June 2024: Domain Activity Highlights

Posted on July 11, 2024

The WhoisXML API research team analyzed more than 7.5 million domains registered between 1 and 30 June 2024 to identify the most popular registrars, top-level domain (TLD) extensions, and other global domain registration trends.

After that, we determined the top TLD extensions used by the more than 58.2 billion domains from our DNS database's A record full file released in June 2024.

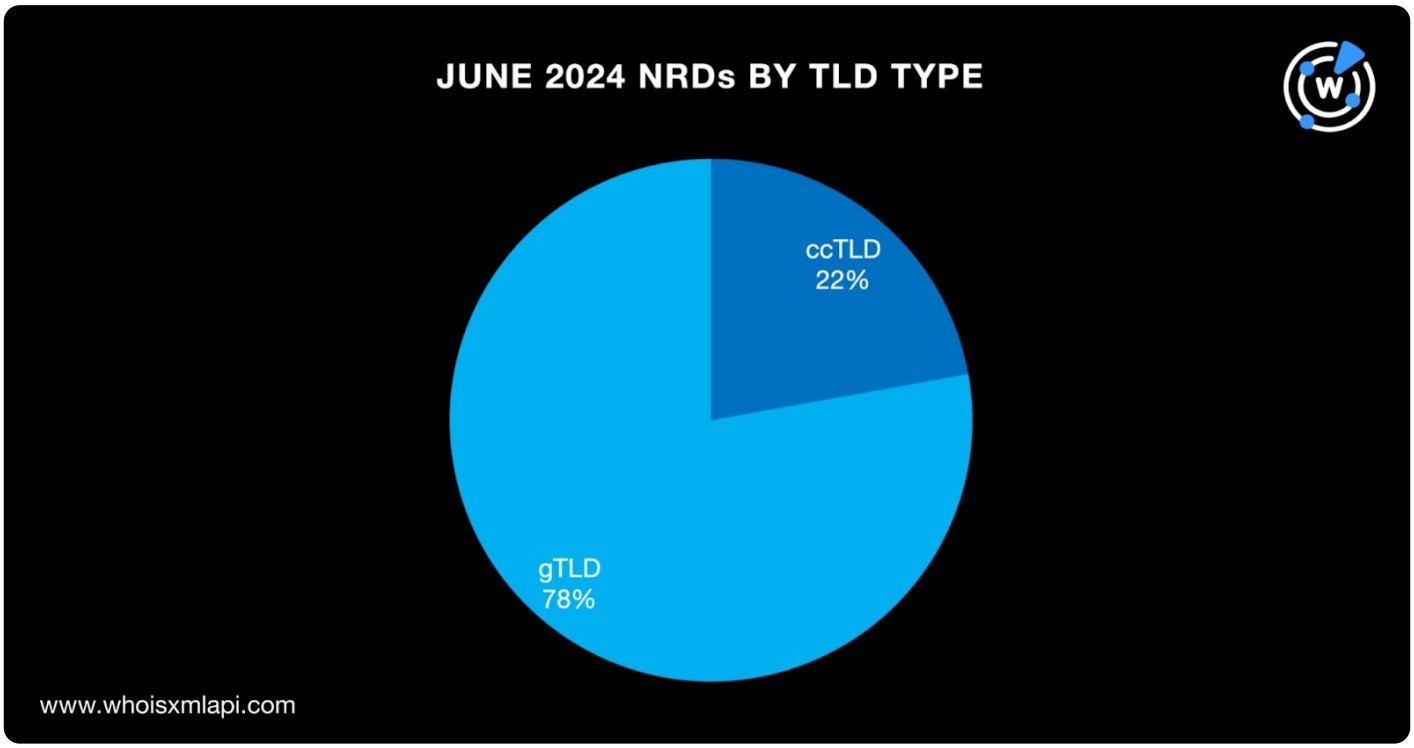
We also studied the top TLDs and associated threat types of more than 1.1 million domains detected as indicators of compromise (IoCs) in June.

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

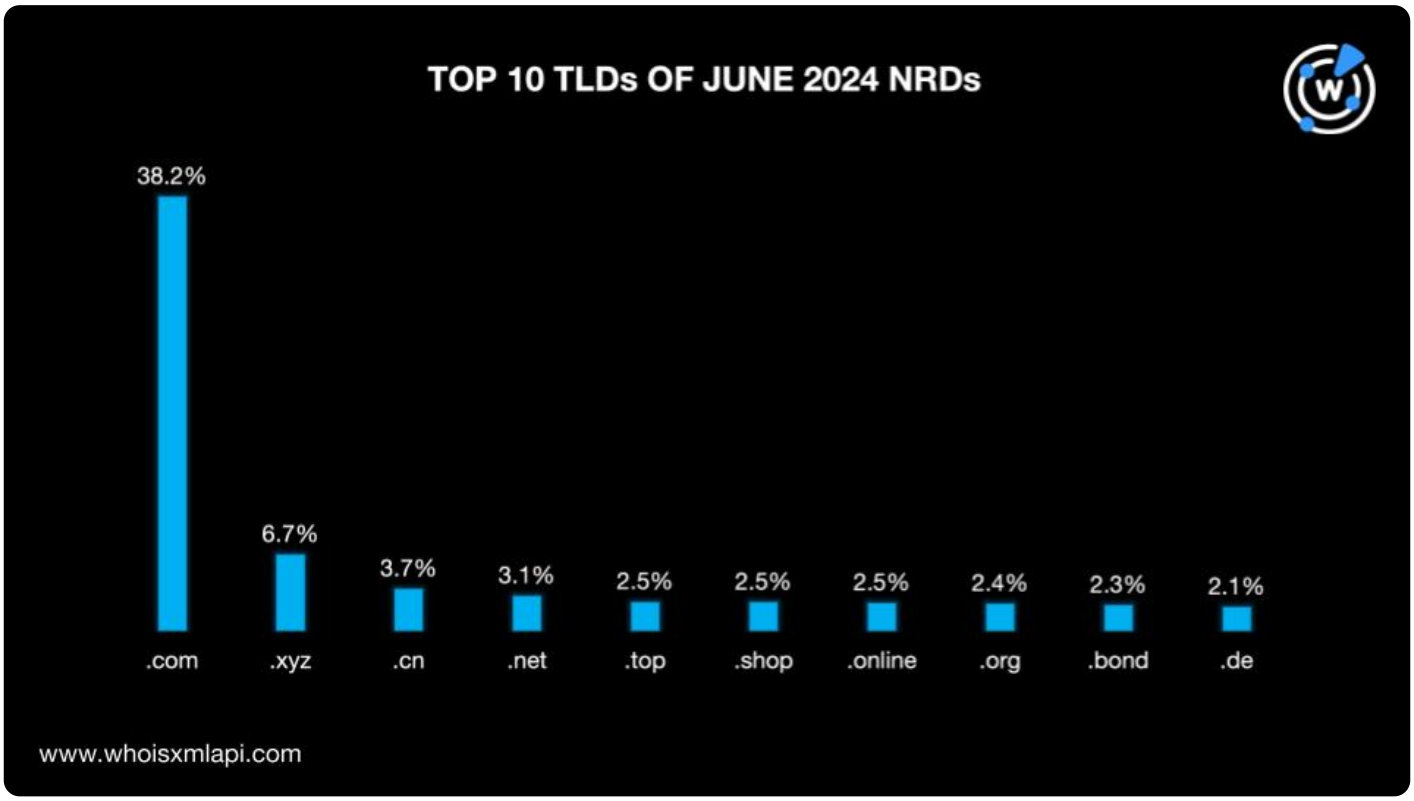
Zooming in on the June NRDs

TLD Distribution

Of the 7.5 million domains registered in June, 77.8% used generic TLD (gTLD) extensions, while 22.2% used country-code TLD (ccTLD) extensions.

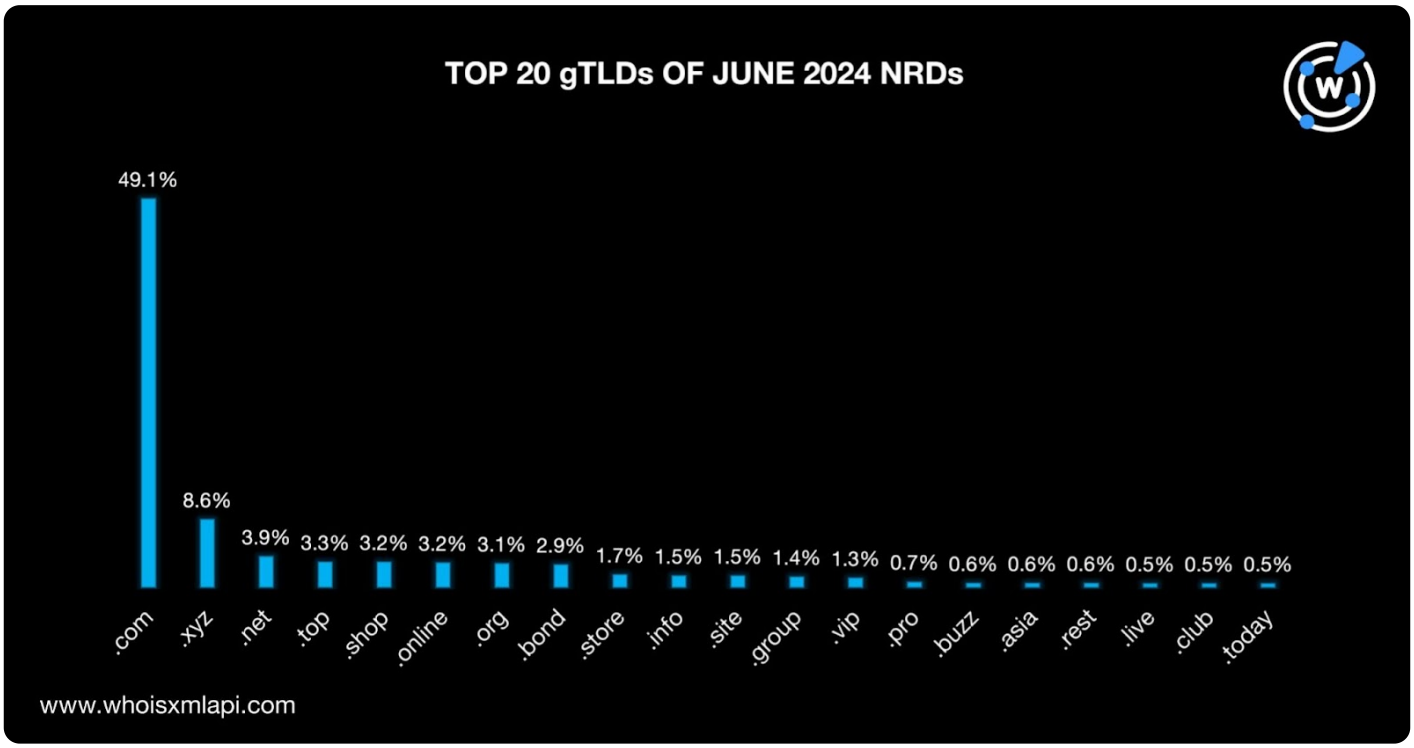


The most popular TLD extension remained .com, accounting for 38.2% of the NRDs. The other most used TLDs on the top 10 followed with a significant gap as in the previous month. They included seven other gTLDs and two ccTLDs, namely, .xyz (6.7%); .cn (3.7%); .net (3.1%); .top, .shop, and .online (2.5%); .org (2.4%); .bond (2.3%); and .de (2.1%).



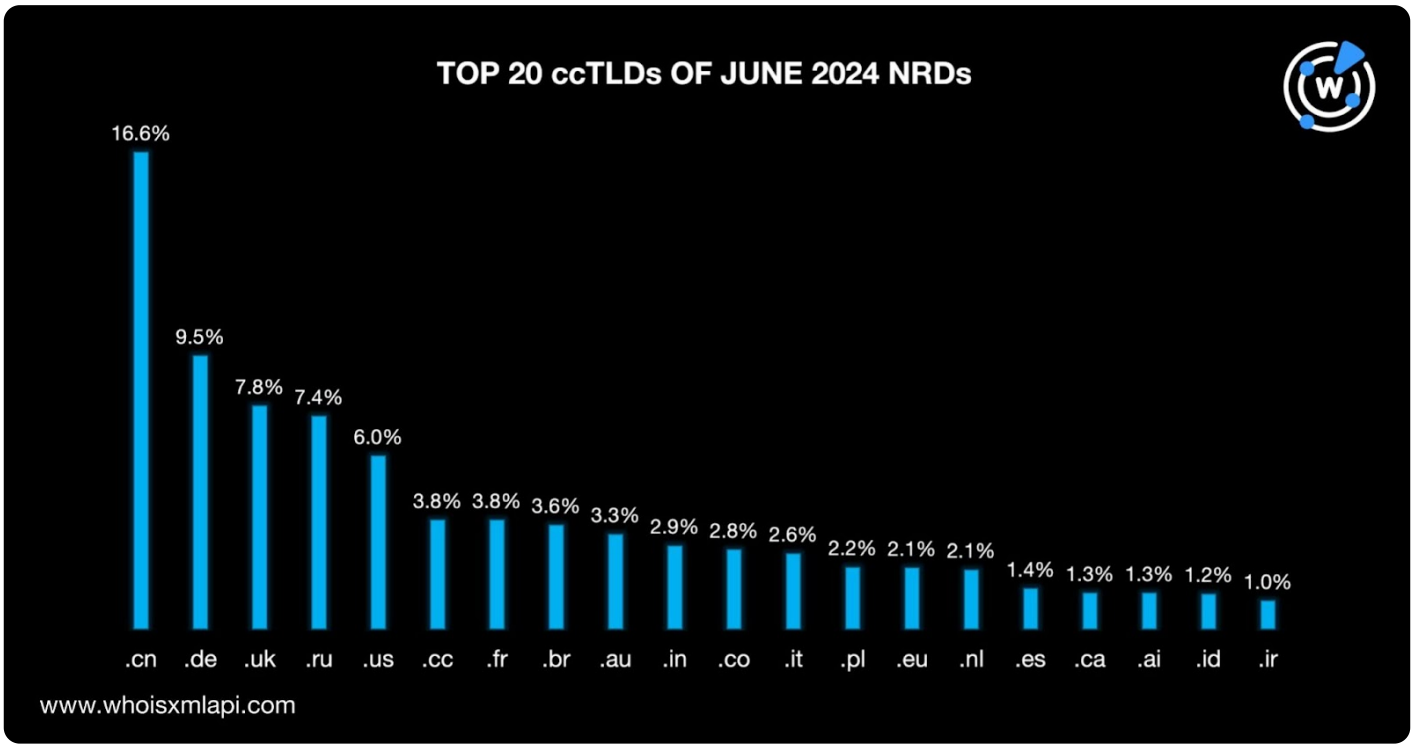
We then analyzed the June TLDs deeper to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of 654 gTLDs, .com was the most used, accounting for a 49.1% share. The rest of the top 20 lagged far behind. In fact, .xyz was second on the list, accounting for only a 8.6% share. One of the oldest gTLDs .net came in third with a 3.9% share, followed by .top with 3.3%. The rest of the most used gTLDs included .shop and .online (3.2%); .org (3.1%); .bond (2.9%); .store (1.7%); .info and .site (1.5%); .group (1.4%); .vip (1.3%); .pro (0.7%); .buzz, .asia, and .rest (0.6%); and .live, .club, and .today (0.5%).



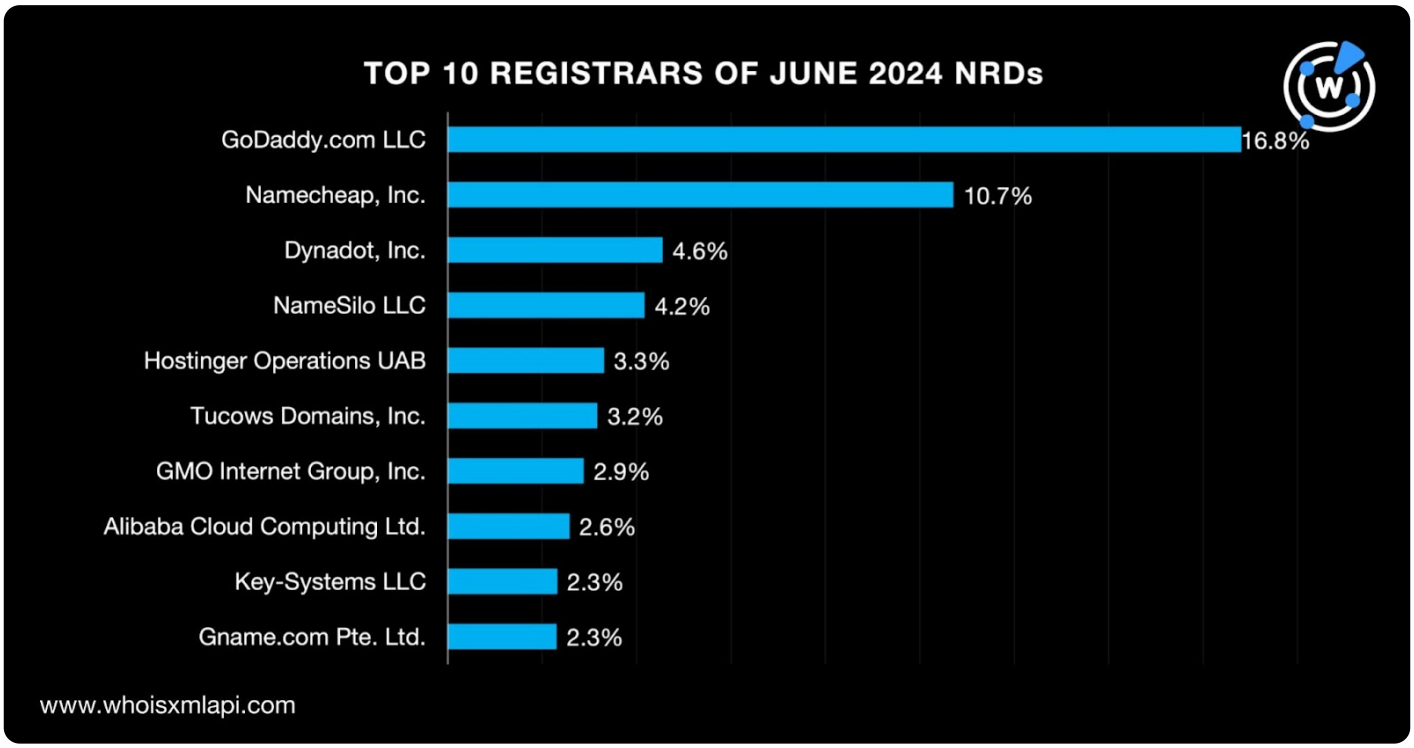
Meanwhile, .cn remained the most used out of 239 ccTLDs with 16.6% share in June, down from 17.9% in May. The other popular ccTLDs included .de (9.5%), .uk (7.8%), .ru (7.4%), .us (6.0%), .cc and .fr (3.8%), .br (3.6%), .au (3.3%), .in (2.9%), .co (2.8%), .it (2.6%), .pl (2.2%), .eu and .nl (2.1%), .es (1.4%), .ca and .ai (1.3%), .id (1.2%), and .ir (1.0%).

All in all, the top 20 ccTLD extensions accounted for 82.6% of the total for June NRDs.



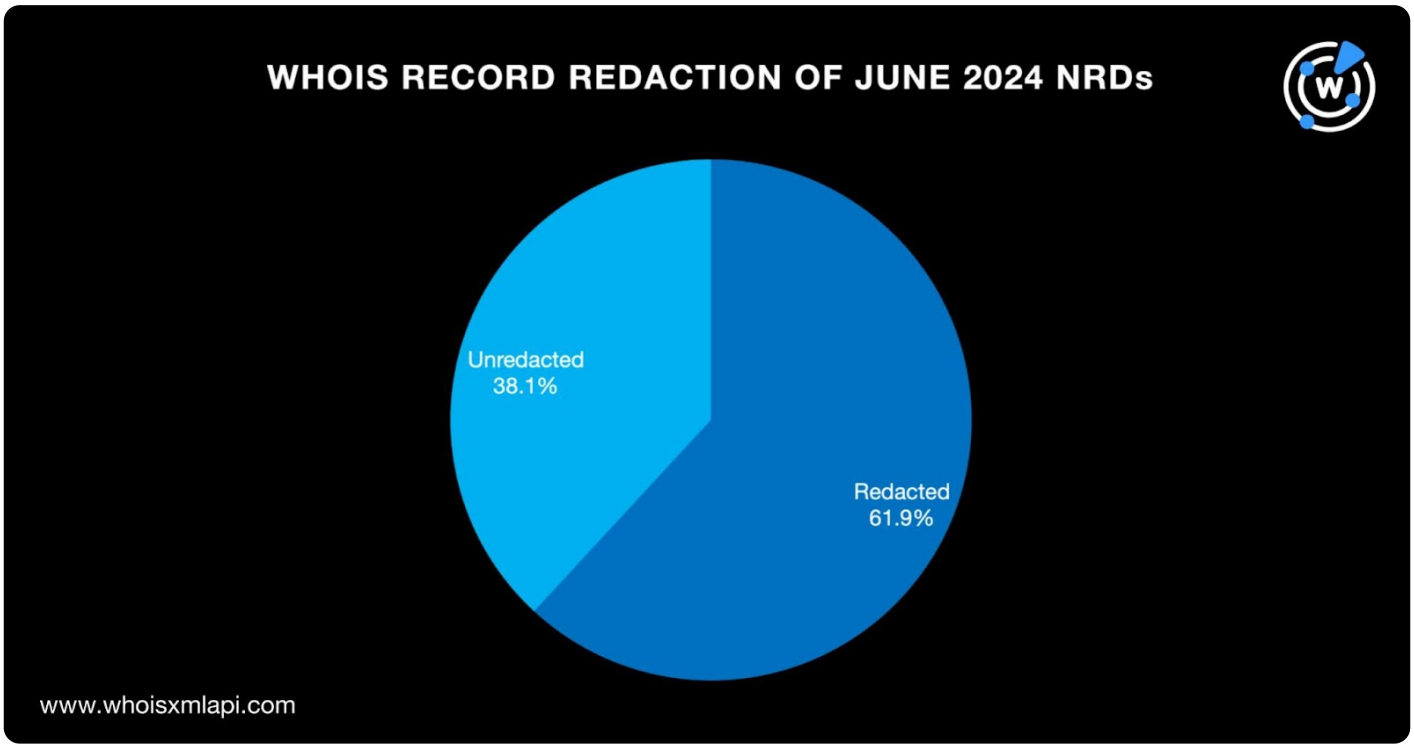
Registrar Distribution

GoDaddy.com LLC remained the most popular registrar, maintaining its 16.8% share from May to June. It was followed by Namecheap, Inc. (10.7%); Dynadot, Inc. (4.6%); NameSilo LLC (4.2%); Hostinger Operations UAB (3.3%); Tucows Domains, Inc. (3.2%); GMO Internet Group, Inc. (2.9%); Alibaba Cloud Computing Ltd. (2.6%); and Key-Systems LLC and Gname.com Pte. Ltd. (2.3%).



WHOIS Data Redaction

A majority of the NRDs, 61.9% to be exact, continued to have redacted WHOIS records, increasing slightly from 60.3% in May. On the other hand, 38.1% of the June NRDs had public WHOIS records.

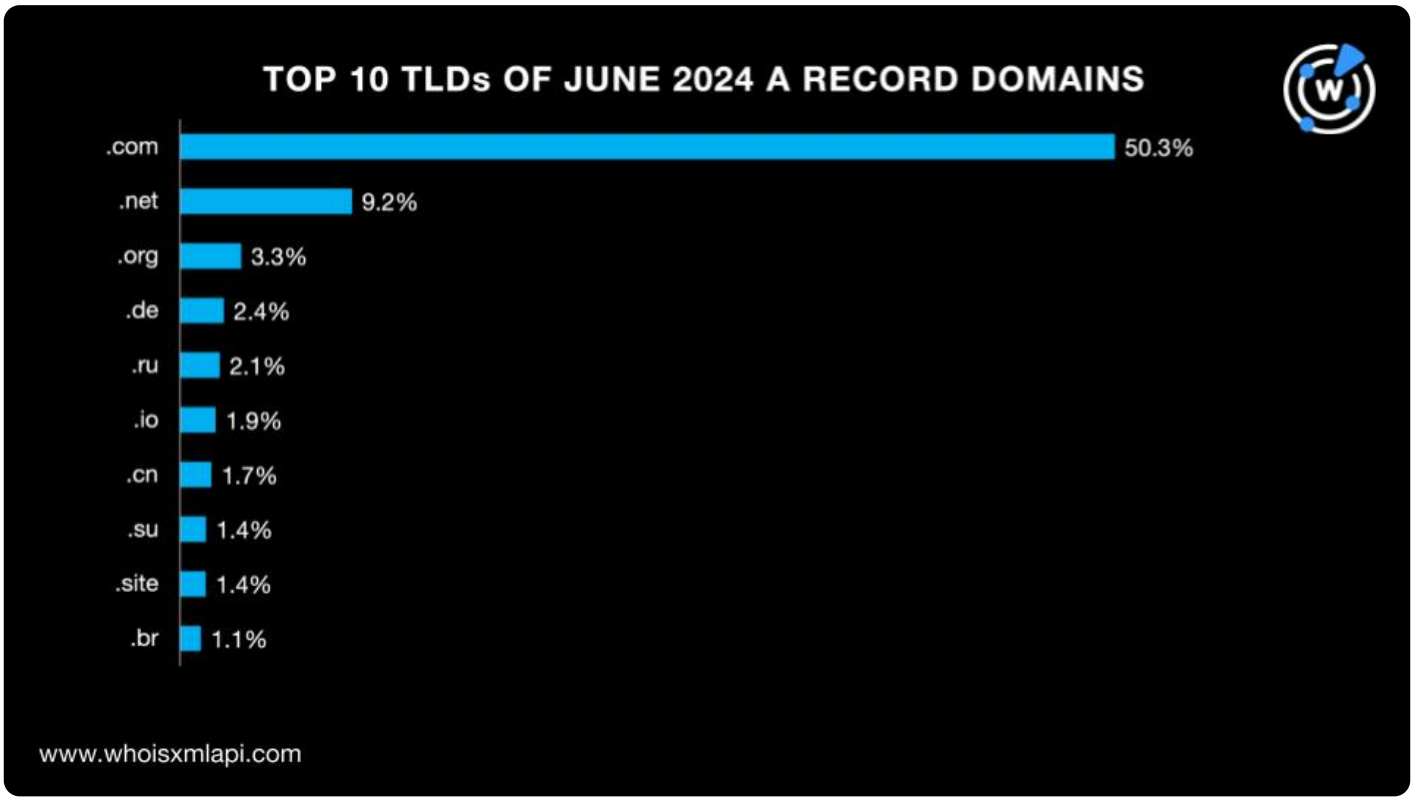


A Closer Look at the June DNS Records

Top TLDs of the A Record Domains

Next, we analyzed over 58.2 billion domains from our DNS database's A record full file for June 2024, which included DNS resolutions from the past 365 days, and found that a majority (50.3%) used the .com TLD.

The rest of the top 10 comprised three other gTLDs—.net (9.2%), .org (3.3%), and .site (1.4%)—and six ccTLDs—.de (2.4%), .ru (2.1%), .io (1.9%), .cn (1.7%), .su (1.4%), and .br (1.1%).

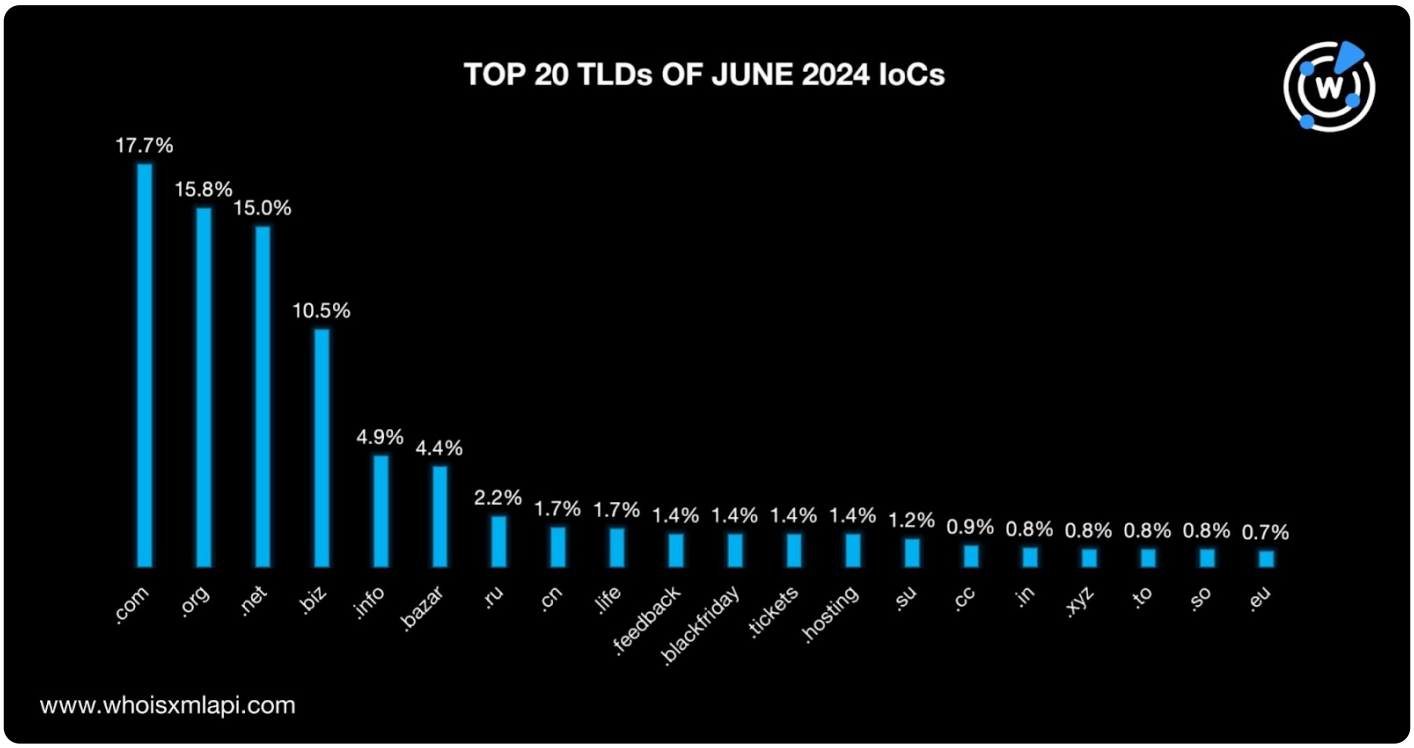


Cybersecurity through the DNS Lens

Top TLDs of the June IoCs

As per usual, we analyzed more than 1.1 million domains tagged as IoCs for various threats detected in June. Our analysis revealed that .com was the most used gTLD for malicious domains with a 17.7% share of the IoCs.

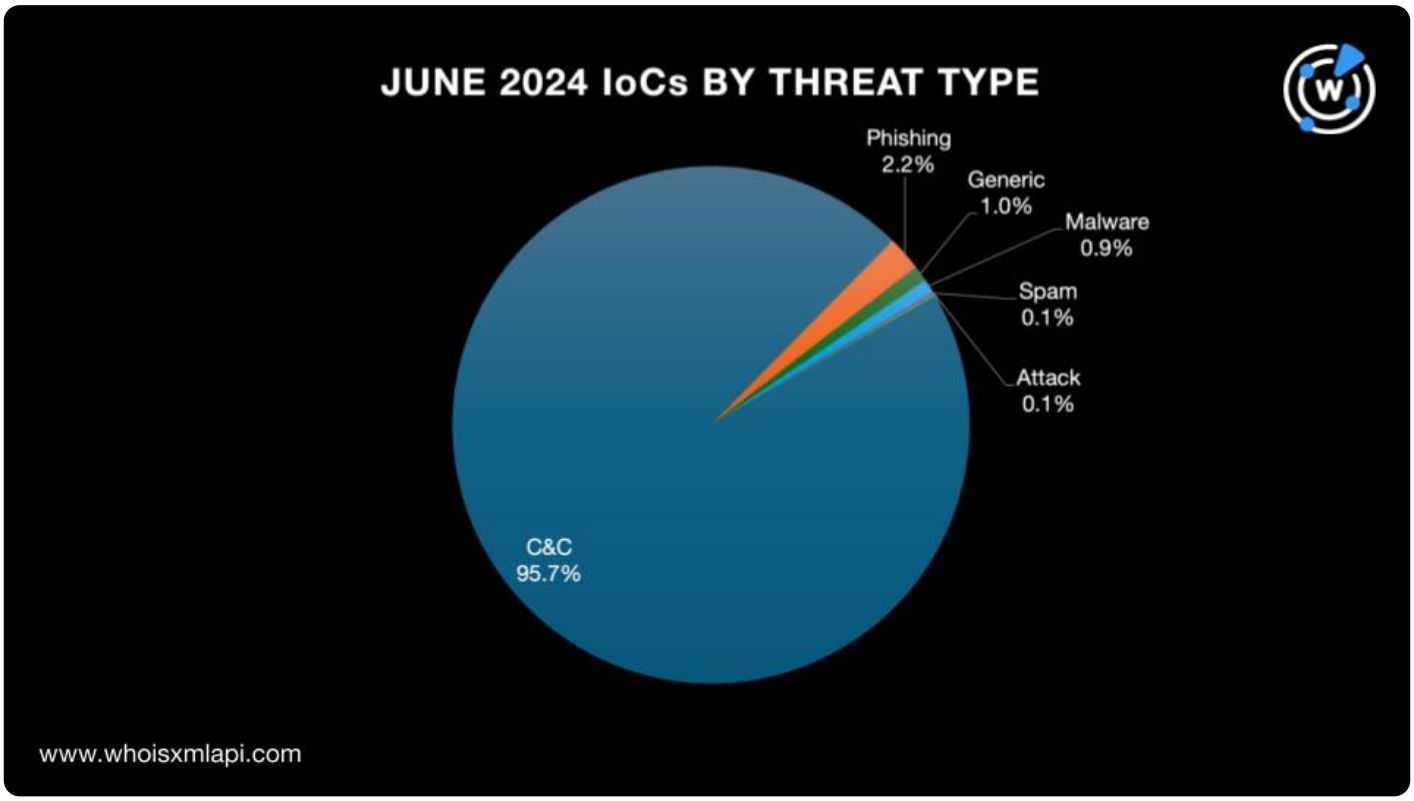
Other major gTLD extensions were also used, such as .org (15.8%), .net (15.0%), .biz (10.5%), and .info (4.9%). Some malicious domains also sported ccTLD extensions, namely, .ru (2.2%); .cn (1.7%); .su (1.2%); .cc (0.9%); .in, .to, and .so (0.8%), and .eu (0.7%). Finally, the remaining IoCs used other gTLDs, specifically .bazar (4.4%); .life (1.7%); .feedback, .blackfriday, .tickets, and .hosting (1.4%); and .xyz (0.8%).



Threat Type Breakdown of the June IoCs

When we grouped the June IoCs based on associated threat type, we discovered that almost all, 95.7% to be exact, were associated with command and control (C&C). This number increased slightly from 95.5% in May.

The rest of the IoCs were related to phishing (2.2%), generic threats (1.0%), malware distribution (0.9%), and spamming and other attacks (0.1%).



Threat Reports

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

- **On the DNS Trail of the Foxit PDF Bug Exploitation Attackers:** The WhoisXML API research team obtained a total of nine IoCs—eight domain names and one IP address—pertaining to the Foxit PDF bug exploitation. Our IoC list expansion analysis led to the discovery of 108 artifacts possibly connected to the threat.

- **Following the DNS Trail of APT Group Newbie Unfading Sea Haze:** The WhoisXML API research team sought to follow the APT group Unfading Sea Haze's digital breadcrumbs in the DNS to identify more connected artifacts. Our IoC list expansion analysis uncovered 1,299 potentially connected threat artifacts.

- **Tracking Down Fake Cryptocurrency Sellers Using DNS Intelligence:** The WhoisXML

API research team obtained a list of 130 domains believed to belong to fake crypto sellers. Our IoC expansion analysis found more than 2,700 artifacts potentially 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.