July 2024: Domain Activity Highlights

Posted on August 14, 2024

The WhoisXML API research team analyzed more than 7.3 million domains registered between 1 and 31 July 2024 in this post to identify five of the most popular registrars, top-level domain (TLD) extensions, and other global domain registration trends.

We also determined the top 5 TLD extensions used by the more than 58.1 billion domains from our DNS database's A record full file released in July 2024.

Next, we studied the top 5 TLDs and associated threat types of more than 1 million domains detected as indicators of compromise (IoCs) in the same month.

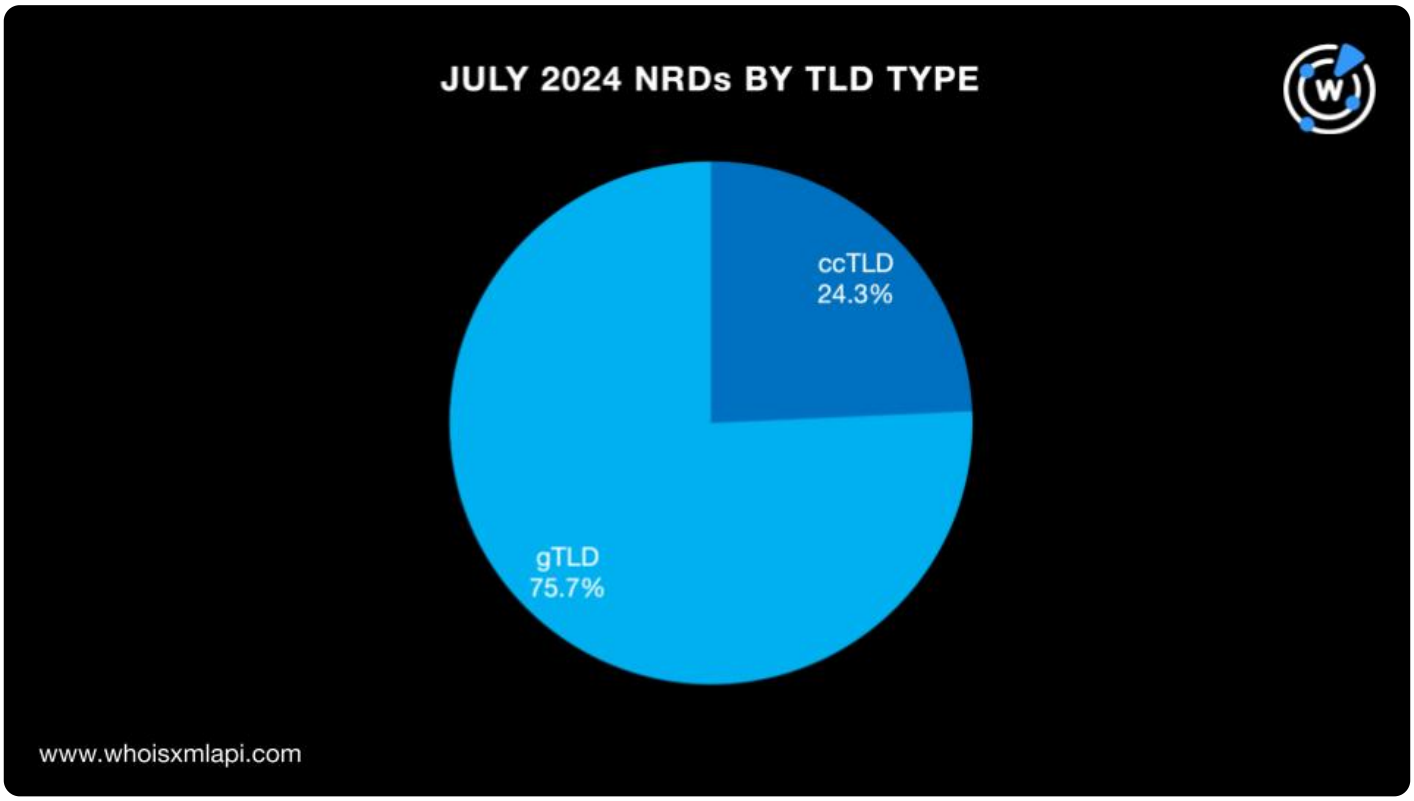
Finally, we summed up our findings and provided links to the threat reports produced using DNS, IP, and domain intelligence sources during the period.

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

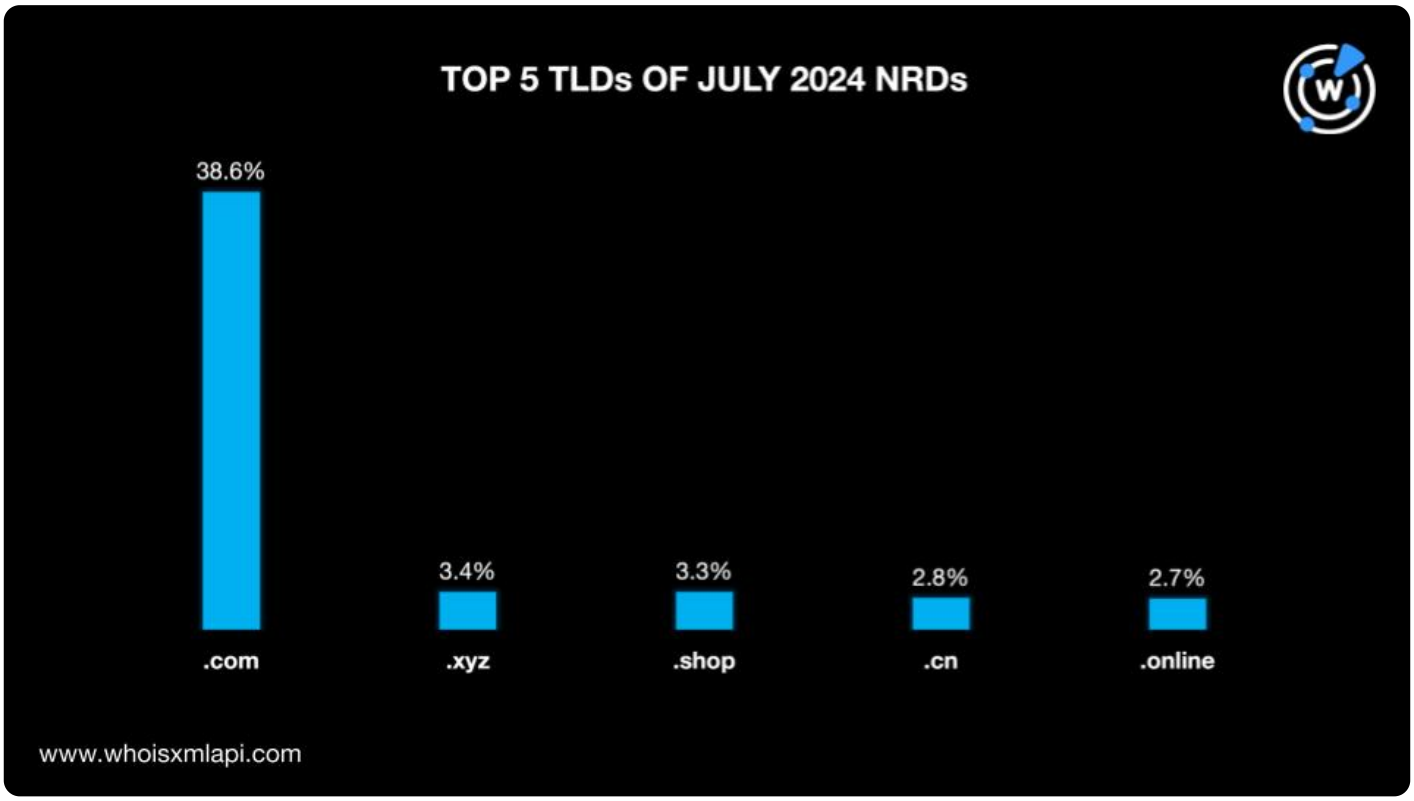
Zooming in on the July NRDs

TLD Distribution

Of the 7.3 million domains registered in July, 75.7% used generic TLD (gTLD) extensions, while 24.3% used country-code TLD (ccTLD) extensions.

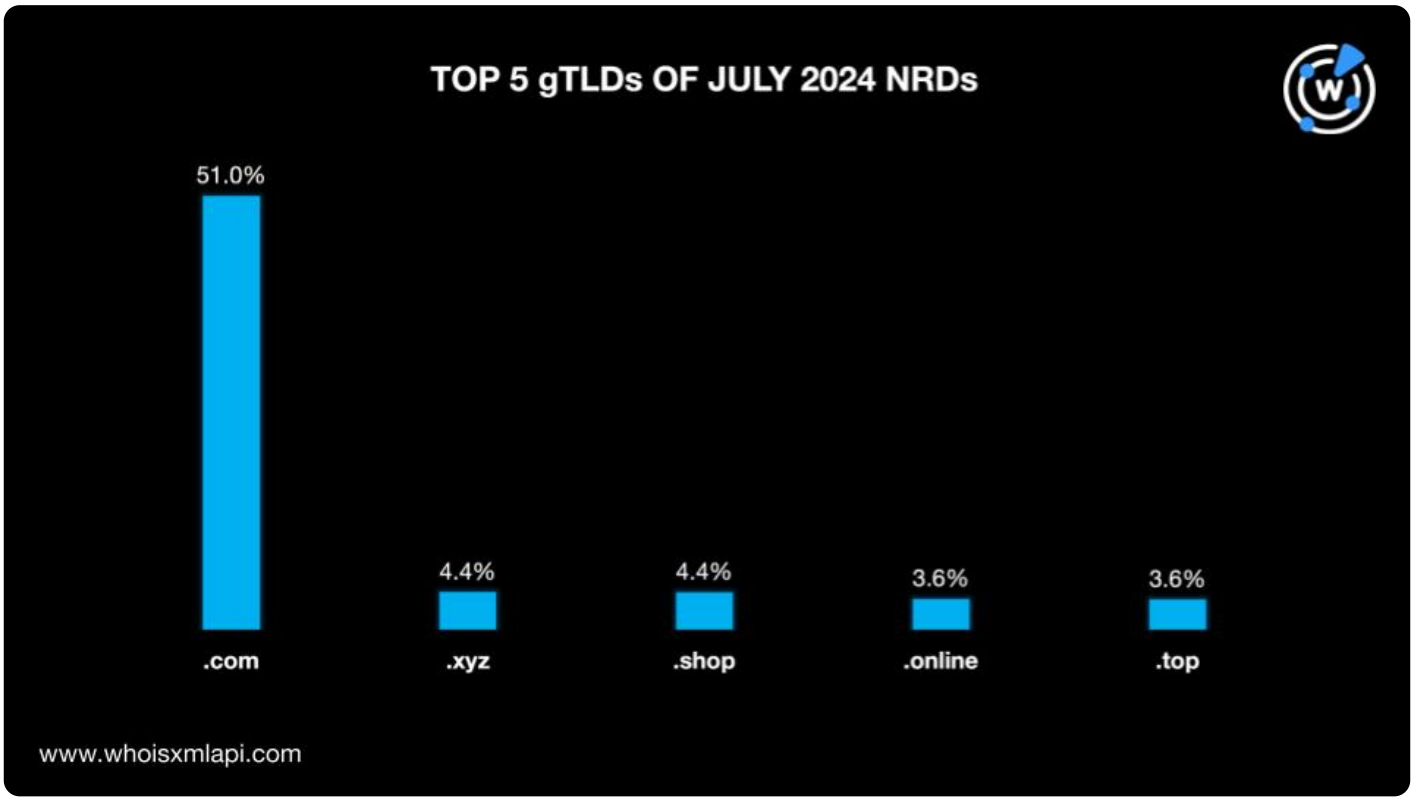


The most popular TLD extension was still .com, accounting for 38.6% of the NRDs. The other most used TLDs on the top 5 followed with a significant gap as in the previous month. They included three other gTLDs and one ccTLD, namely, .xyz and .shop (3.4% each), and .cn and .online (2.8% each).

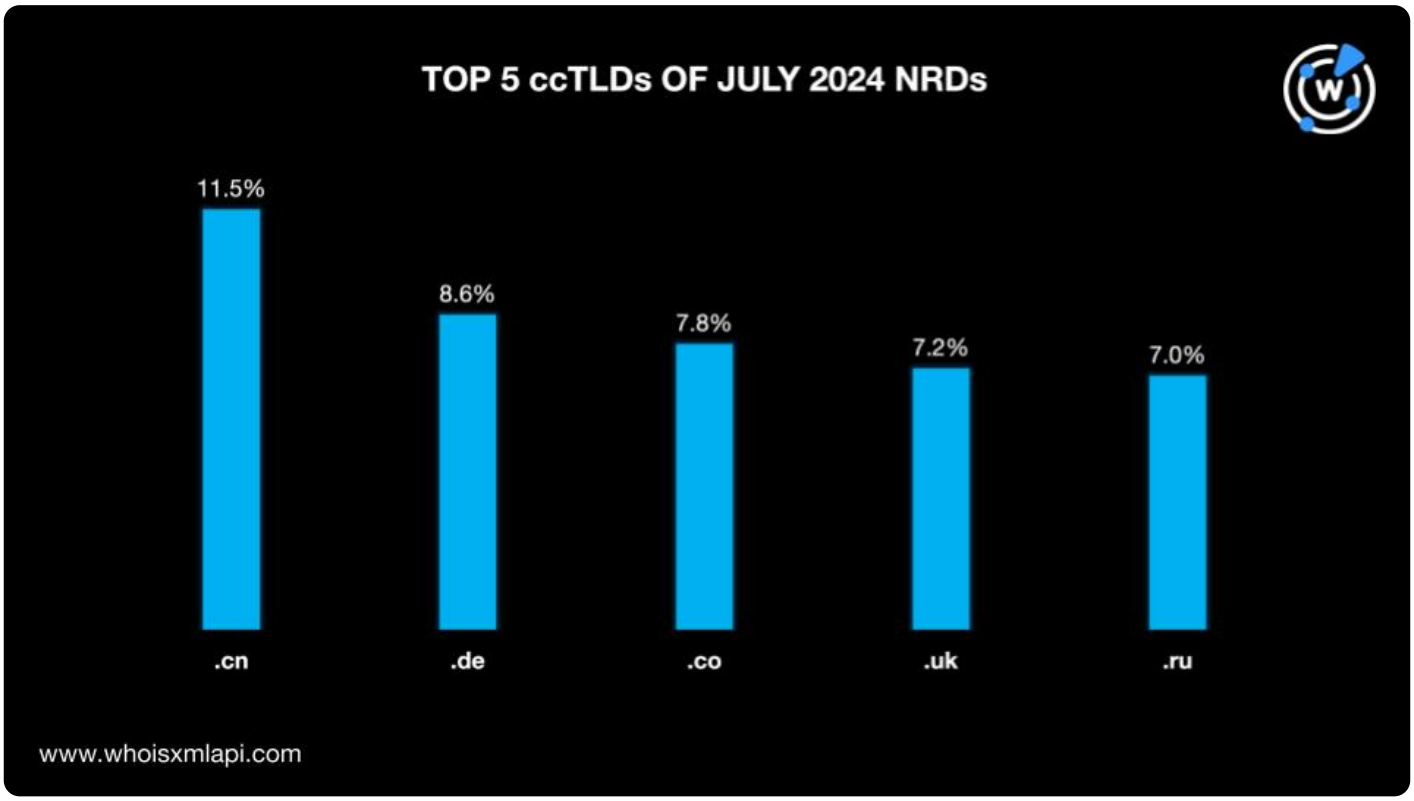


We then analyzed the July TLDs deeper to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 640 gTLDs, .com was the most used, accounting for a 51.0% share. The rest of the top 5 lagged far behind. In fact, .xyz and .shop tied in second place, accounting for only a 4.4% share each. New gTLDs .online and .top tied for the third spot with a 3.6% share each. Note that .net was ousted from the top 3 position it attained in June 2024.

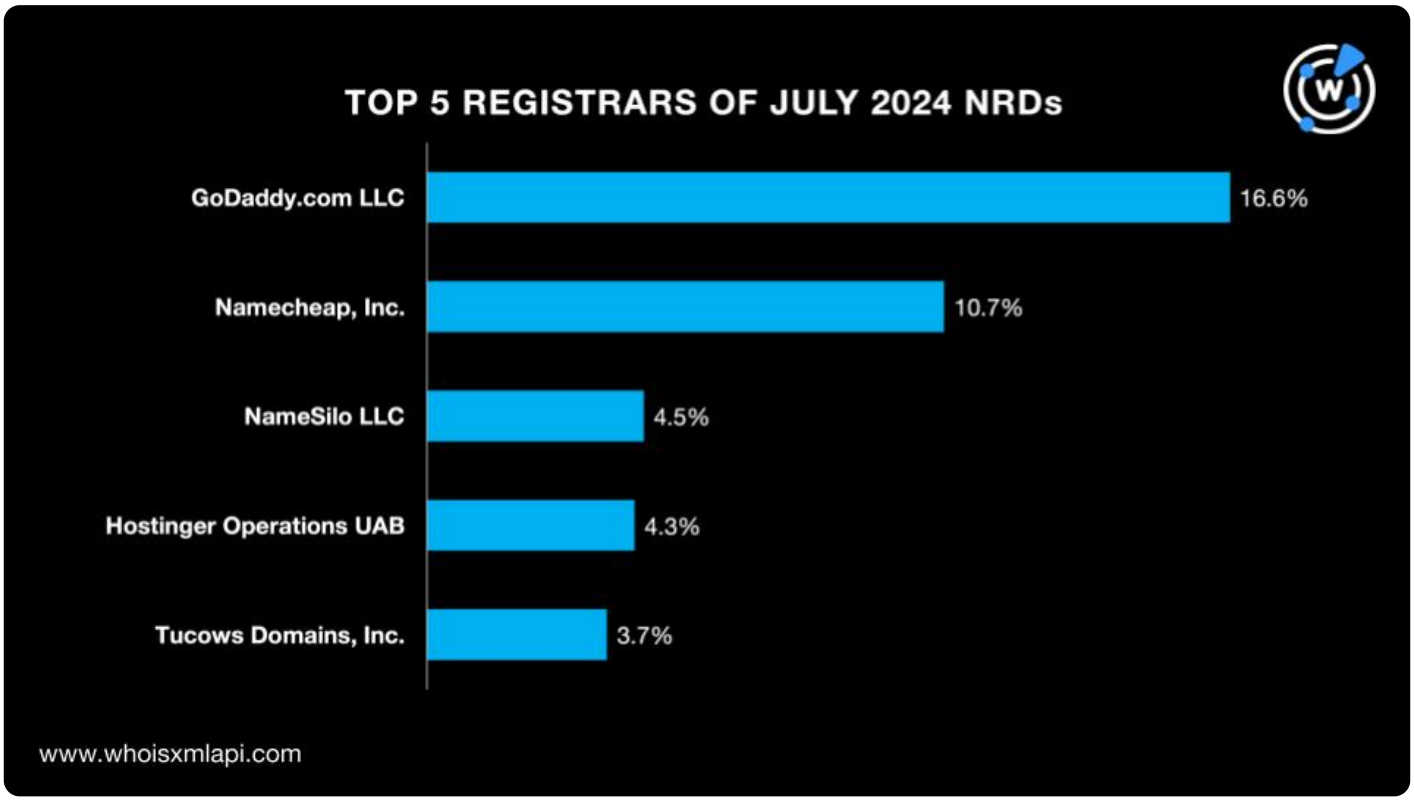


Meanwhile, .cn remained the most used out of 236 ccTLDs with an 11.5% share in July, down from 16.6% in June. The other popularly used ccTLDs included .de (8.6%), .co (7.8%), .uk (7.2%), and .ru (7.0%).



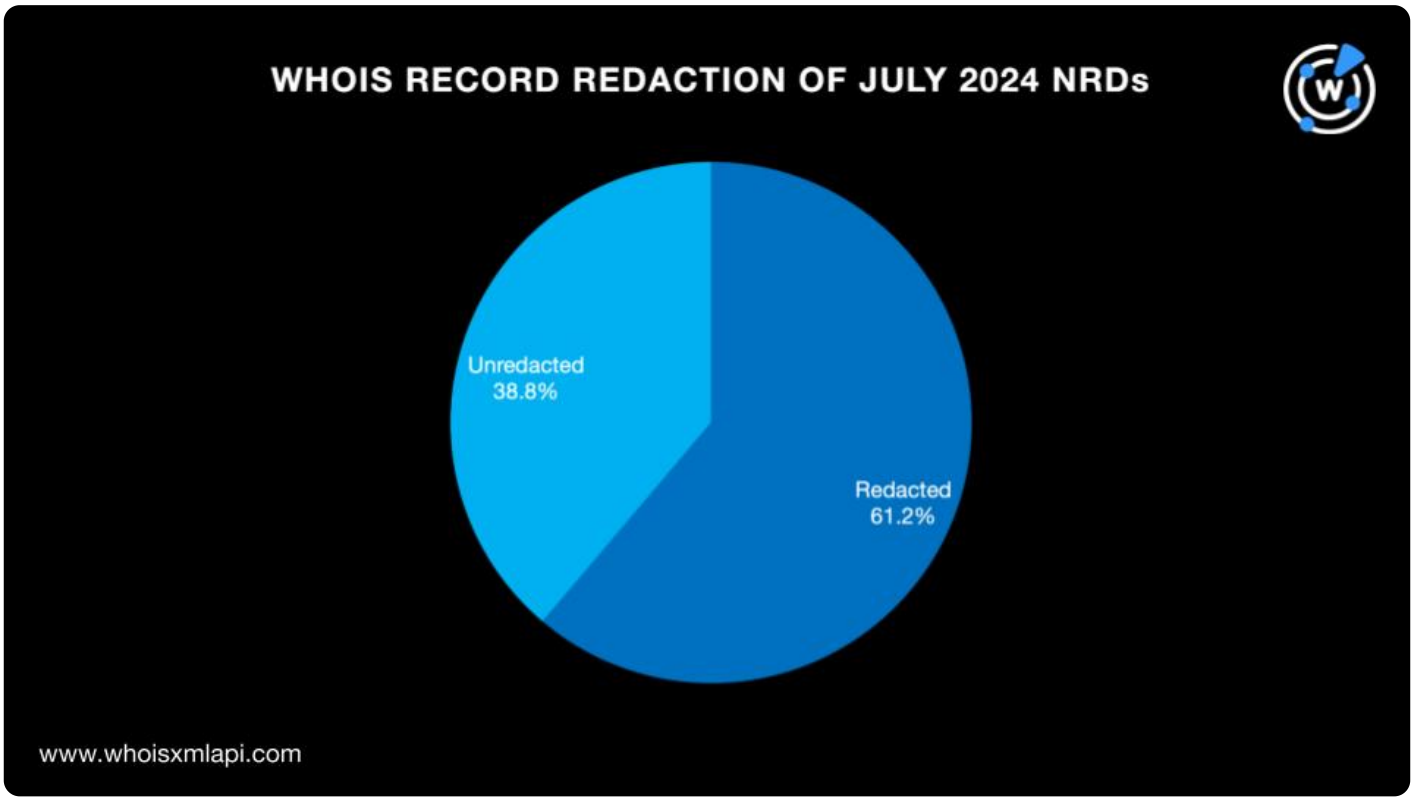
Registrar Distribution

GoDaddy.com LLC remained the most popular registrar, with a 16.6% share in July, 0.2 shy of its June share. Namecheap, Inc. followed in second place with a 10.7% share. NameSilo LLC (4.5%); Hostinger Operations UAB (4.3%); and Tucows Domains, Inc. (3.7%) completed the top 5.



WHOIS Data Redaction

A majority of the NRDs, 61.2%, continued to have redacted WHOIS records, decreasing slightly from 61.9% in June. On the other hand, it means that 38.8% of the July NRDs had public WHOIS records.

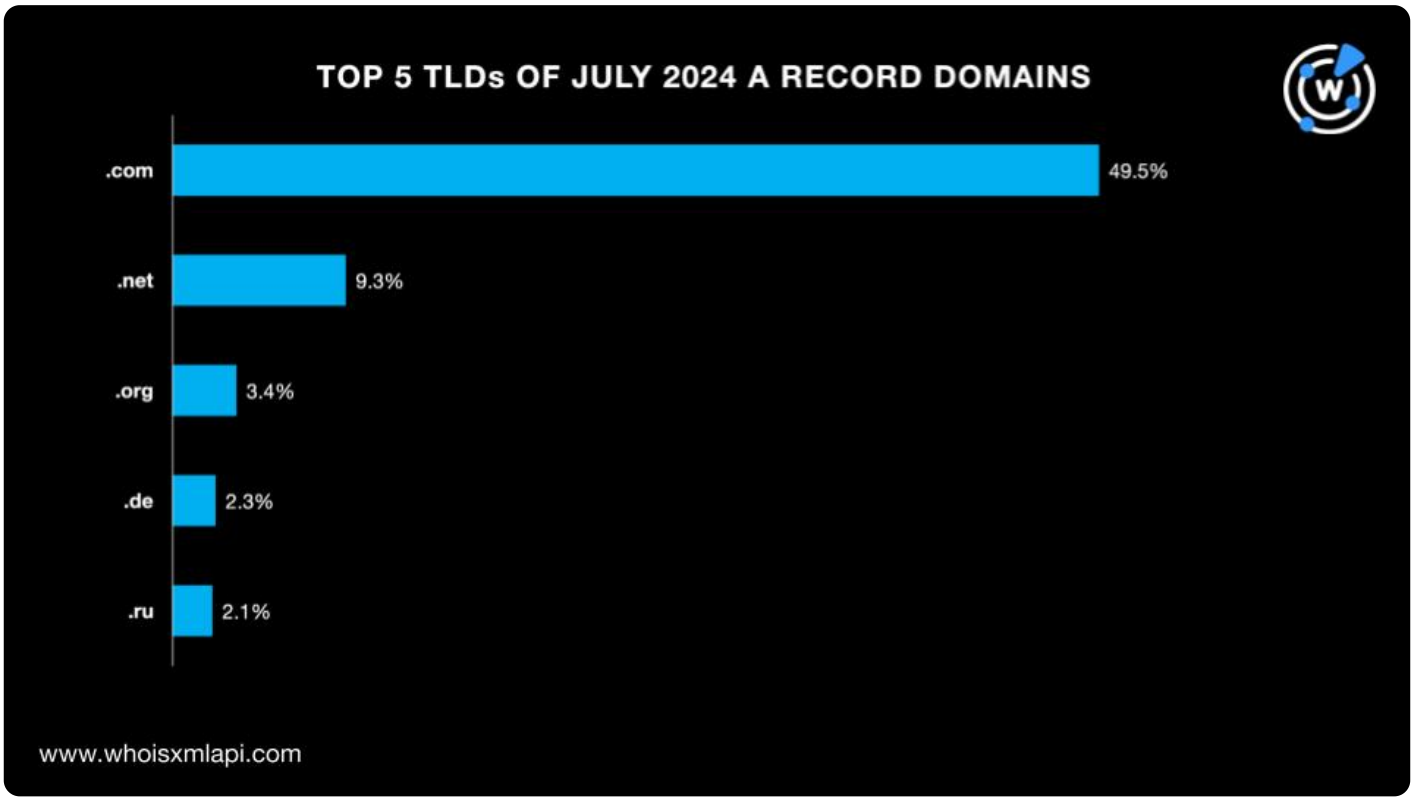


A Closer Look at the July DNS Records

Top TLDs of the A Record Domains

Next, we analyzed more than 58.1 billion domains from our DNS database's A record full file for July 2024, which included DNS resolutions from the past 365 days, and found that almost half (49.5%) used the .com TLD.

The rest of the top 5 comprised two other gTLDs, namely, .net (9.3%) and .org (3.4%), along with two ccTLDs, specifically .de (2.3%) and .ru (2.1%).

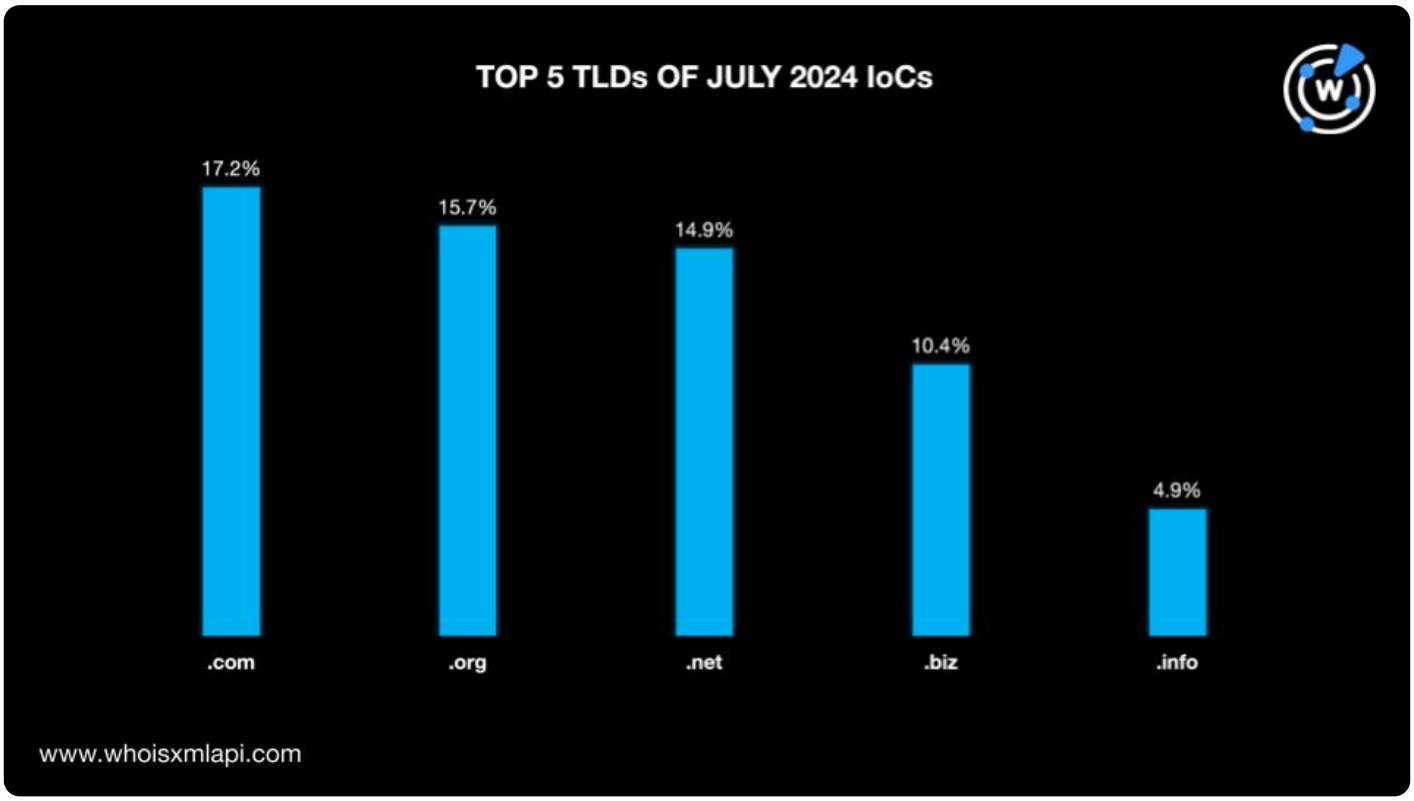


Cybersecurity through the DNS Lens

Top TLDs of the July IoCs

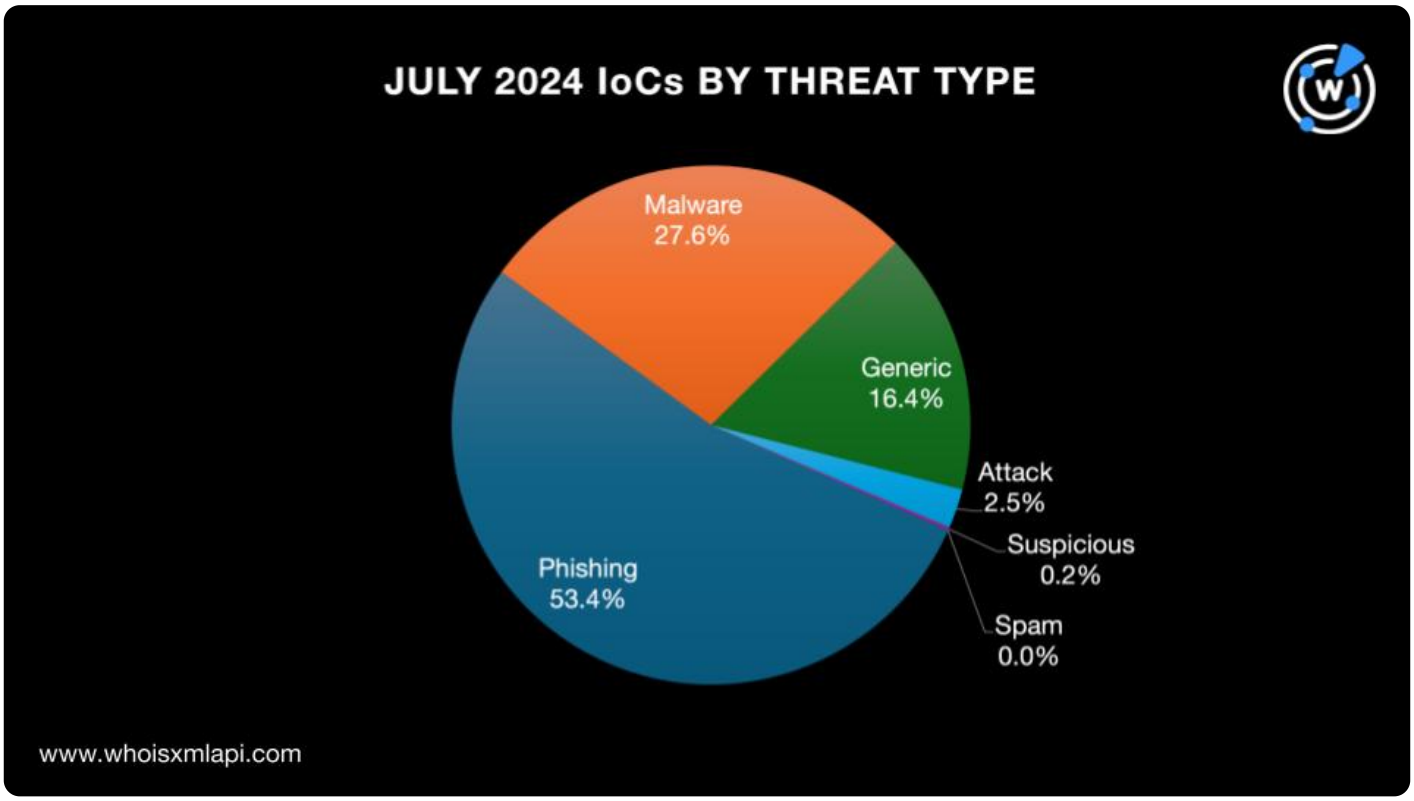
As per usual, we analyzed more than 1 million domains tagged as IoCs for various threats detected in July. Our analysis revealed that .com was the most used gTLD for malicious domains with a 17.2% share of the IoCs.

Interestingly, all of the top 5 TLDs used for the IoCs were major gTLDs. The remaining four were .org (15.7%), .net (14.9%), .biz (10.4%), and .info (4.9%).



Threat Type Breakdown of the July IoCs

When we grouped the July IoCs based on associated threat type, we discovered that a majority, 53.4% to be exact, were associated with phishing. The rest of the IoCs were related to malware distribution (27.6%), generic threats (16.4%), attacks (2.5%), suspicious campaigns (0.2%), and spam campaigns (0.004%).



Threat Reports

Below are some of the threat reports we published in July.

- **The Most Phished Brands of 2024 in the DNS Spotlight:** The WhoisXML API research team conducted a DNS intelligence analysis for the 20 most phished brands of 2024. That led to the discovery of 3,128 domains and subdomains that could be weaponized for phishing campaigns. Fourteen IP addresses that played host to the web properties already classified as IoCs were also named.

- **Uncovering DNS Details on Operation Celestial Force:** The WhoisXML API research team sought to uncover artifacts potentially connected to advanced persistent threat (APT) group Cosmic Leopard's latest campaign dubbed “Celestial Force.” Our IoC list expansion analysis uncovered 3,980 potentially connected threat artifacts.

- **On the Hunt for Remnants of the Samourai Wallet Crypto Mixing Services in the DNS:** The WhoisXML API research team obtained three domains believed to be part of the Samourai Wallet crypto mixing service. Our IoC expansion analysis found 72 artifacts potentially related to the threat.

- **A Peek at the V3B Phishing Kit Attack via the DNS Lens:** The WhoisXML API research team performed an IoC list expansion analysis of 28 domains tagged as IoCs for a V3B Phishing Kit-enabled attack and found 4,808 connected artifacts.

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

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