September 2024: Domain Activity Highlights

Posted on October 14, 2024

The WhoisXML API research team analyzed more than 7.1 million domains registered between 1 and 30 September 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 the more than 60.1 billion domains from our DNS database's A record full file released in the same month.

Next, we studied the top TLDs and associated threat types of more than 1.0 million domains detected as indicators of compromise (IoCs) in September.

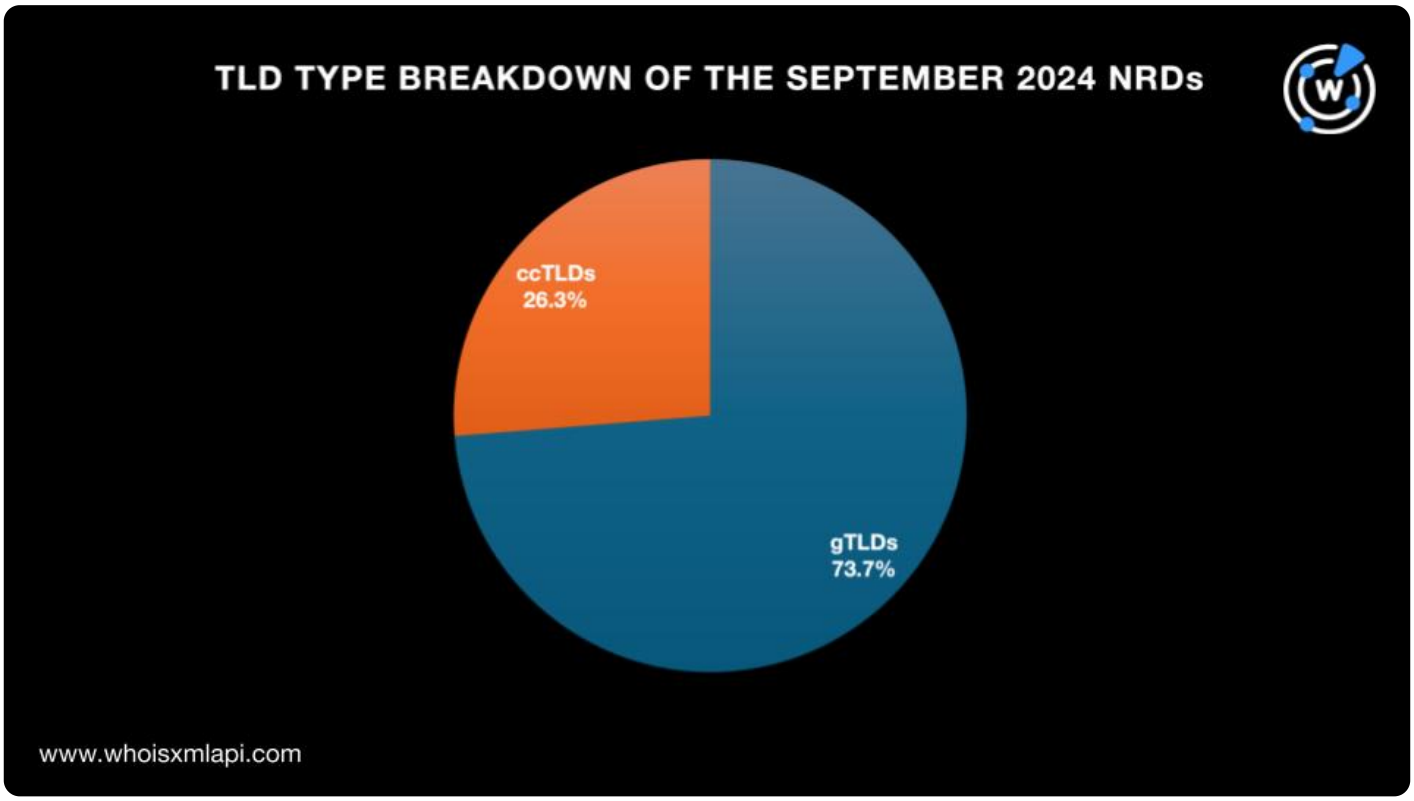
Finally, we summed up our findings and provided links to the threat reports produced using DNS, IP, and domain intelligence sources during the period.

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

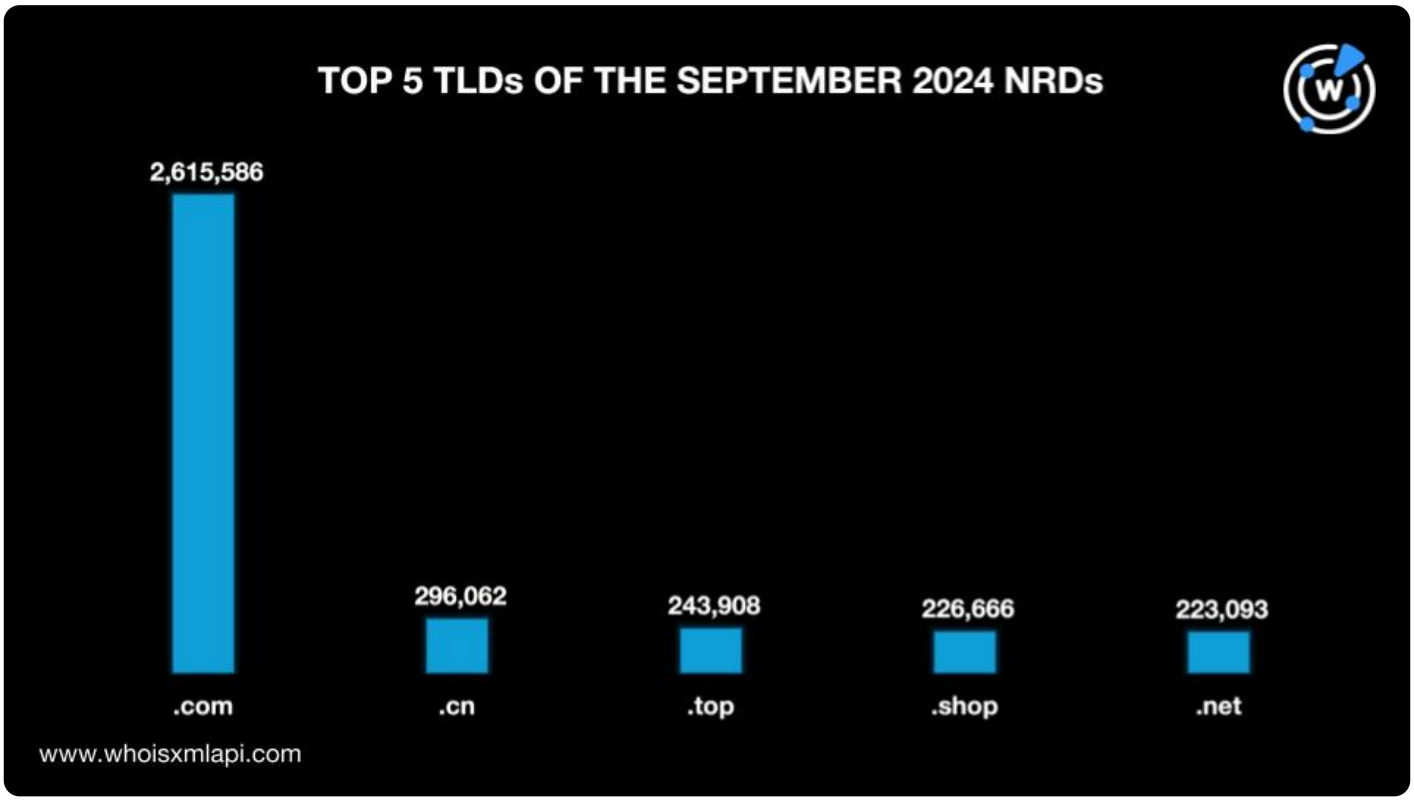
Zooming in on the September 2024 NRDs

TLD Distribution

Of the 7.1 million domains registered in September, 73.7% used generic TLD (gTLD) extensions, while 26.3% used country-code TLD (ccTLD) extensions.

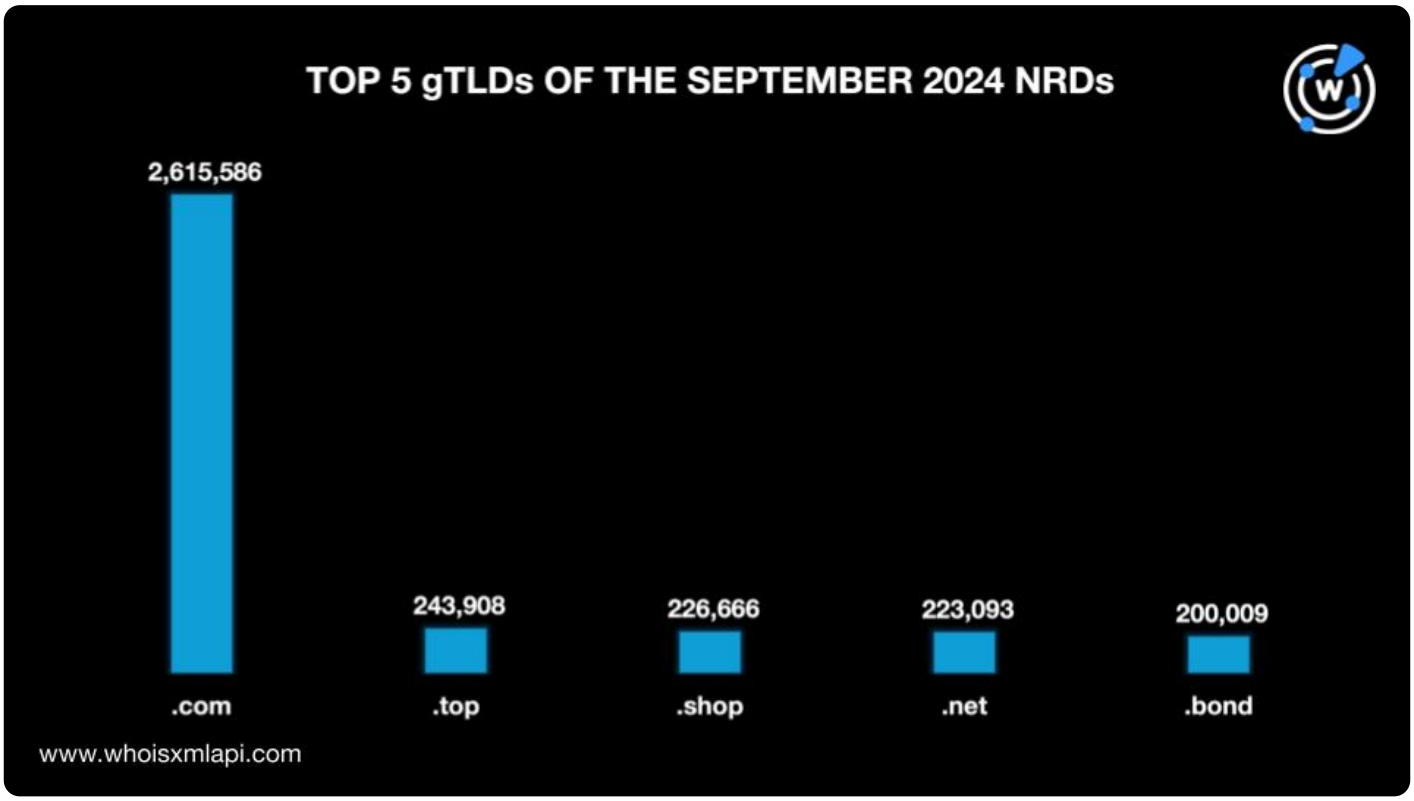


The .com TLD remained the most popular extension used by 36.4% of the total number of newly registered domains (NRDs) in September, down from 39.1% in August. The other most used TLDs on the top 5 followed with a significant gap as in the previous month. They included three other gTLDs and one ccTLD, namely, .cn (4.1%), .top (3.4%), .shop (3.2%), and .net (3.1%).

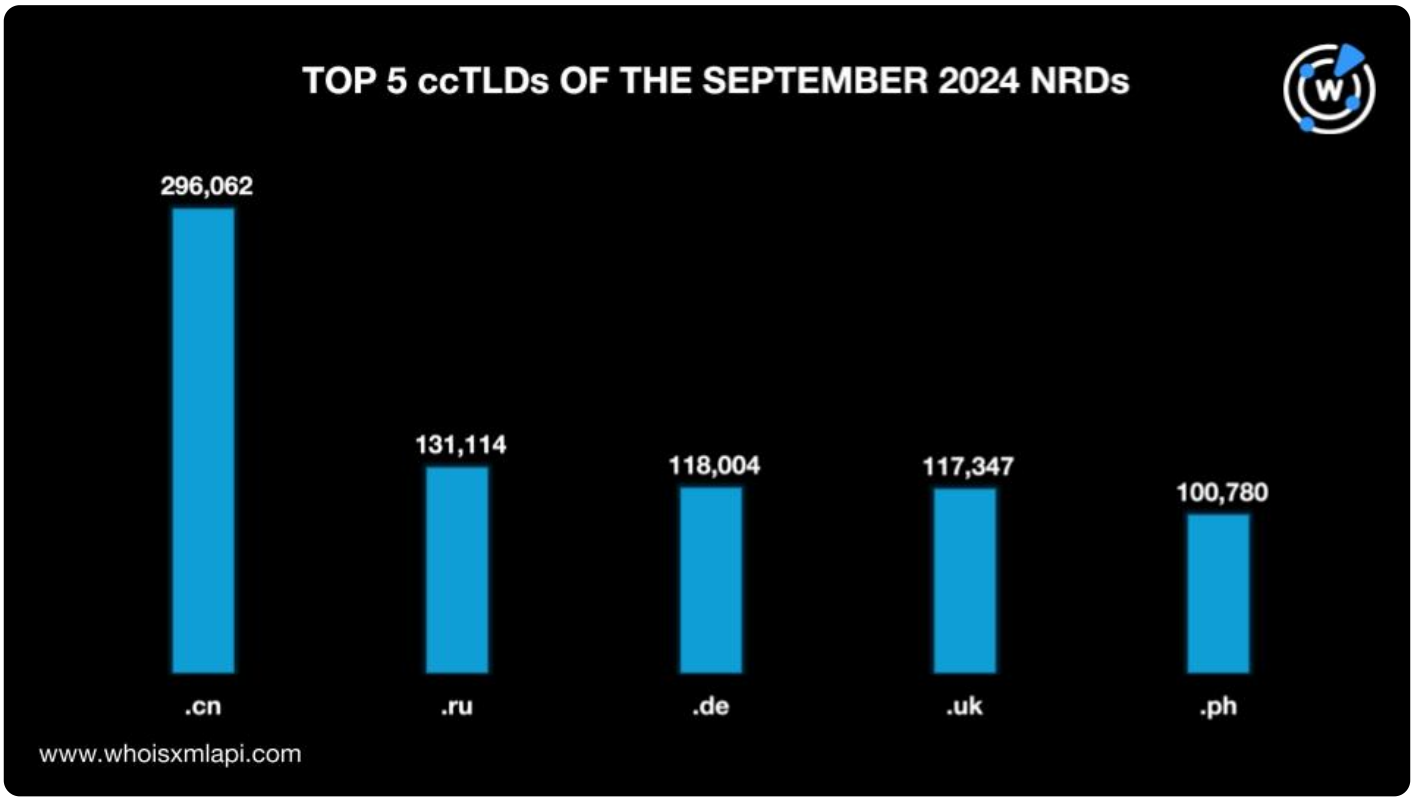


We then analyzed the September TLDs further to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 637 gTLDs, .com remained the most used, accounting for a 49.3% share, down from 51.0% in August. The rest of the top 5 lagged far behind. In fact, .top only had a 4.6% share. The three other gTLDs in the list were .shop (4.3%), .net (4.2%), and .bond (3.8%).

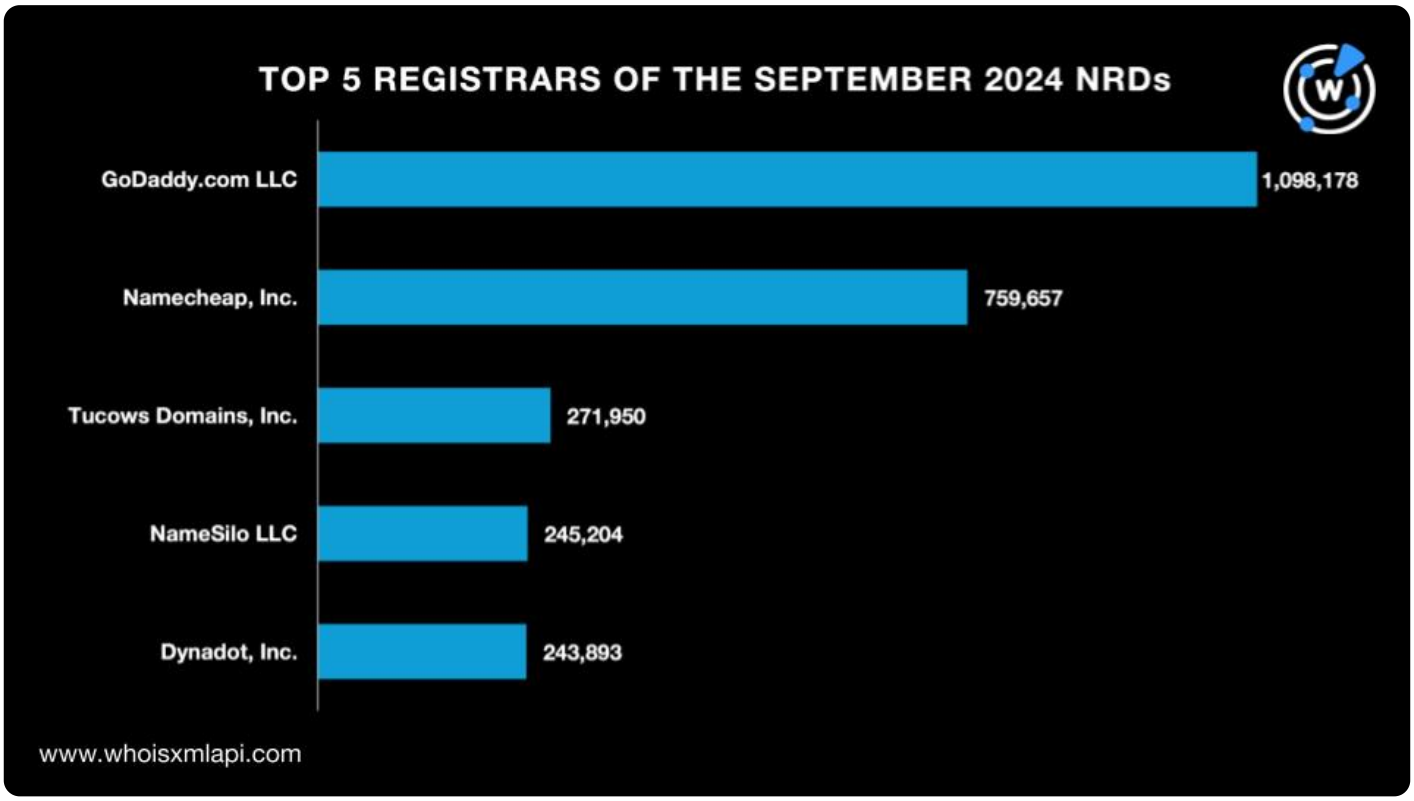


Meanwhile, .cn remained the top ccTLD out of 242 extensions with a 15.7% share, up from 13.1% in August. The other commonly used ccTLDs were .ru (6.9%), .de and .uk (6.2%), and .ph (5.3%).



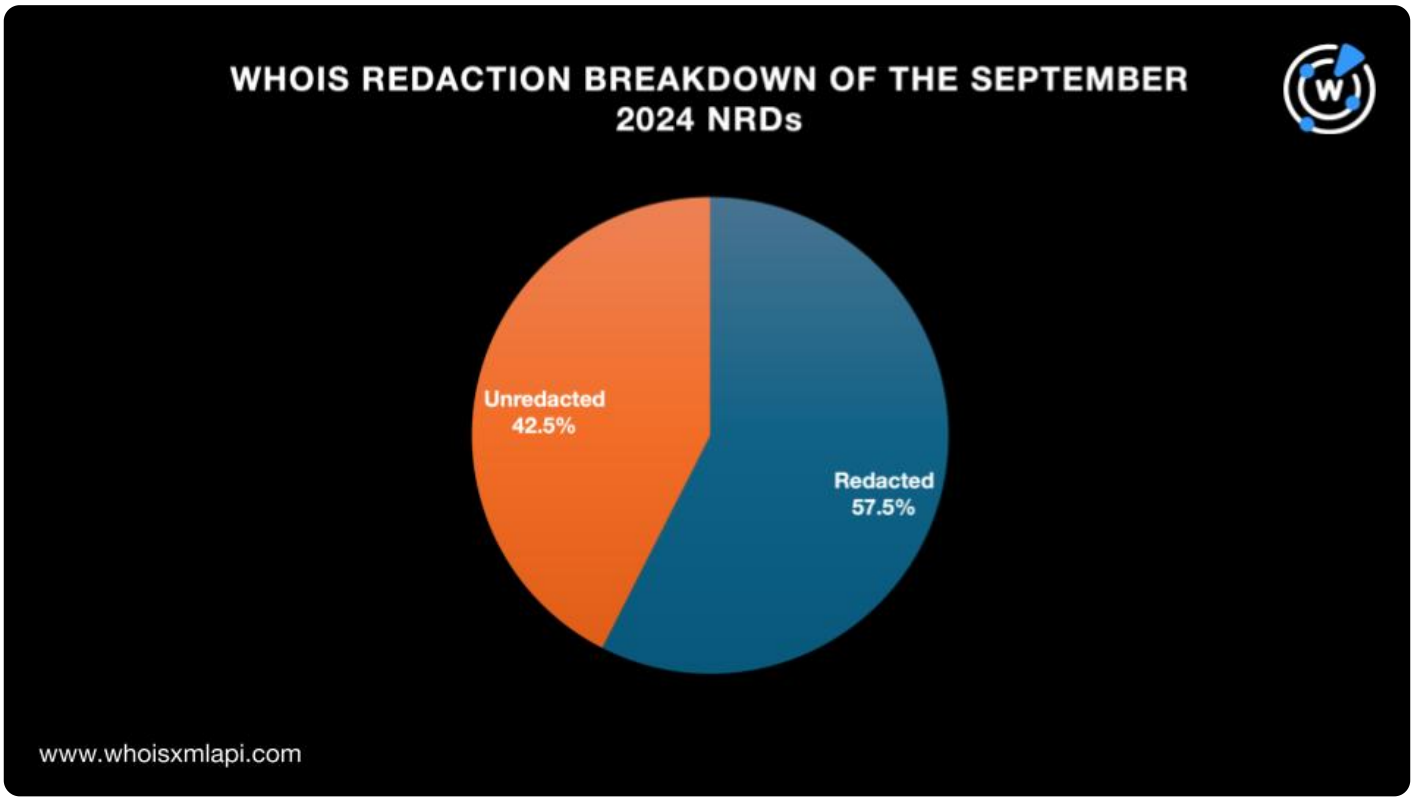
Registrar Distribution

GoDaddy.com LLC continued to top the list of registrars with a 15.4% share, down from 17.0% in August. Namecheap, Inc. came in second place with a 10.6% share. Tucows Domains, Inc. (3.8%) and NameSilo LLC and Dynadot, Inc. (3.4% each) rounded out the top 5.



WHOIS Data Redaction

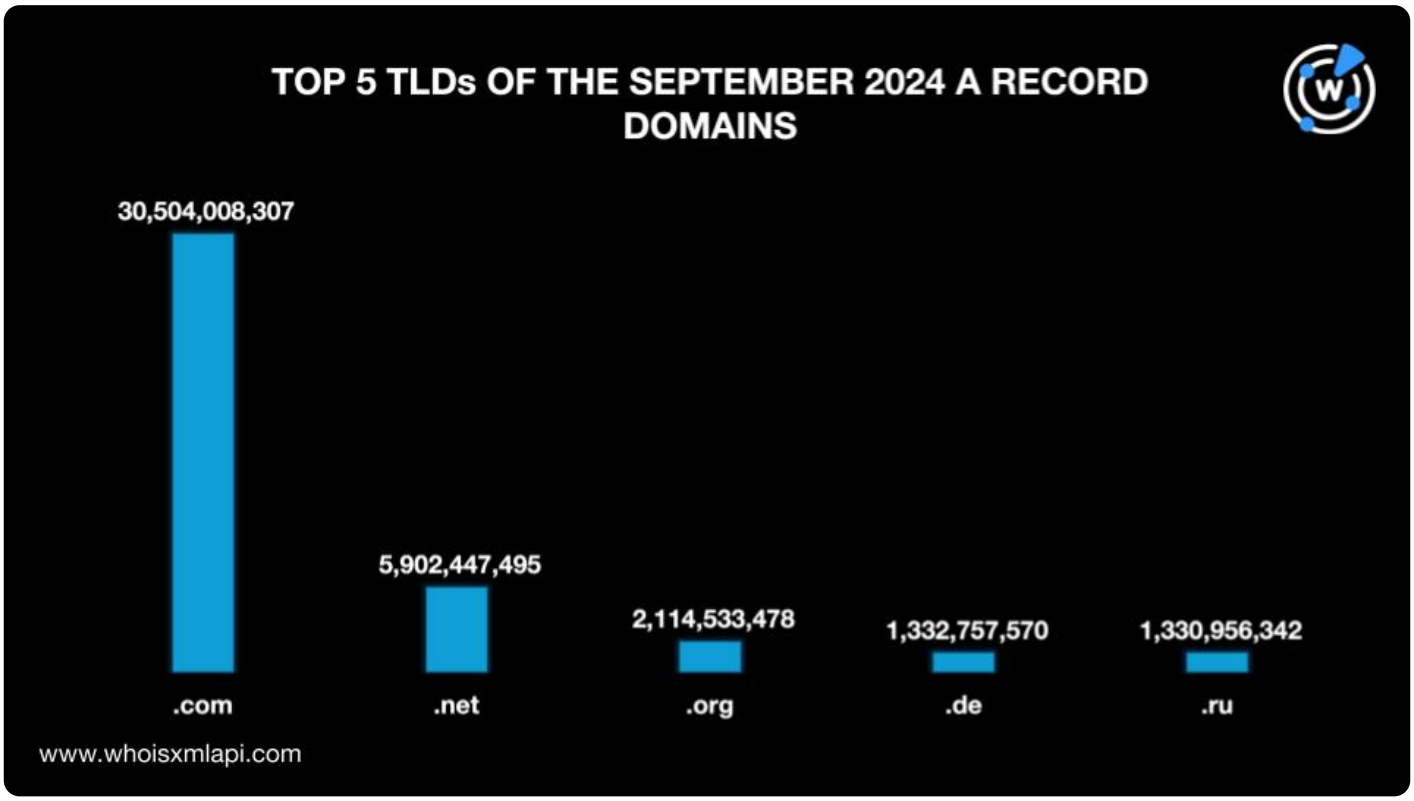
A majority of the NRDs, 57.5% to be exact, continued to have redacted WHOIS records. On the other hand, 42.5% of the September NRDs had public WHOIS records.



A Closer Look at the September 2024 DNS Records

Top TLDs of the A Record Domains

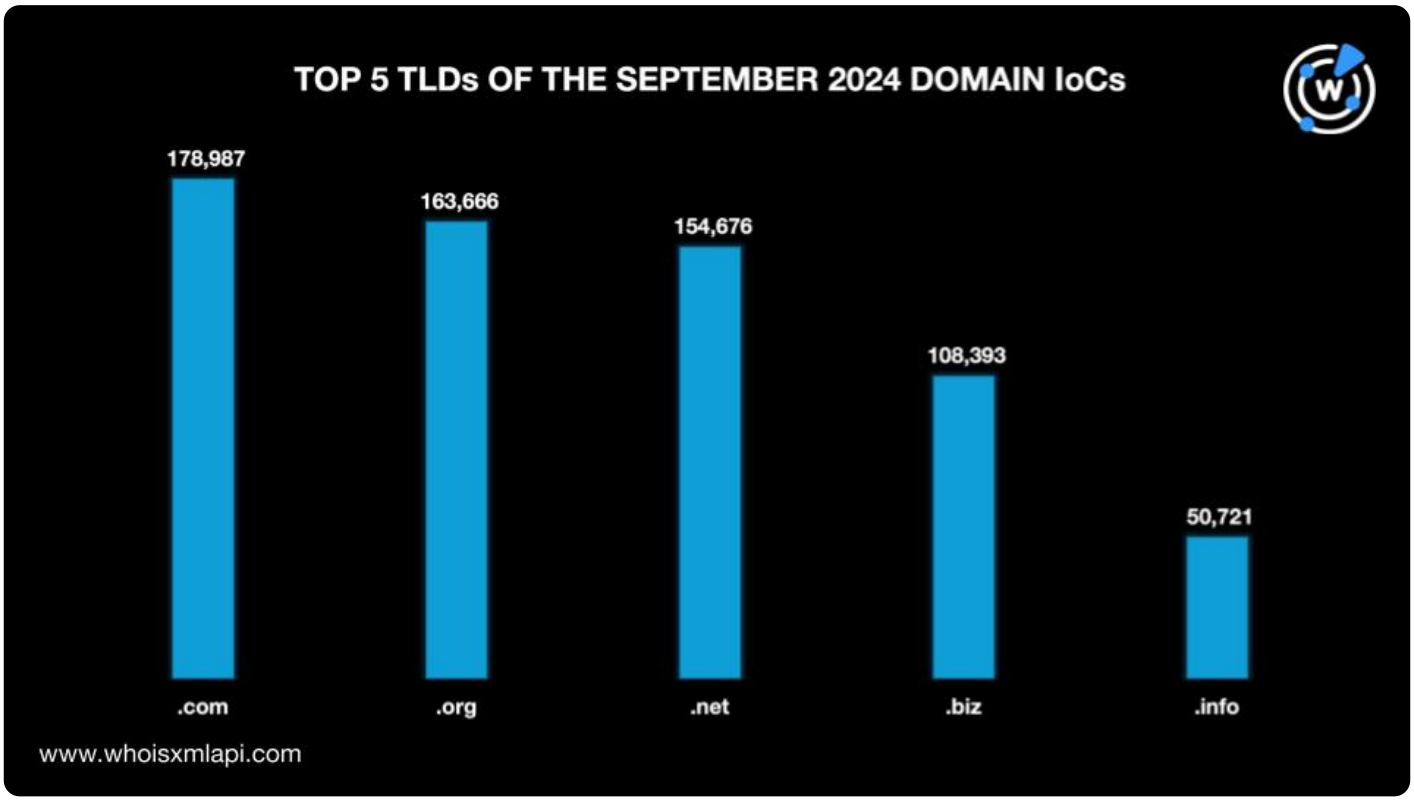
Next, we analyzed more than 60.1 billion domains from our DNS database's A record full file for September 2024, which included DNS resolutions from the past 365 days. We found that 50.7% used the .com TLD. The rest of the top 5 comprised two other gTLDs, namely, .net (9.8%) and .org (3.5%) and two ccTLDs, specifically, .de and .ru (2.2% each).



Cybersecurity through the DNS Lens

Top TLDs of the September 2024 Domain IoCs

As usual, we analyzed more than 1.0 million domains tagged as IoCs for various threats detected in September. Our analysis revealed that .com remained the most popular TLD with a 17.2% share, down from 17.4% in August. The remaining top TLDs were all gTLDs as well, namely, .org (15.7%), .net (14.9%), .biz (10.4%), and .info (4.9%).



Threat Reports

Below are the threat reports we published in September 2024.

- **Inspecting Konfety's Evil Twin Apps through the DNS Lens:** The WhoisXML API research team expanded a list of 23 IoCs related to Konfety that created evil twins for at least 250 mobile apps on Google Play. We uncovered 640+ potentially connected artifacts.
- **The Extended Reach of the Extension Trojan Campaign in the DNS:** WhoisXML API researchers sought to determine how widespread the Extension Trojan infrastructure is in the DNS by analyzing 22 IoCs. In the process, we found 150 additional threat artifacts.
- **Tracking the DNS Footprint of the Polyfill Supply Chain Attackers:** WhoisXML API's investigation pivoting off six IoCs led to the discovery of 200+ artifacts that could be tied to the massive Polyfill supply chain attacks.

- **A DNS Deep Dive into the NetSupport RAT Campaign:** The WhoisXML API researchers looked into the DNS footprint of NetSupport RAT by expanding a list of nine IoCs that led to the discovery of 1,250+ potentially connected artifacts.
- **Stripping Down the BlackSuit Ransomware Network Aided by DNS Data:** WhoisXML API's IoC list expansion for BlackSuit, which jumped off 91 IoCs, uncovered 280 artifacts related to the threat.

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.