 4.3%.



WHOIS Data Redaction

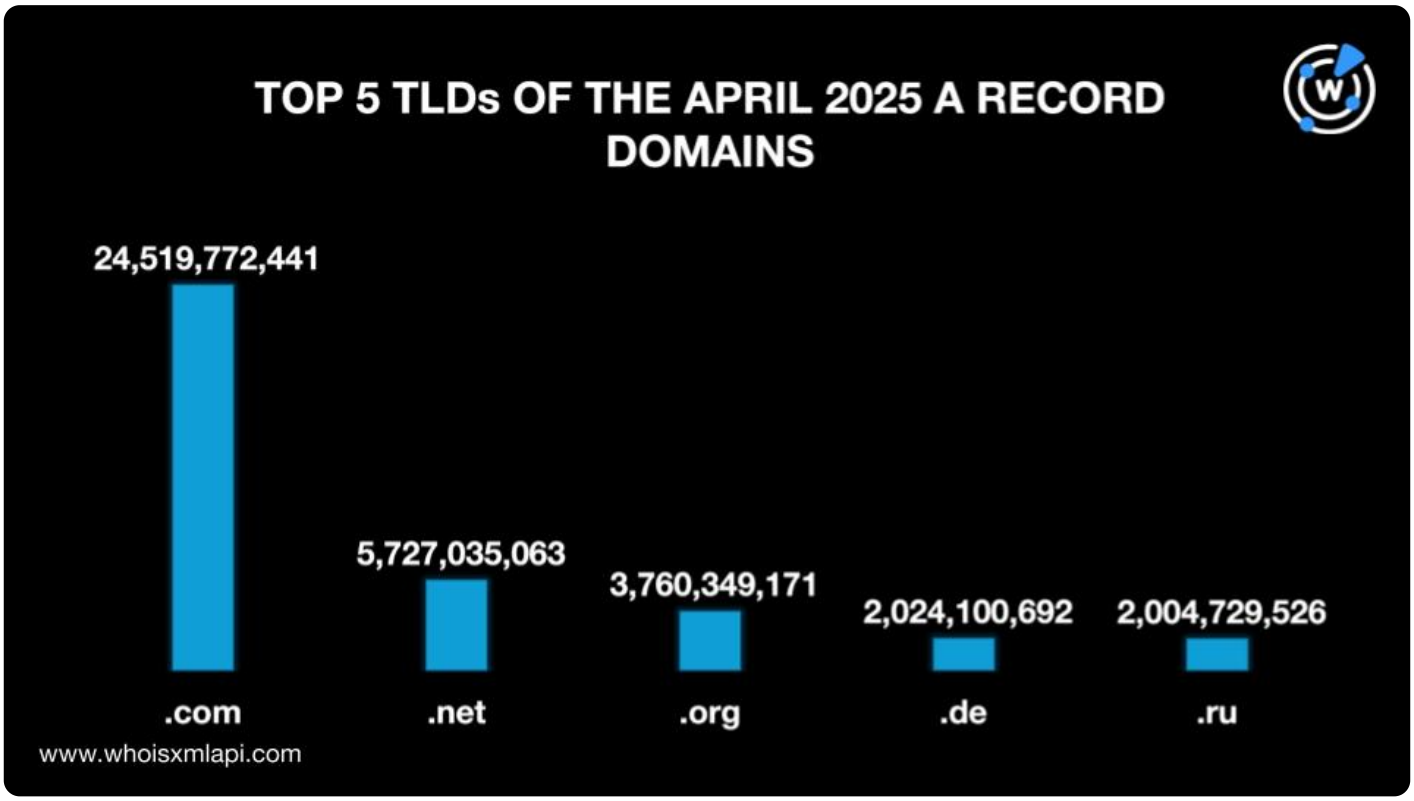
Fewer NRDs had redacted WHOIS records in April, 58.8% to be exact, down from 61.0% in March. The remaining 41.2%, meanwhile, had public WHOIS records.



A Closer Look at the April 2025 DNS Records

Top TLDs of the A Record Domains

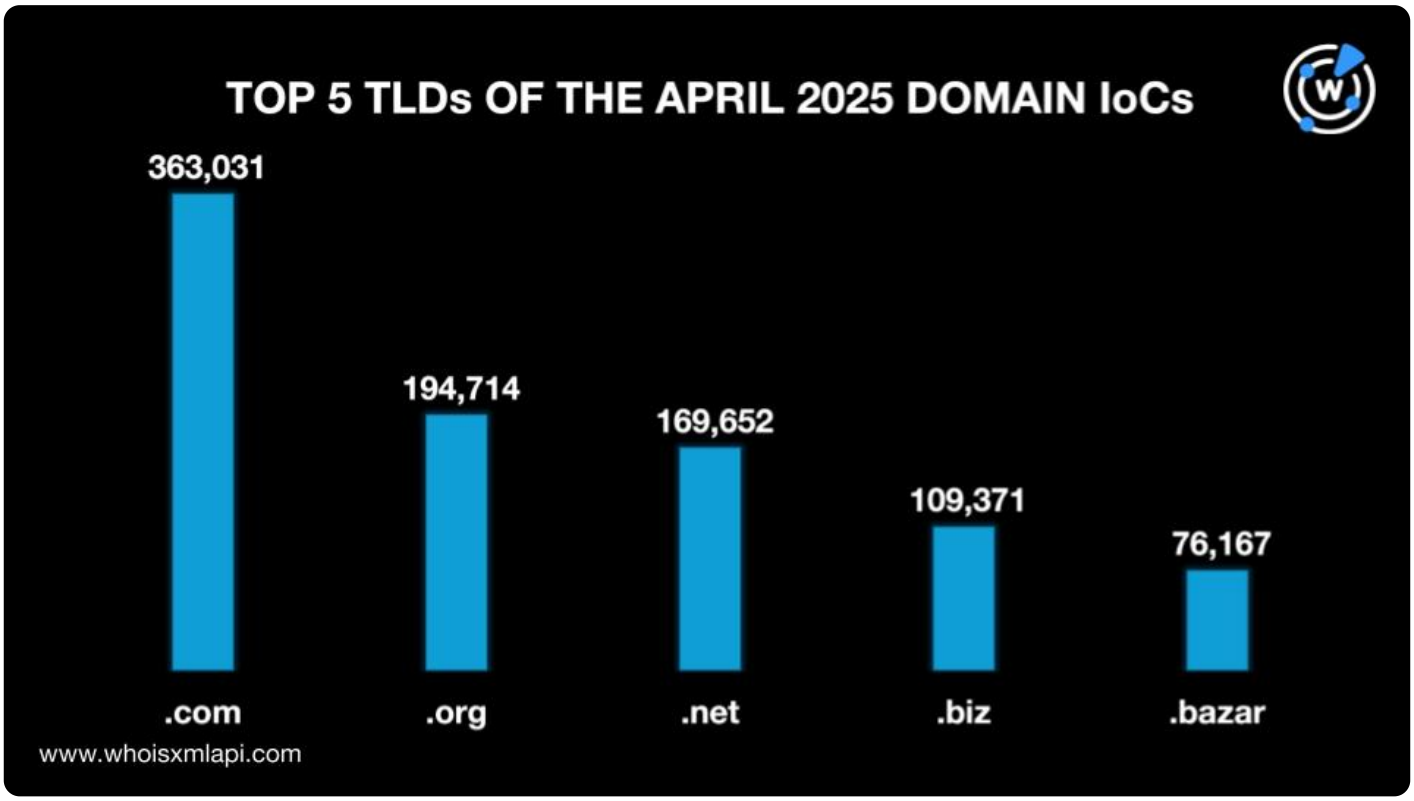
Next, we analyzed 55.8+ billion domains from our DNS database's A record full file dated 3 April 2025, which included DNS resolutions from the past 365 days. We found that 43.9%, up very slightly from 43.3% in March, sported the .com TLD. The rest of the top 5 comprised two other gTLDs (i.e., .net with a 10.2% share and .org with 6.7%) and two ccTLDs (i.e., .de and .ru with a 3.6% share each).



Cybersecurity through the DNS Lens

Top TLDs of the April 2025 Domain IoCs

As usual, we analyzed 1.5+ million domains tagged as IoCs for various threats detected in April. Our analysis revealed that .com remained the most popular TLD with a 23.0% share, up from 16.8% in March. The remaining top TLDs were all gTLDs as well, namely, .org with a 12.3% share, .net with 10.8%, .biz with 6.9%, and .bazar with 4.8%.



Threat Reports

Below are the threat reports we published in April 2025.

- **Tracing the DNS Footprints of REF7707:** REF7707 targeted the foreign ministry of a South American country. The actors used three new malware—FINALDRAFT, GUIDLOADER, and PATHLOADER—for the attack. WhoisXML API expanded the current list of 13 IoCs and uncovered 170 connected artifacts.

- **Decrypting the Inner DNS Workings of EncryptHub:** EncryptHub unknowingly exposed elements of its malicious enterprise. These errors shed light on the group's operations, including their attack chain and methodologies. WhoisXML API expanded the list of 20 IoCs that led to the discovery of 564 new connected artifacts.

- **Rounding Up the DNS Traces of RA World Ransomware:** Researchers reported that a

threat actor who has been involved in installing backdoors in the systems of target government institutions instigated an RA World ransomware attack. WhoisXML API expanded a list of five IoCs and uncovered 223 connected artifacts.

- **Unearthing the DNS Roots of the Latest Lotus Blossom Attack:** Lotus Blossom launched several cyber espionage campaigns targeting government, manufacturing, telecommunications, and media organizations using Sagerunex and other hacking tools. Researchers identified 38 IoCs that WhoisXML API expanded through a DNS deep dive. Our analysis led to the discovery of 212 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.