May 2024: Domain Activity Highlights

Posted on June 14, 2024

WhoisXML API researchers analyzed more than 7.4 million domains registered between 1 and 31 May 2024 to identify the most popular registrars, top-level domain (TLD) extensions, and other global domain registration trends.

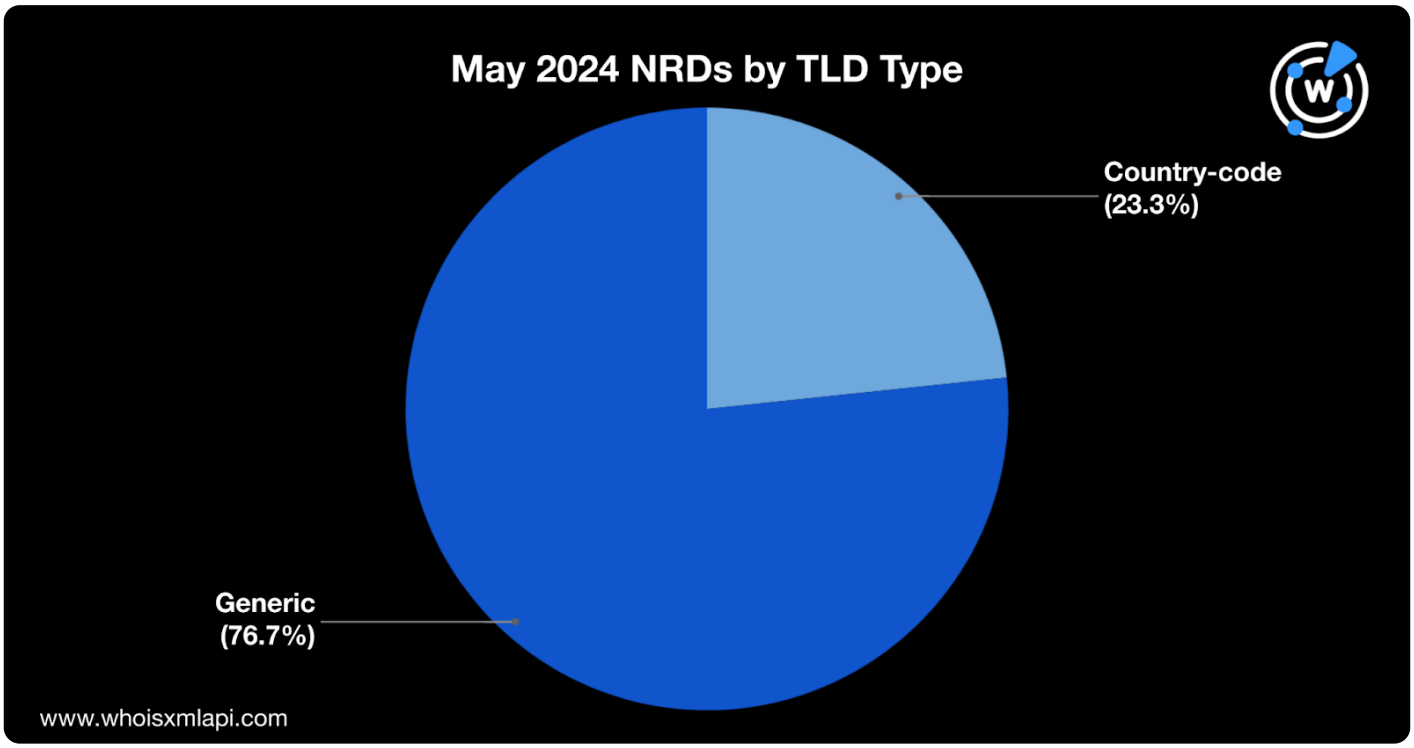
We also studied the top TLDs and associated threat types of more than 1 million domains detected as indicators of compromise (IoCs) in May.

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

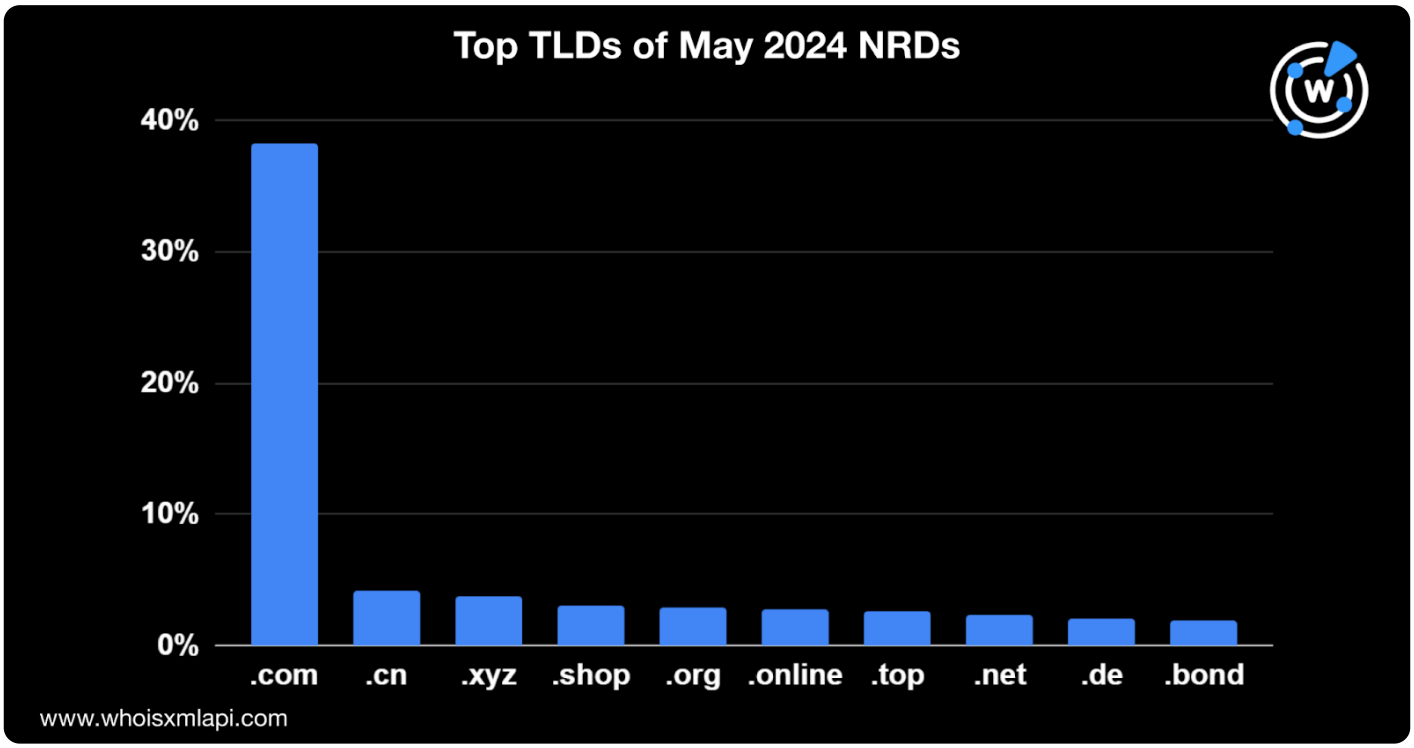
Zooming in on the May NRDs

TLD Distribution

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

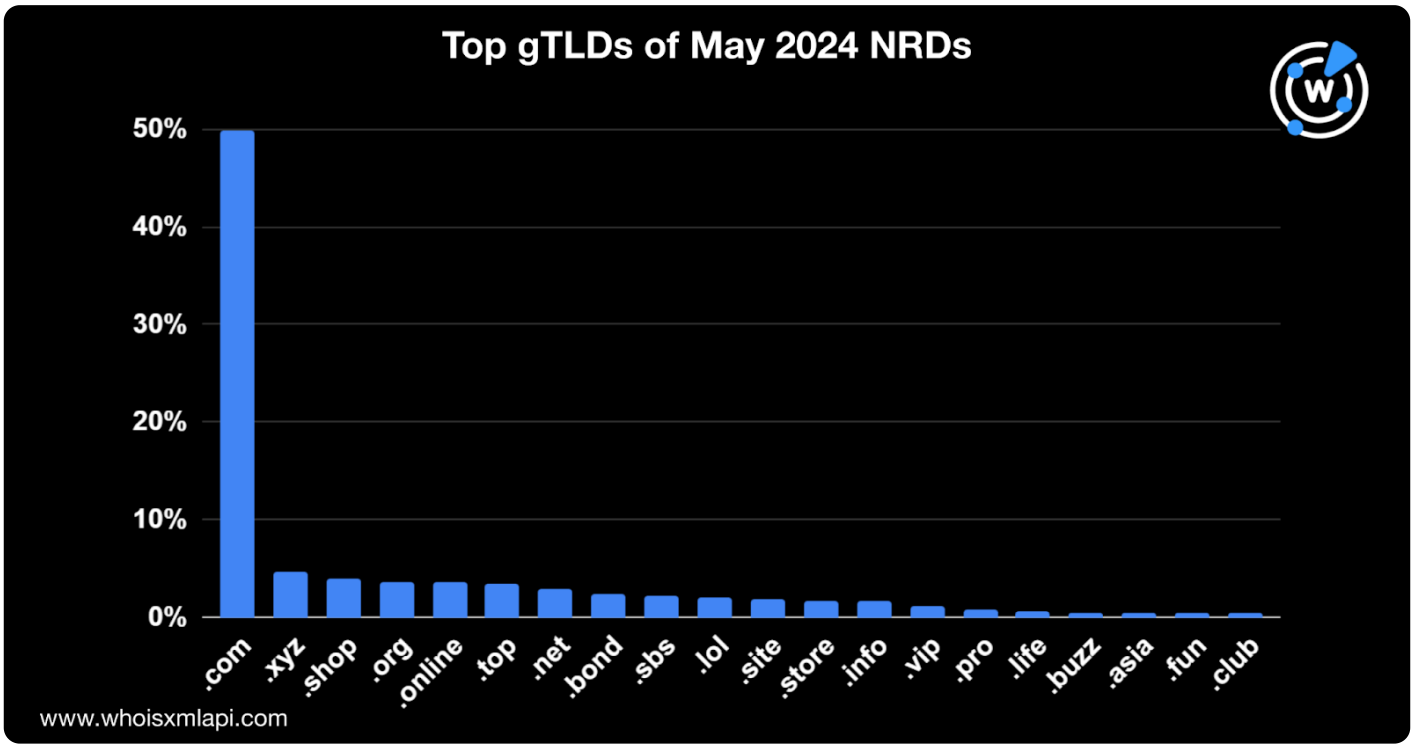


The most popular TLD extension was still .com, accounting for 38.3% of the NRDs. The other TLDs on the top 10 most used TLDs followed with a significant gap as in the previous months. They include seven gTLDs and two ccTLDs, namely, .cn (4.2%), .xyz (3.7%), .shop (3.1%), .org (2.9%), .online (2.7%), .top (2.6%), .net (2.3%), .de (2%), and .bond (1.8%).



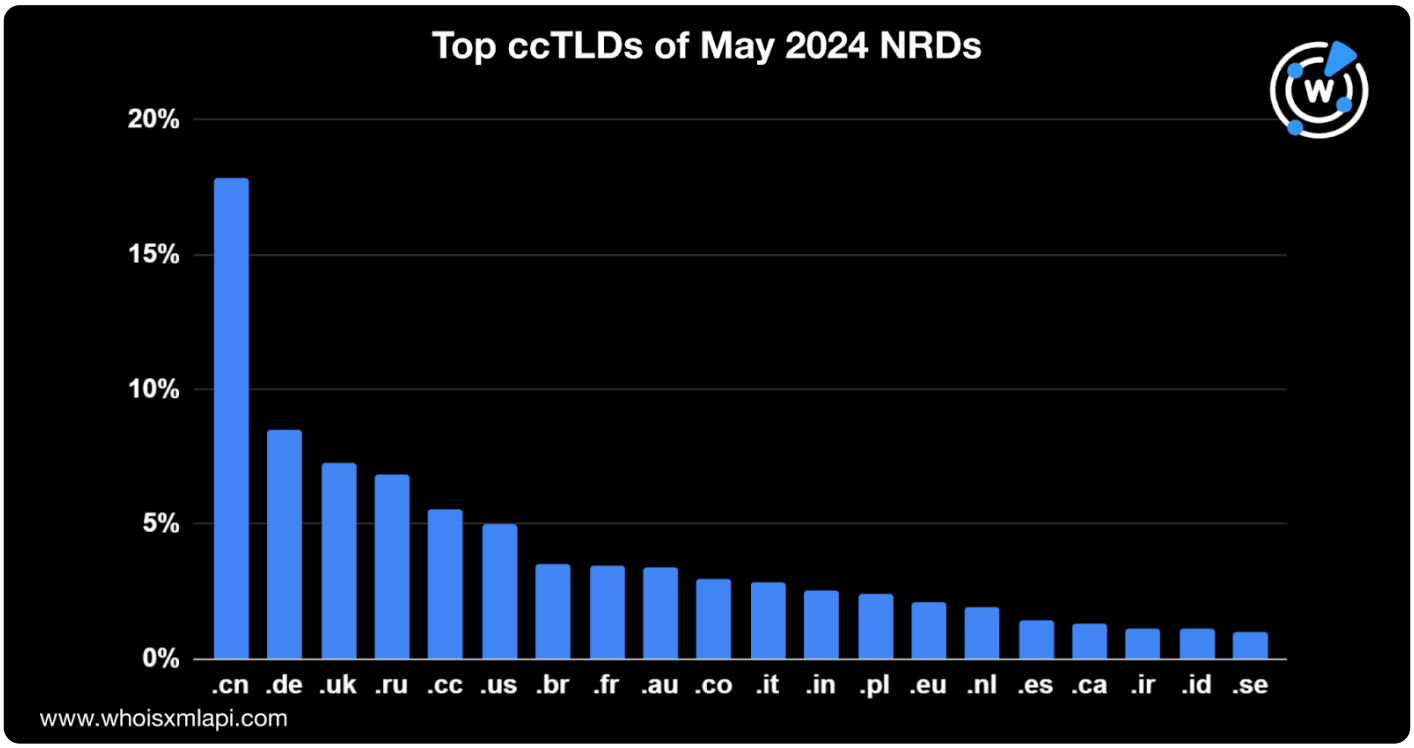
We analyzed the May TLDs deeper to identify the most popular gTLDs and ccTLDs among the new domain registrations.

Out of more than 630 gTLDs, .com was the most used, accounting for 49.9% of the NRDs. The rest of the top 20 lagged far behind. In fact, .xyz was second on the list, accounting for only 4.8% of the NRDs. E-commerce-related gTLD .shop came next with a 4% share, followed by .org with 3.7%. The rest of the most used gTLDs included .online (3.6%), .top (3.5%), .net (3%), .bond (2.4%), .sbs (2.3%), .lol (2.1%), .site (1.8%), .store (1.7%), .info (1.7%), .vip (1.2%), .pro (0.8%), .life (0.6%), .buzz (0.6%), .asia (0.6%), .fun (0.5%), and .club (0.5%).



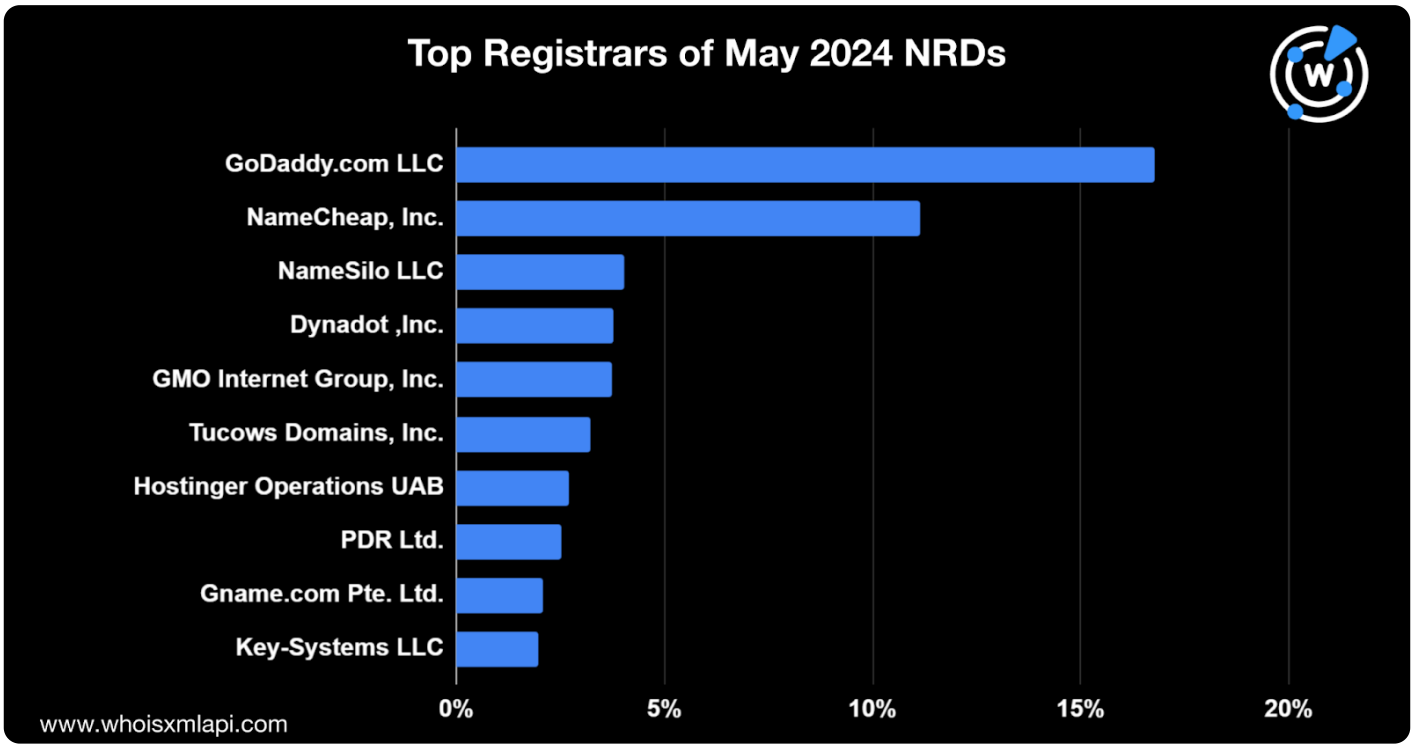
On the other hand, .cn remained the most used out of more than 230 ccTLDs, increasing from 12.4% new domains in April to 17.9% share in May. The other popular ccTLDs included .de with a 8.5% share; .uk with 7.3%, .ru with 6.9%, .cc with 5.5%, .us with 5%, .br and .fr with 3.5% each, .au with 3.4%, .co with 3%, .it with 2.8%, .in with 2.5%, .pl with 2.4%, .eu with 2.1%, .nl with 1.9%, .es with 1.4%, .ca with 1.3%, .ir and .id with 1.1% each, and .se with 1%.

In total, the top 20 extensions accounted for 82% of the May NRDs with ccTLD extensions.



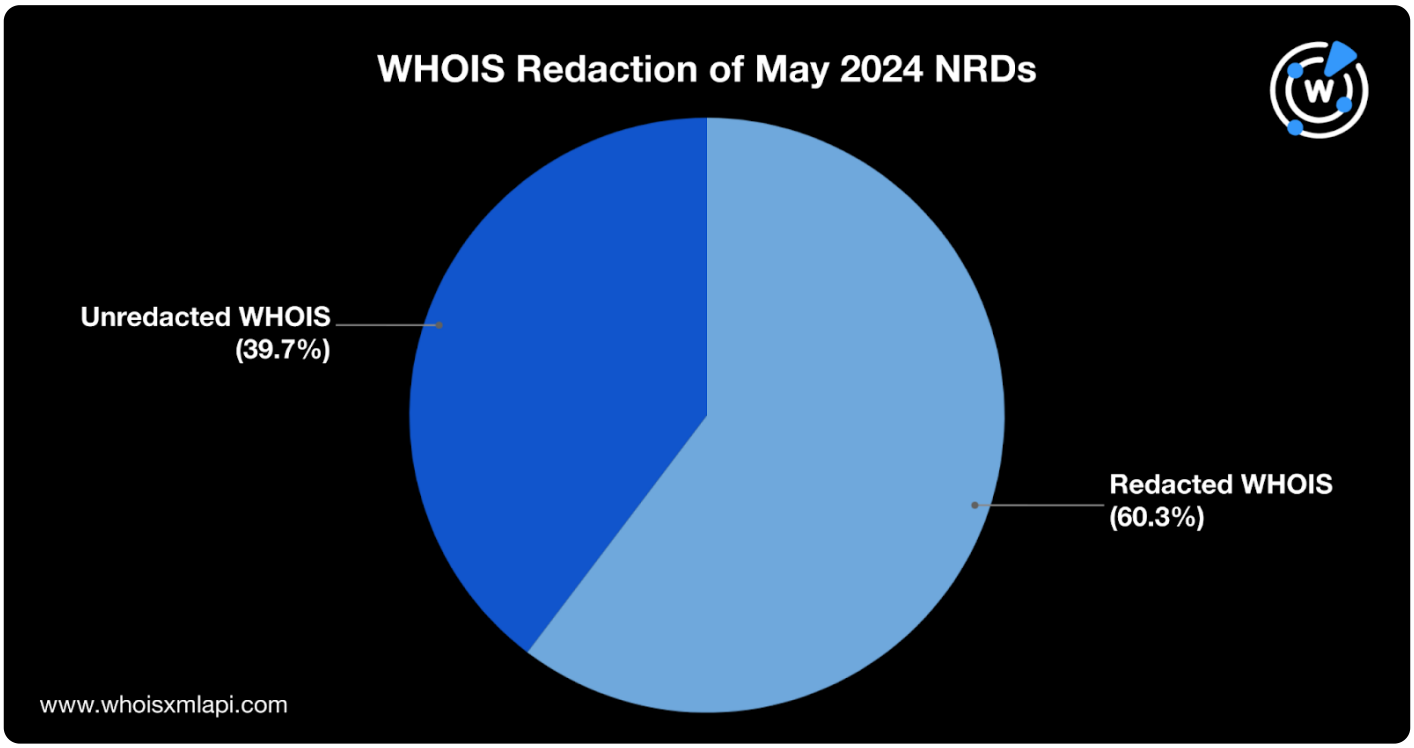
Registrar Distribution

GoDaddy.com LLC remained the most popular registrar, although its share dropped slightly from 18.1% in April to 16.8% in May. It was followed by Namecheap, Inc. (11.1%); NameSilo LLC (4%); Dynadot, Inc. (3.8%); GMO Internet Group, Inc. (3.8%); Tucows Domains, Inc. (3.2%); Hostinger Operations UAB (2.7%); PDR Ltd. (2.5%); Gname.com Pte. Ltd. (2.1%); and Key-Systems LLC (2.1%).



WHOIS Data Redaction

A majority of the NRDs continue to have redacted WHOIS records at 60.3%. The figure was roughly the same as in April, when 60.6% of the NRDs had privacy-redacted WHOIS details. On the other hand, 39.7% of the May NRDs had public WHOIS records.

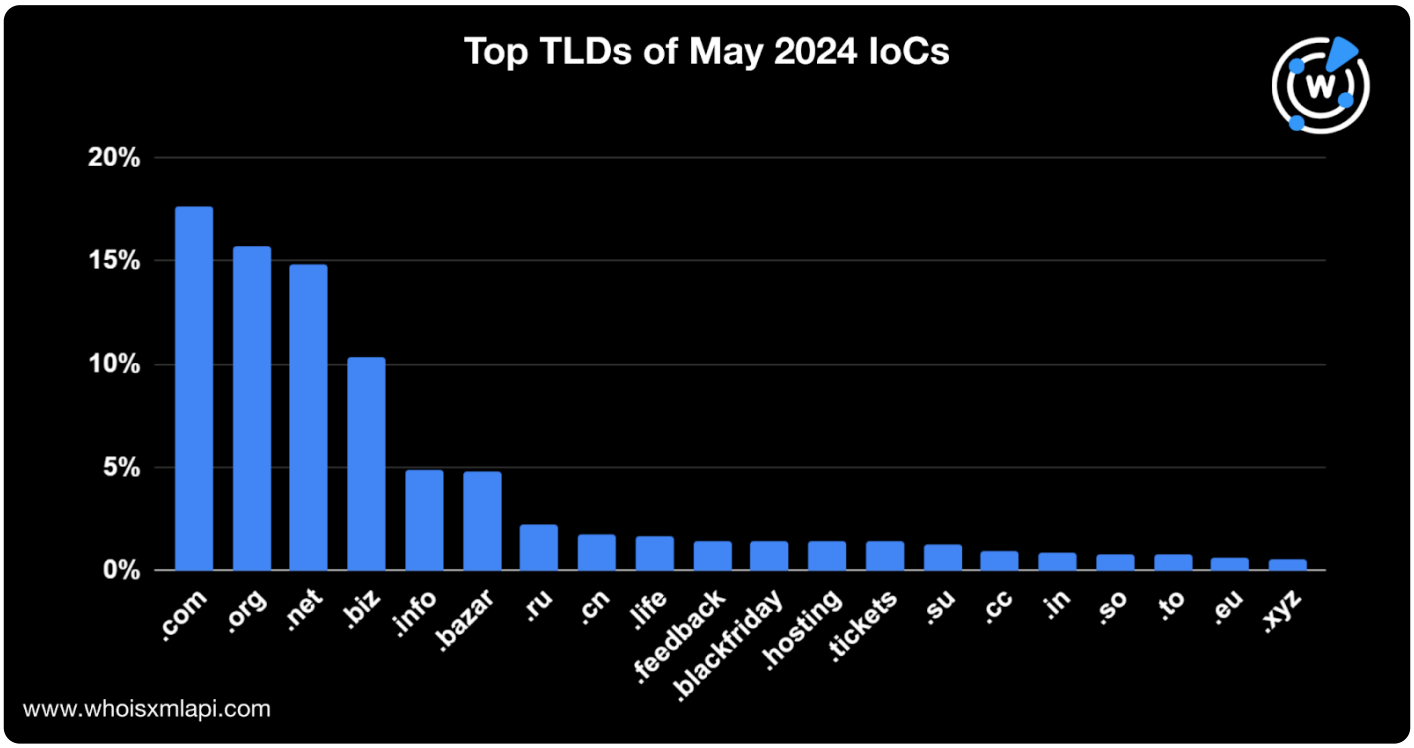


Cybersecurity through the DNS Lens

Top TLDs of the May IoCs

As is our usual next step, we analyzed more than 1 million domains tagged as IoCs for various threats in May. This analysis revealed that .com was the most popular gTLD used for malicious domains with a 17.6% share of the IoCs.

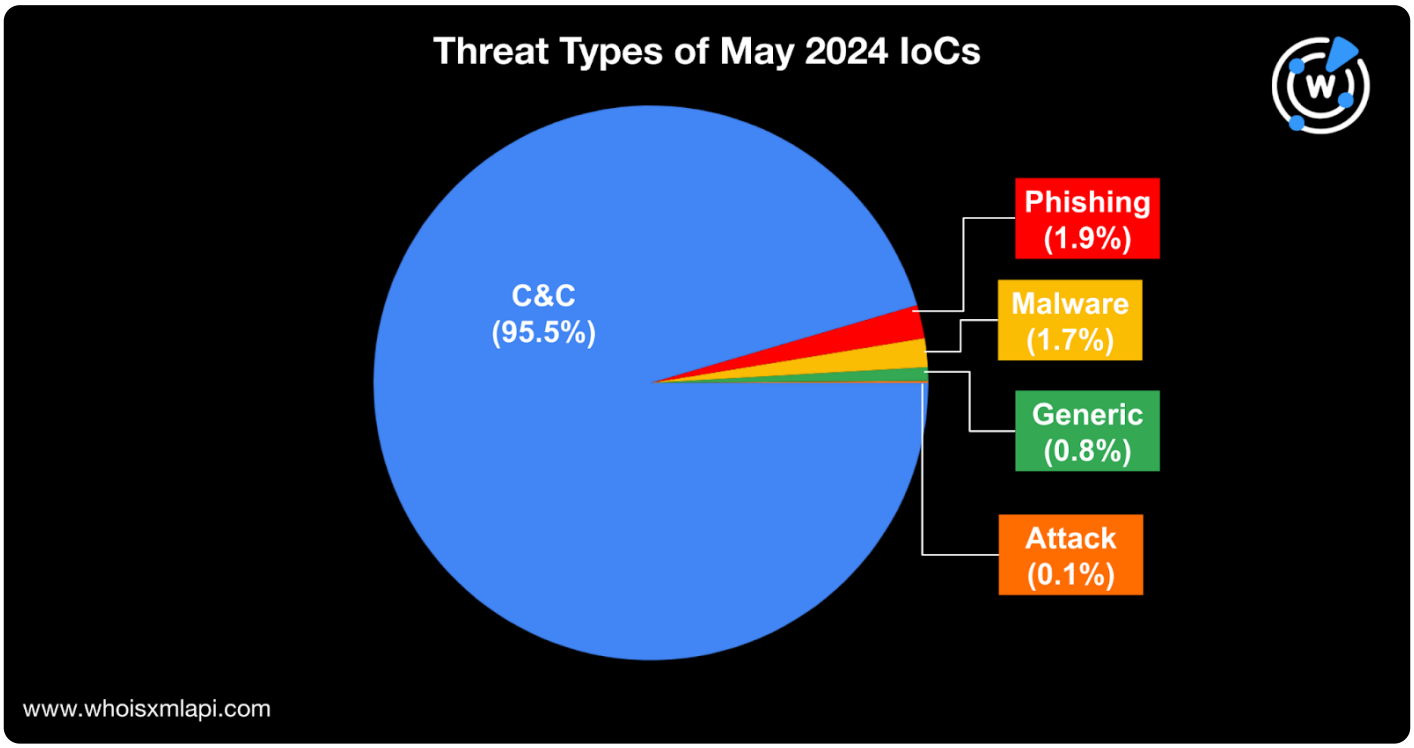
Other major gTLD extensions were also used, such as .org with a 15.7% share, .net with 14.8%, and .biz with 10.3%. Some malicious domains also sported ccTLD extensions, such as .ru with a 2.3% share, .cn with 1.8%, and .su with 1.2%, among others.



Threat Type Breakdown of the May IoCs

When we grouped the May IoCs based on associated threat type, we discovered that almost all, 95.5% to be exact, were associated with command and control (C&C). This number increased significantly from 86.6% in April.

The rest of the IoCs were related to phishing (1.9%), malware distribution (1.7%), and generic and other forms of cyber attacks (0.9%).



Threat Reports

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

- **Profiling a Popular DDoS Booter Service's Ecosystem:** Our research team built on 644 IoCs associated with a popular DDoS booter service, leading us to more than 2,000 additional threat artifacts.
- **A DNS Investigation of the Phobos Ransomware 8Base Attack:** We investigated 63 IoCs tagged in the Phobos Ransomware 8Base Attack, which enabled us to uncover hundreds of email-, IP-, and string-connected domains.
- **A DNS Investigation of the Typhoon 2FA Phishing Kit:** Our research team did an in-depth analysis of the IoCs related to Typhoon 2FA, a phishing-as-a-service (PhaaS) kit that can bypass two-factor authentication (2FA). We found more than 4,000 connected 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.