August 2024: Domain Activity Highlights

Posted on September 13, 2024

The WhoisXML API research team analyzed more than 7.4 million domains registered between 1 and 31 August 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 59.2 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 August.

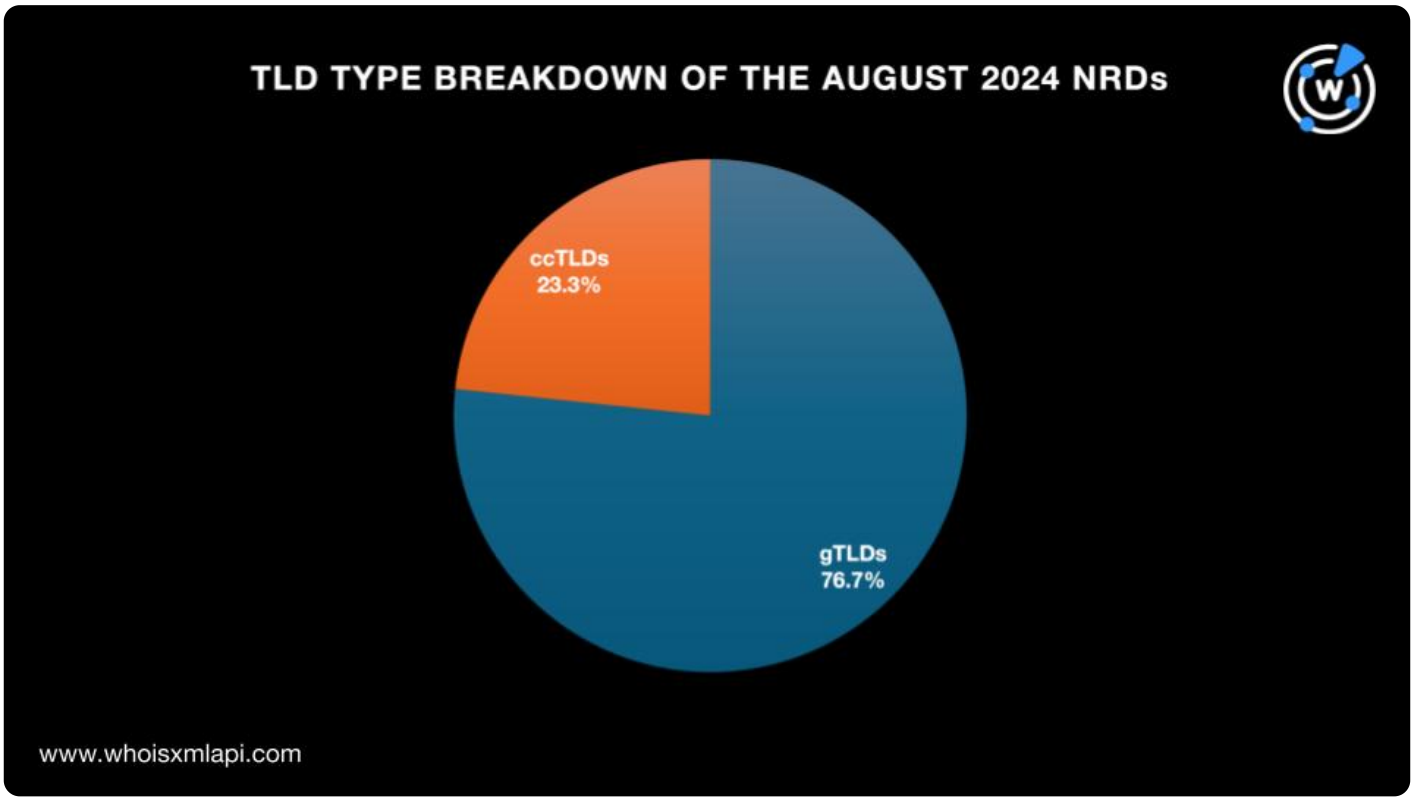
Finally, we summed up our findings and provided links to the threat reports produced using DNS, IP, and domain intelligence sources during the period.

Want more insights? Download the full top 10 gTLD and ccTLD analysis results from our website.

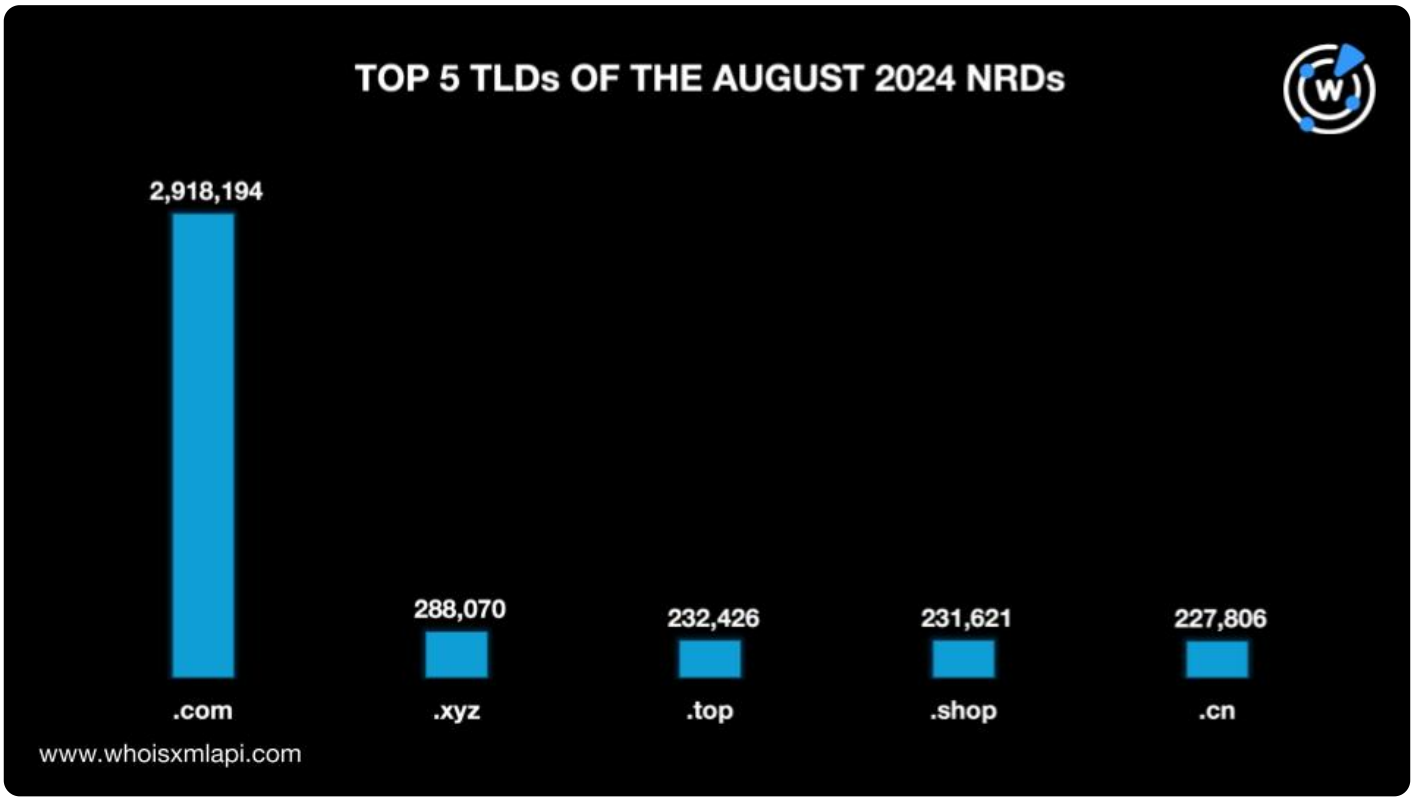
Zooming in on the August 2024 NRDs

TLD Distribution

Of the 7.4 million domains registered in August, 76.7% used generic TLD (gTLD) extensions, while 23.3% used country-code TLD (ccTLD) extensions.

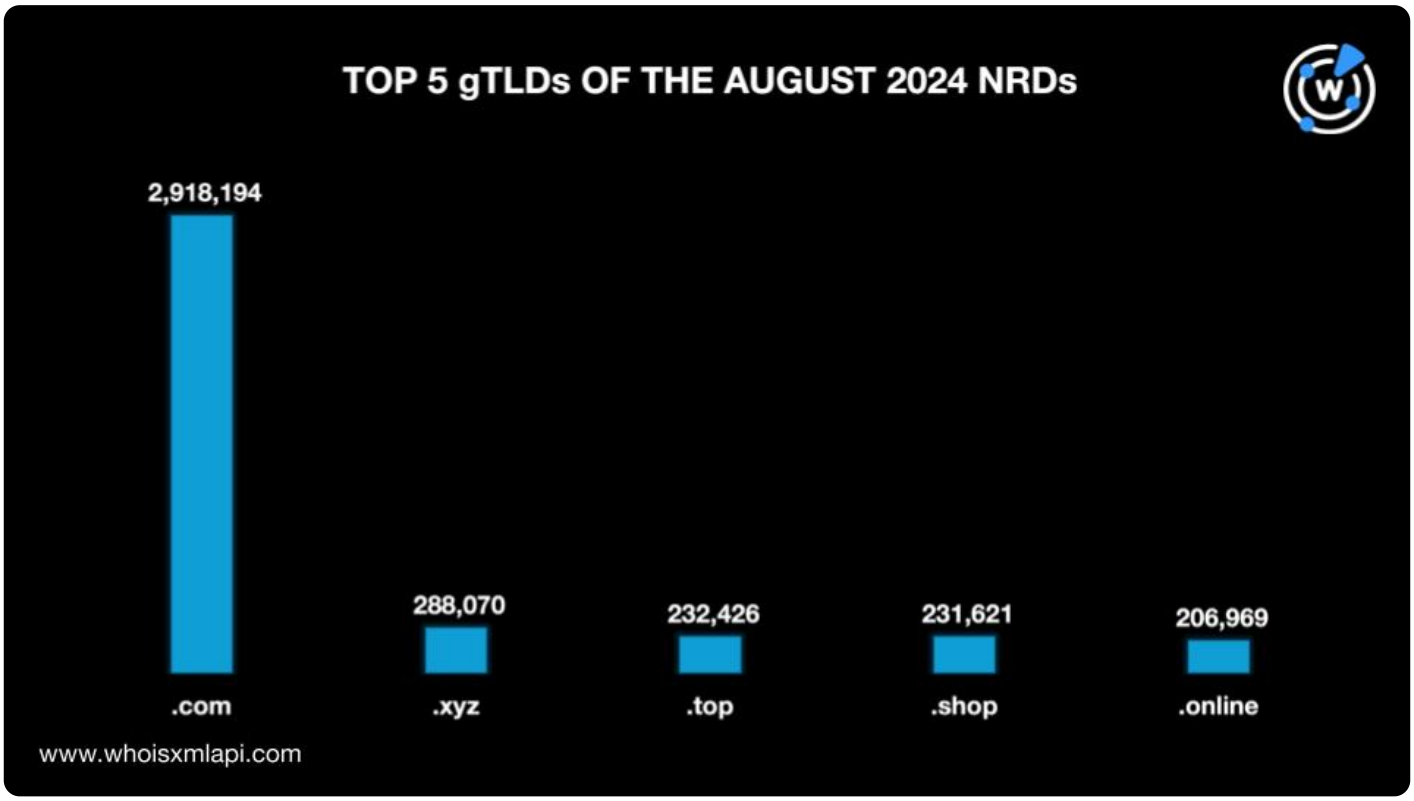


The .com TLD remained the most popular extension used by 39.1% of the total number of newly registered domains (NRDs) in August. The other most used TLDs on the top 5 followed with a significant gap as in the previous month. They included three other gTLDs and one ccTLD, namely, .xyz (3.9%), .top and .shop (3.1% each), and .cn (3.0%).

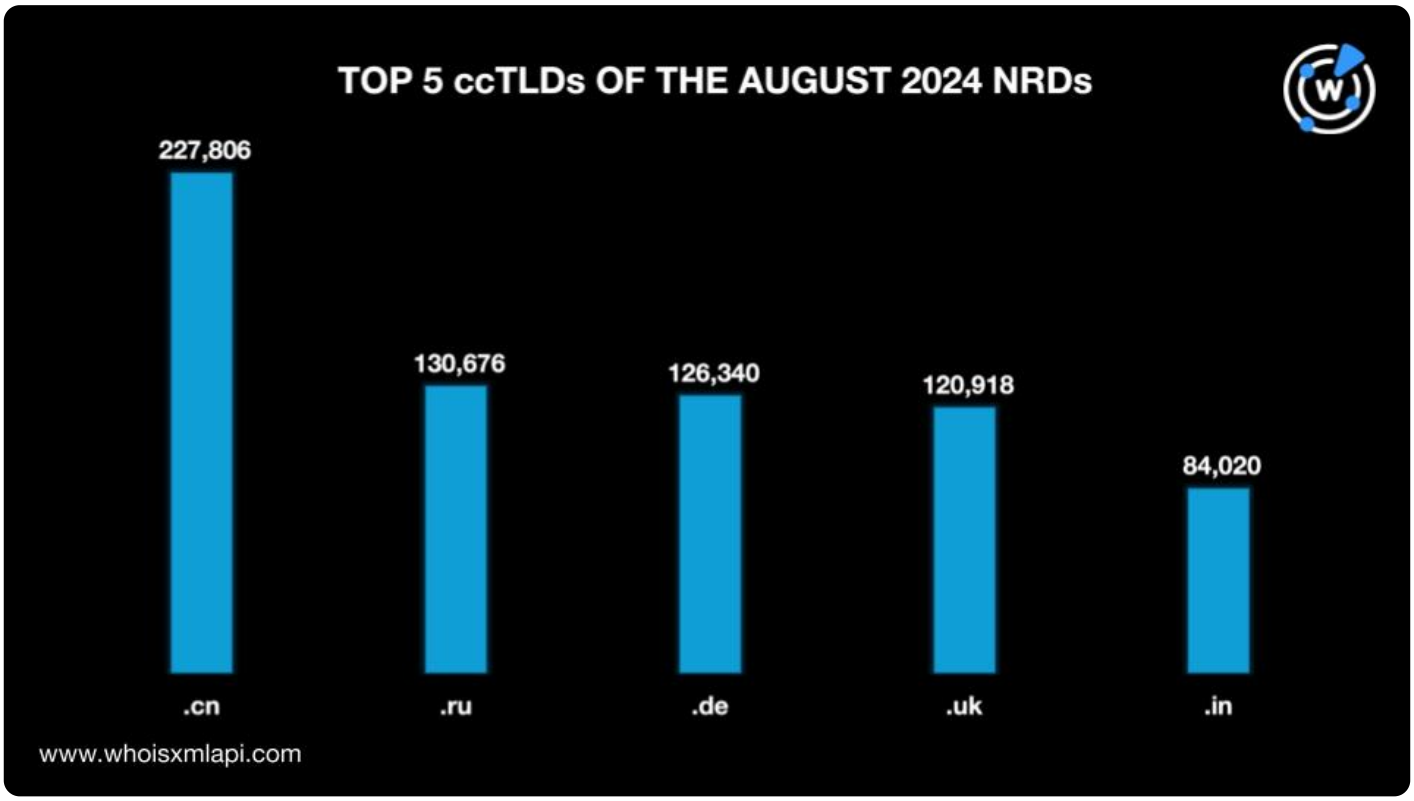


We then analyzed the August TLDs further to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 636 gTLDs, .com remained the most used, accounting for a 51.0% share. The rest of the top 5 lagged far behind. In fact, .xyz only had a 5.0% share. The three other gTLDs in the list were .top (4.1%), .shop (4.0%), and .online (3.6%).

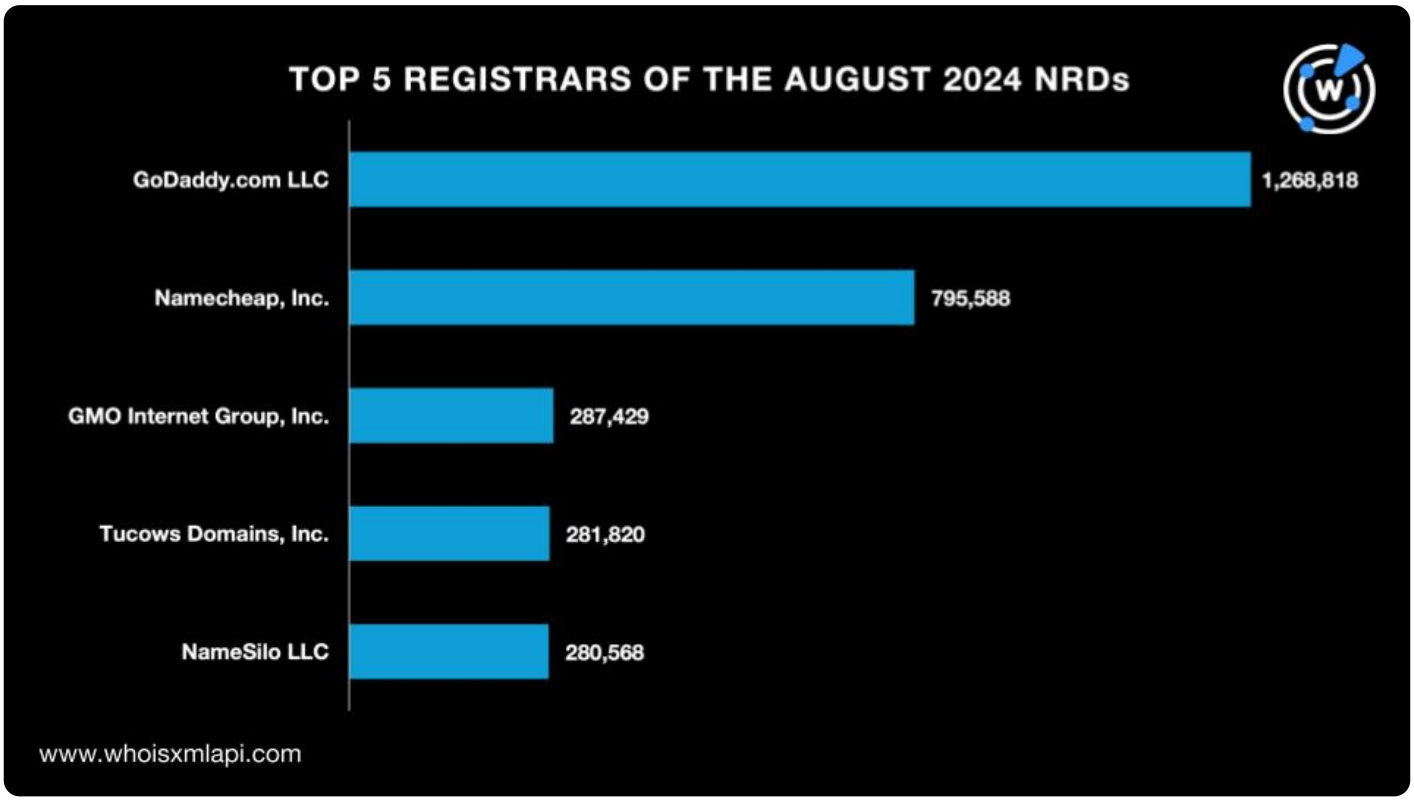


Meanwhile, .cn remained the top ccTLD out of 241 extensions with a 13.1% share, up from 11.3% in July. The other commonly used ccTLDs were .ru (7.5%), .de (7.3%), .uk (6.9%), and .in (4.8%).



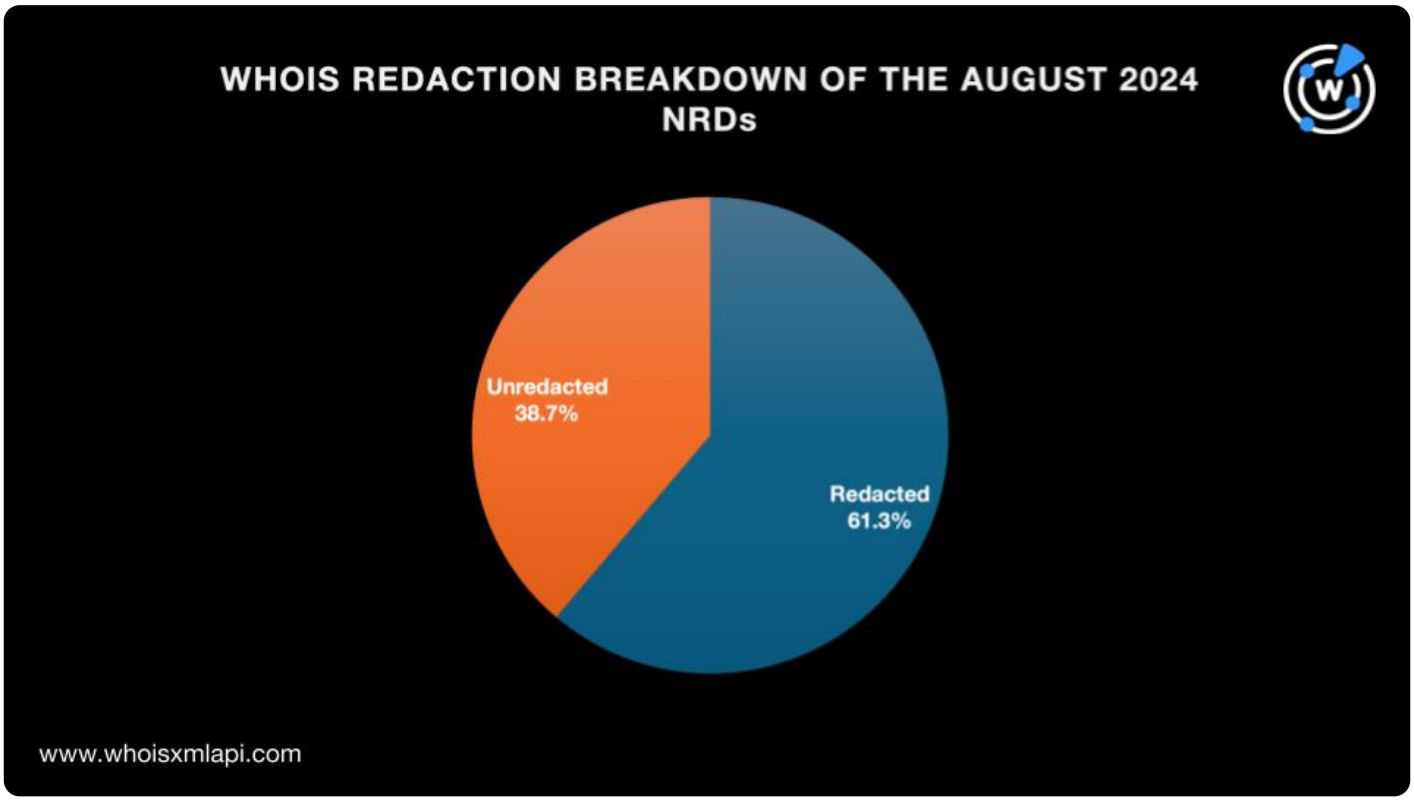
Registrar Distribution

GoDaddy.com LLC continued to top the list of registrars with a 17.0% share, up from 16.6% in July. Namecheap, Inc. came in second with a 10.7% share. GMO Internet Group, Inc. (3.9%) and Tucows Domains, Inc. and NameSilo LLC (3.8% each) rounded out the top 5.



WHOIS Data Redaction

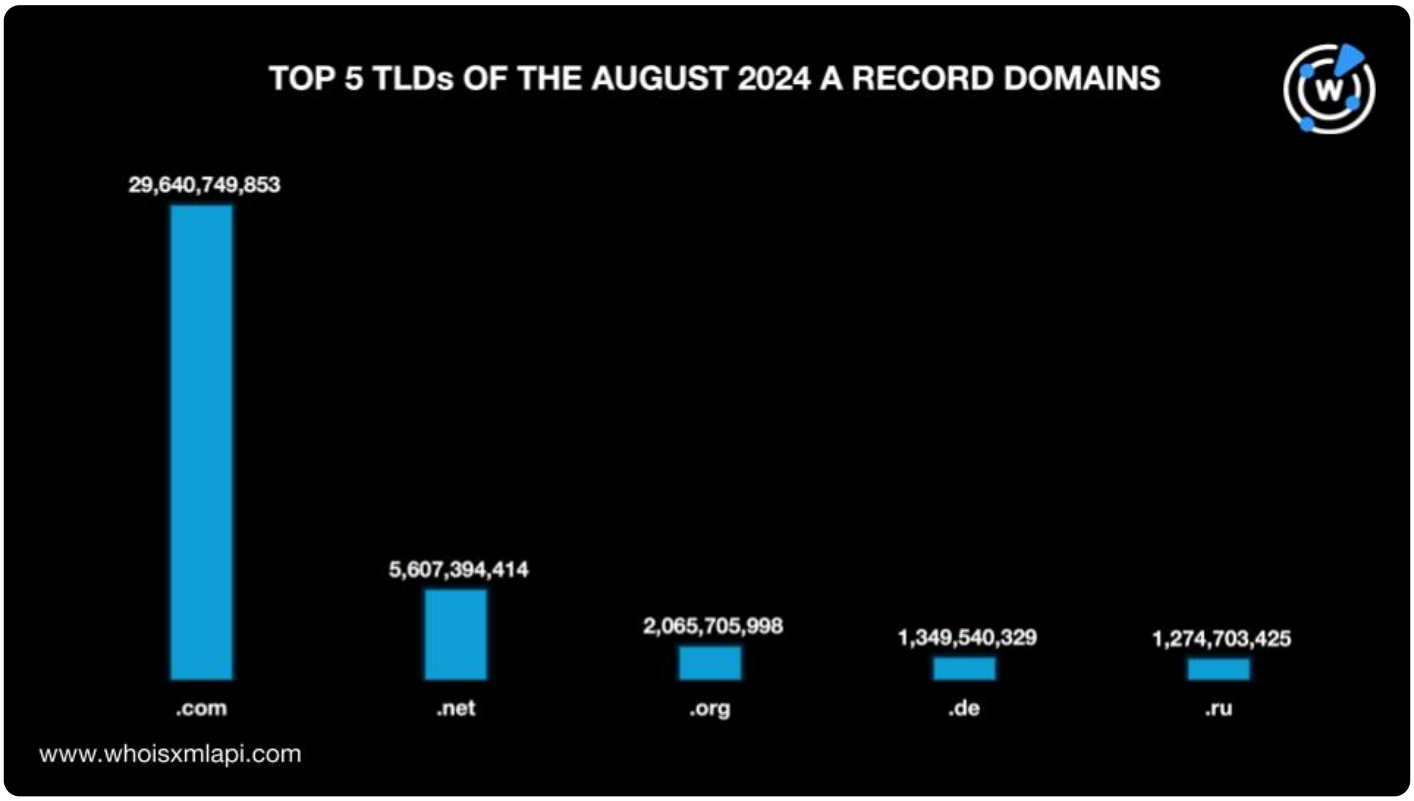
A majority of the NRDs, 61.3% to be exact, continued to have redacted WHOIS records. On the other hand, 38.7% of the August NRDs had public WHOIS records.



A Closer Look at the August 2024 DNS Records

Top TLDs of the A Record Domains

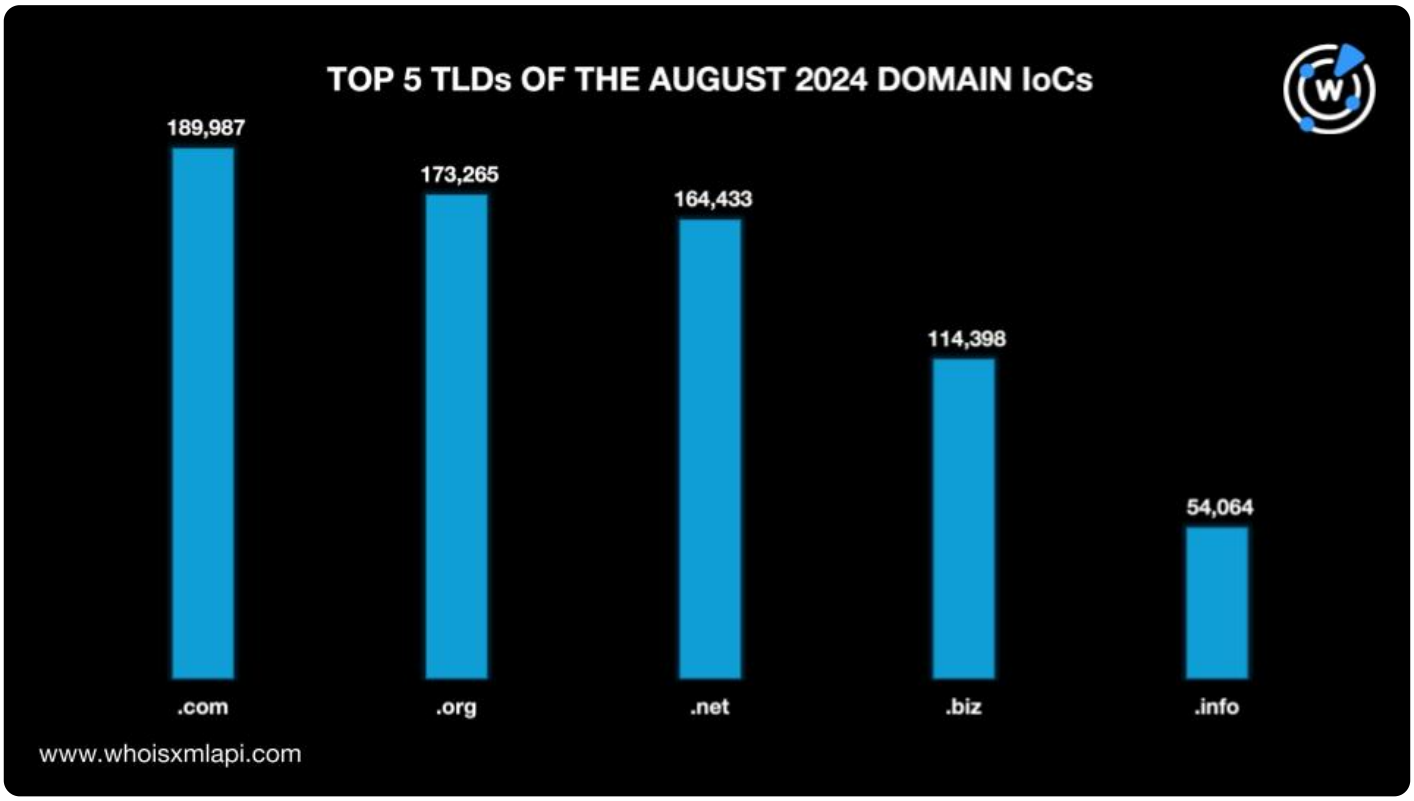
Next, we analyzed more than 59.2 billion domains from our DNS database's A record full file for August 2024, which included DNS resolutions from the past 365 days. We found that half of them used the .com TLD. The rest of the top 5 comprised two other gTLDs, namely, .net (9.5%) and .org (3.5%), and two ccTLDs, specifically, .de (2.3%) and .ru (2.2%).



Cybersecurity through the DNS Lens

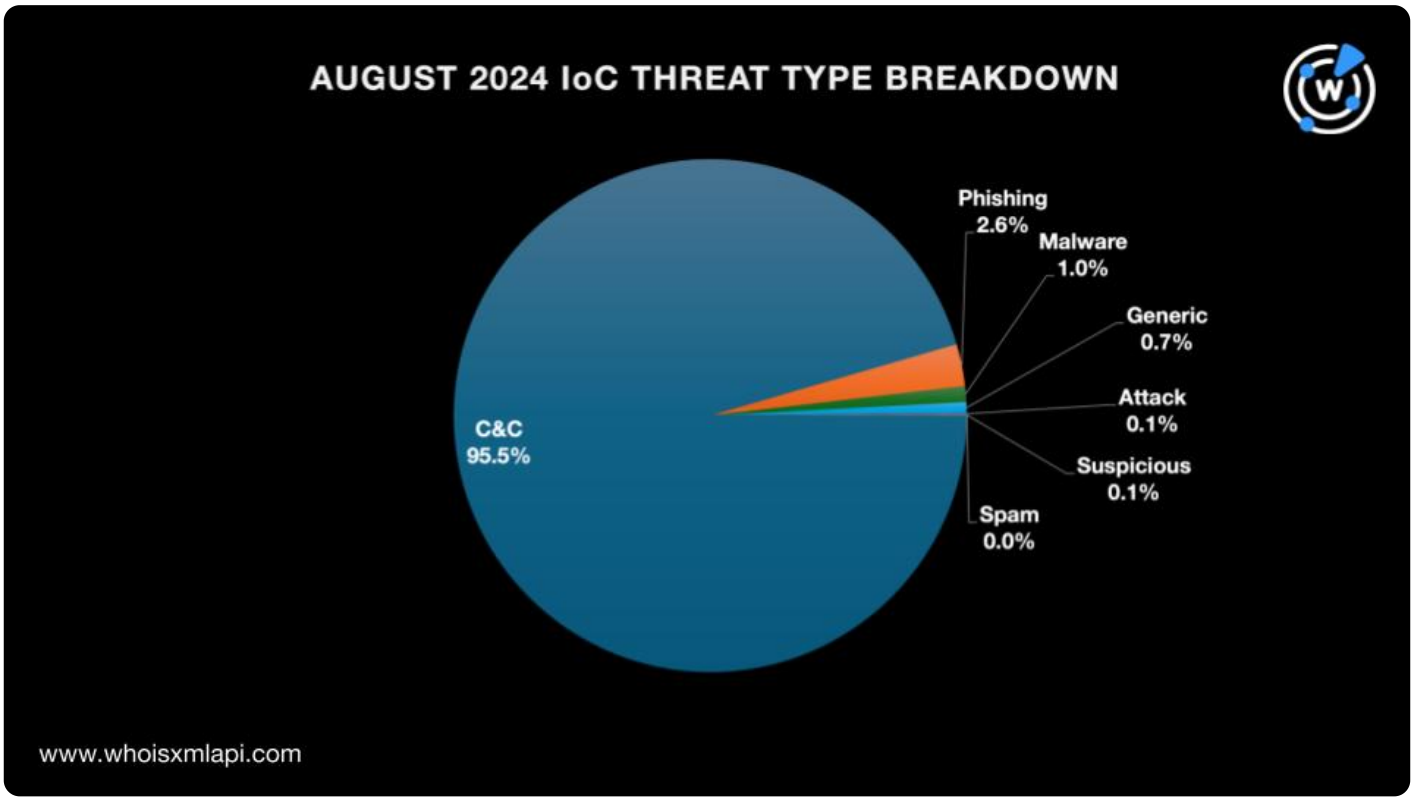
Top TLDs of the August 2024 Domain IoCs

As usual, we analyzed more than 1.0 million domains tagged as IoCs for various threats detected in August. Our analysis revealed that .com remained the most popular TLD with a 17.4% share of the total number of IoCs. The remaining top TLDs were all gTLDs as well, namely, .org (15.9%), .net (15.1%), .biz (10.5%), and .info (5.0%).



Threat Type Breakdown of the August 2024 Domain IoCs

When we grouped the August domain IoCs based on associated threat type, we discovered that an overwhelming majority, 95.5% to be exact, seemingly served as command-and-control (C&C) servers. This trend varied significantly from July when none of the IoCs were connected to C&C. The rest of the IoCs were related to six other threat types, namely, phishing (2.6%), malware attacks (1.0%), generic threats (0.7%), other attack types (0.1%), suspicious activities (0.1%), and spam campaigns (0.0%, which translates to 2 domains).



Threat Reports

Below are the threat reports we published in August 2024.

- **On a DNS Threat Hunt for DISGOMOJI:** The WhoisXML API research team expanded a list of IoCs for a UTA0137 cyber espionage campaign targeting Indian organizations. The threat actors used DISGOMOJI, a malware coded in Golang and came in the guise of emojis, a first for cyber attacks.
- **A Closer Look at the Meduza Stealer through a DNS Deep Dive:** The WhoisXML API researchers sought to uncover artifacts potentially connected to the Meduza Stealer, likely the first stealer we analyzed that exploited a vulnerability.
- **Hunting for U.S. Presidential Election-Related Domain Threats in the DNS:** The WhoisXML API research team discovered that the 2024 U.S. presidential elections is not just

a hotbed for tension, but also cybersquatting. Our study uncovered a staggering number of cyber resources linked to presidential candidates and election-related keywords.

You can find more reports created in the past months here.

Download the August 2024 Top 10 gTLD and ccTLD Highlights from our website or contact us for more product information.