April 2024: Domain Activity Highlights

Posted on May 9, 2024

WhoisXML API researchers analyzed more than 6.6 million domains registered between 1 and 30 April 2024 to identify the most popular registrars, top-level domain (TLD) extensions, and other global domain registration trends.

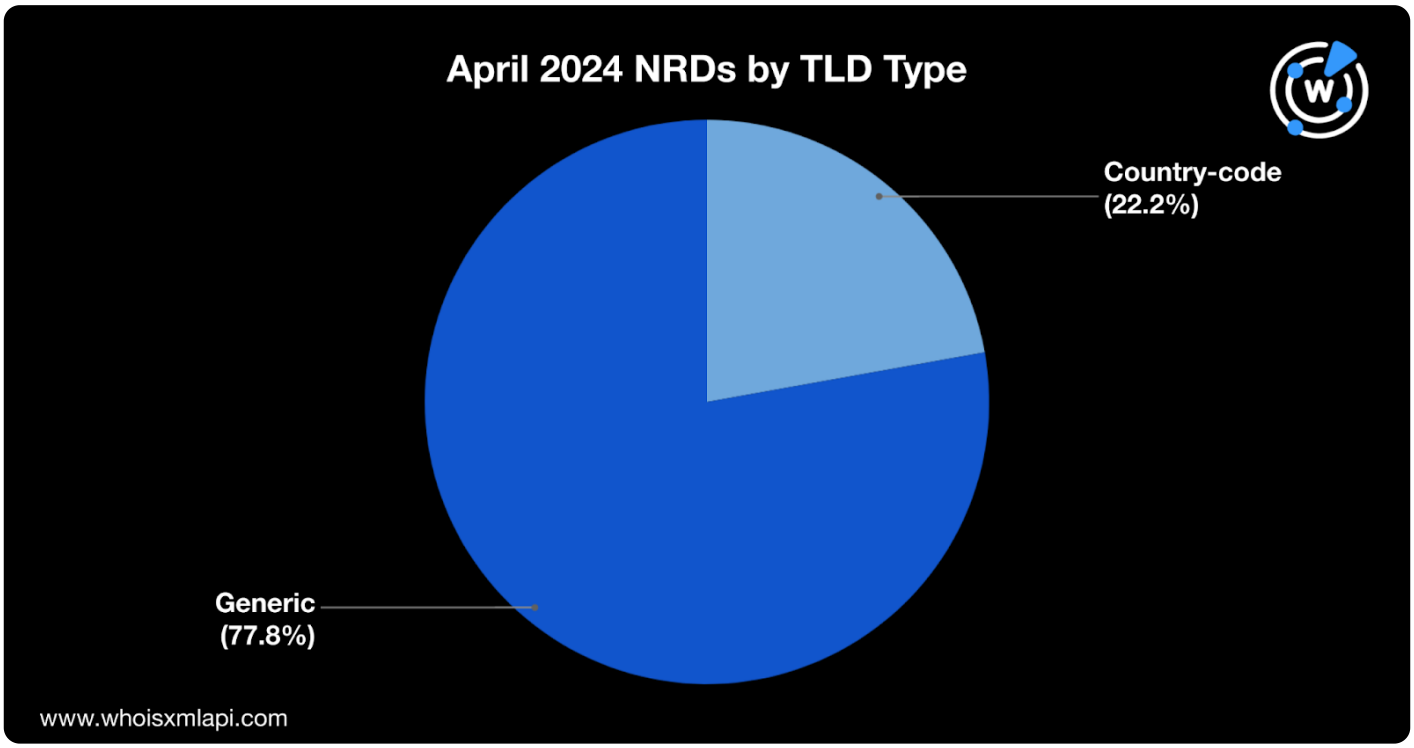
We also studied the top TLDs and associated threat type breakdown of more than 1.1 million domains detected as indicators of compromise (IoCs) in April.

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

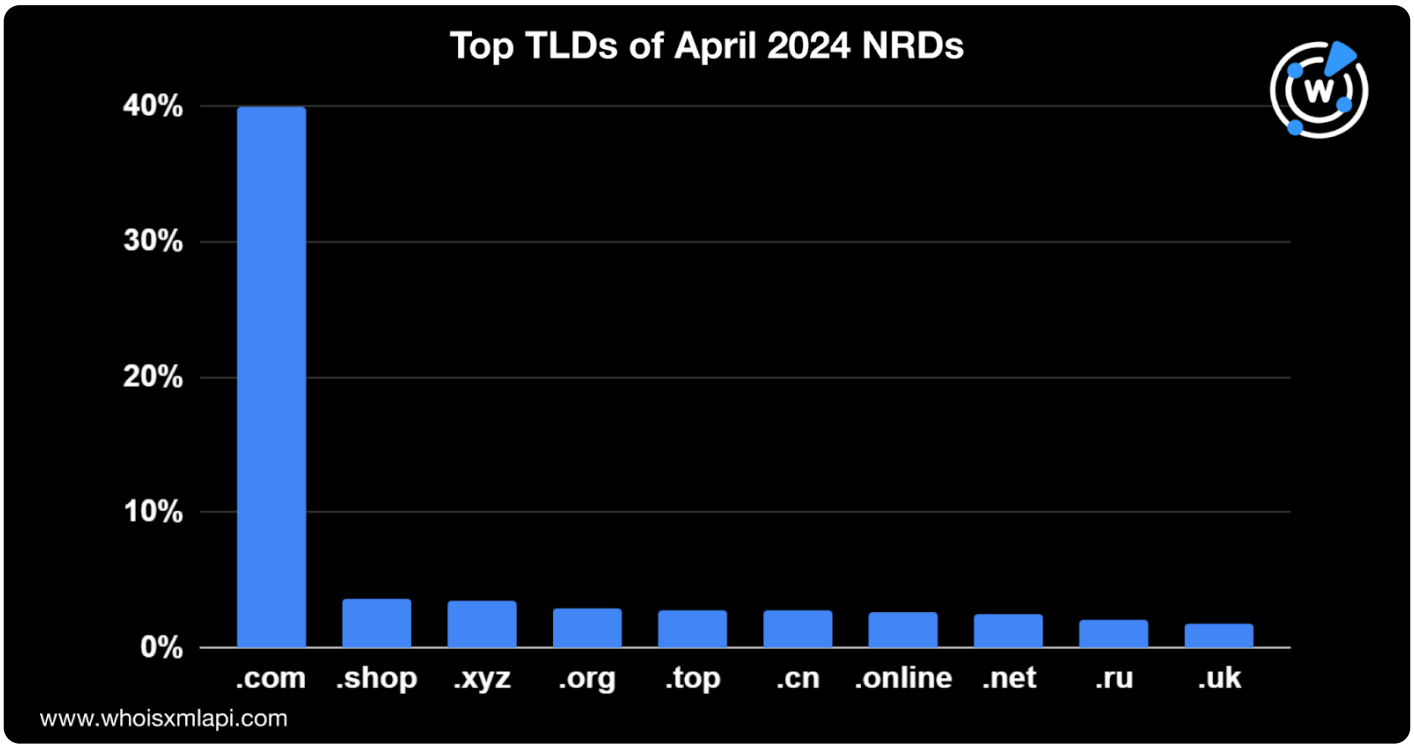
Zooming in on the April NRDs

TLD Distribution

About 77.8% of the 6.6 million domains registered in April used generic TLD (gTLD) extensions, while 22.2% used country-code TLD (ccTLD) extensions.

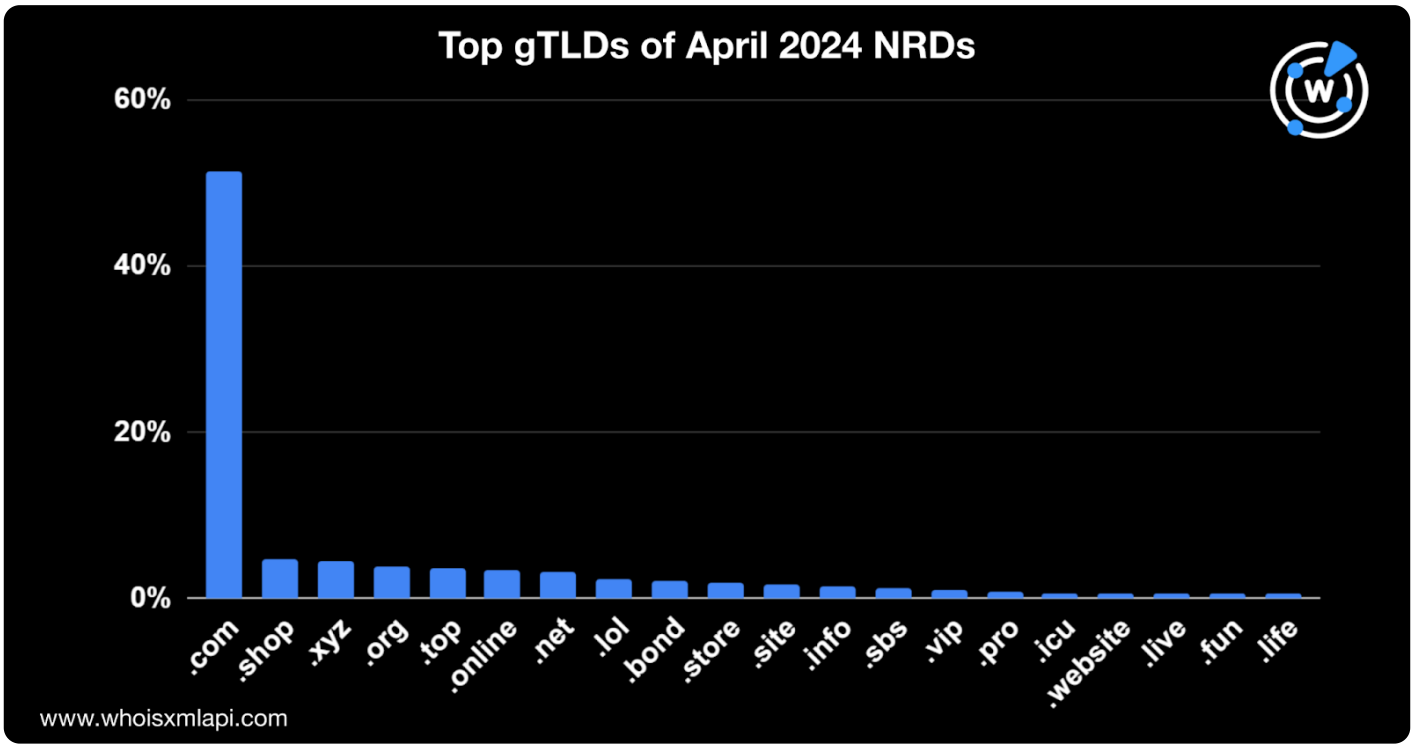


As in previous months, .com continued to be the most popular TLD extension with a 39.9% share of the NRDs. The other TLDs on the top 10 most used TLDs followed with a significant gap. They include .shop (3.6%), .xyz (3.5%), .org (3%), .top (2.8%), .cn (2.7%), .online (2.7%), .net (2.5%), .ru (2%), and .uk (1.8%).

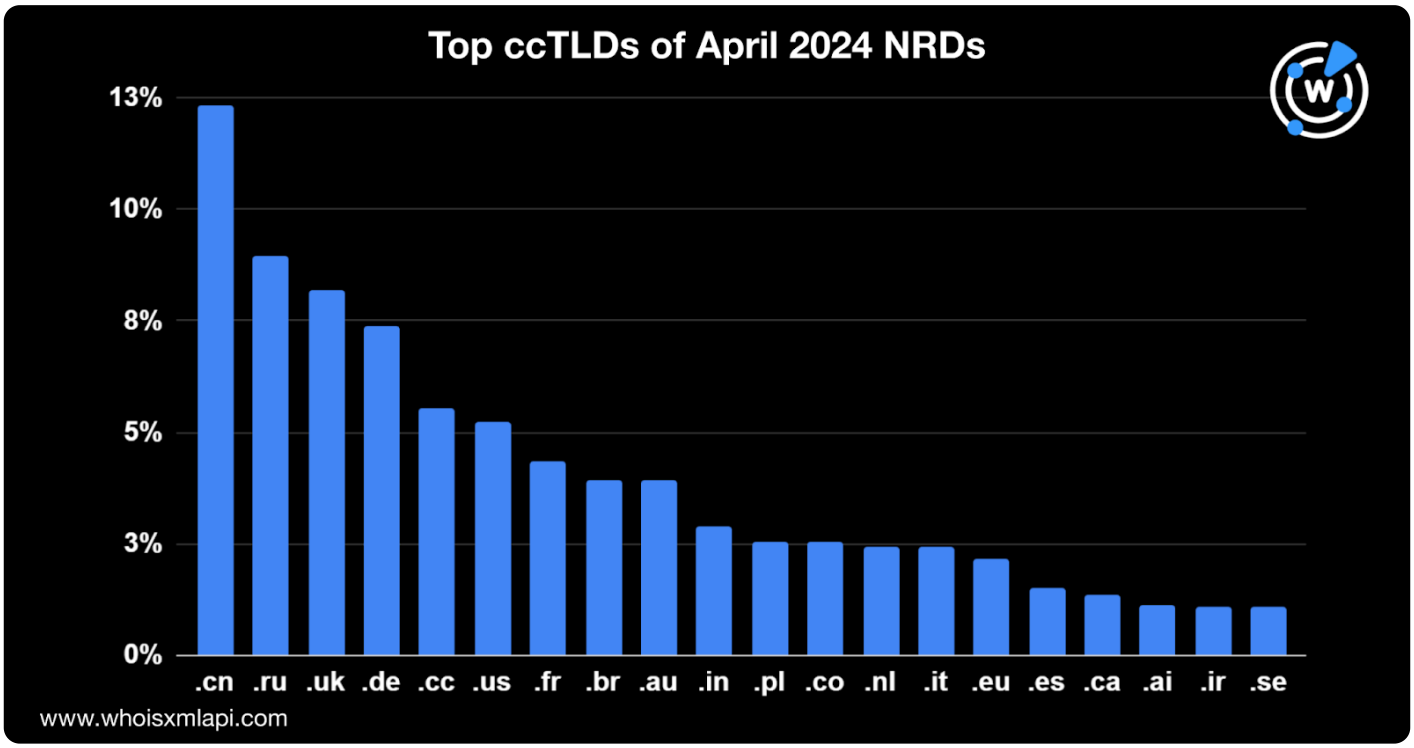


Digging deeper into our TLD analysis, we determined the most popular gTLDs and ccTLDs among the new domain registrations.

Out of more than 640 gTLDs, about 51.3% used .com. The rest of the top 20 lagged far behind. E-commerce-related gTLD .shop came in second place with a 4.6% share, closely followed by .xyz with a 4.4% share. The rest of the most used gTLDs included .org with a 3.8% share; .top with 3.6%; .online with 3.4%; .net with 3.2%; .lol with 2.3%; .bond with 2.2%; .store with 1.9%; .site with 1.8%; .info with 1.5%; .sbs with 1.3%; .vip with 1.1%; .pro with 0.7%; .icu and website with 0.6% each; and .live, .fun and .life with 0.5% each.

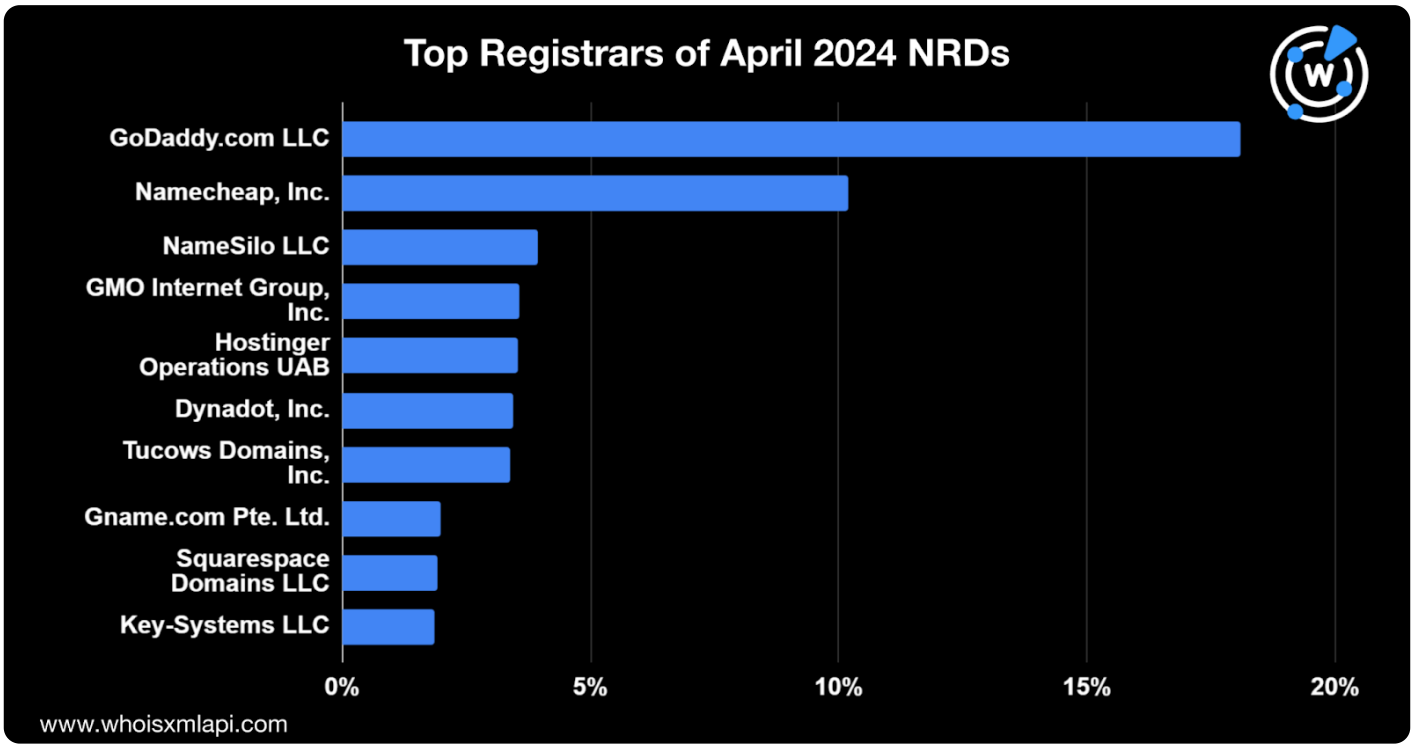


On the other hand, .cn remained the most used out of more than 230 ccTLDs, increasing from 10.3% new domains in March to 12.4% share in April. The other popular ccTLDs included .ru with a 9% share; .uk with 8.2%; .de with 7.4%; .cc with 5.6%; .us with 5.3%; .fr with 4.4%; .br and .au with 3.9% each; .in with 2.9%; .pl and .co with 2.6% each; .nl and .it with 2.4% each; .eu with 2.2%; .es with 1.5%; .ca with 1.4%; and .ai, .ir, and .se with 1.1% each. The top 20 extensions accounted for 81% of the April NRDs with ccTLD extensions.



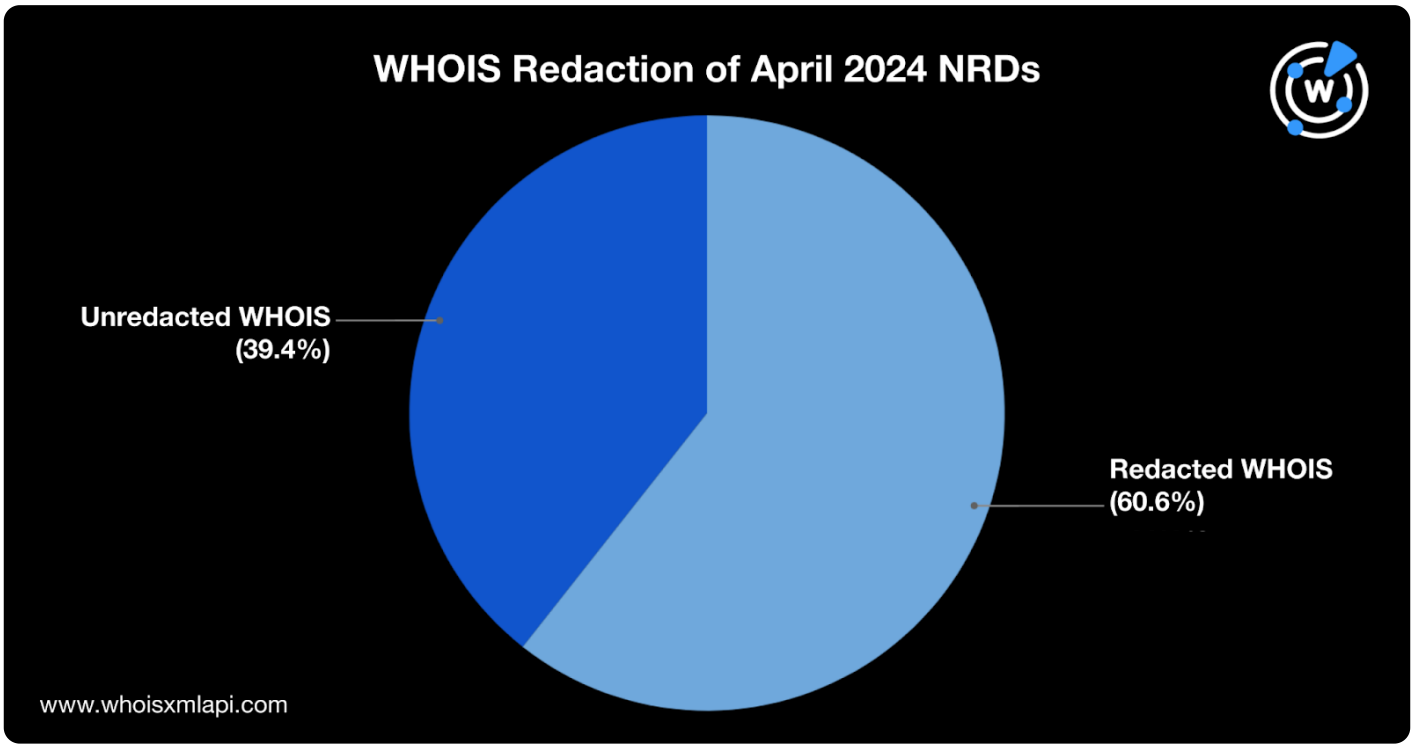
Registrar Distribution

As in previous months, GoDaddy.com LLC was still the most popular registrar with an 18.1% share of the April domain registrations. It was followed by Namecheap, Inc. (10.2%); NameSilo LLC (3.9%); GMO Internet Group, Inc. (3.6%); Hostinger Operations UAB (3.5%); Dynadot, Inc. (3.4%); Tucows Domains, Inc. (3.4%); Gname.com Pte. Ltd. (2%); Squarespace Domains LLC (1.9%); and Key-Systems LLC (1.8%).



WHOIS Data Redaction

WHOIS record redaction continued to increase. From 58.6% in February and 59.2% in March, the NRDs with privacy-redacted WHOIS details rose to 60.6% in April, while 39.4% had public WHOIS records.

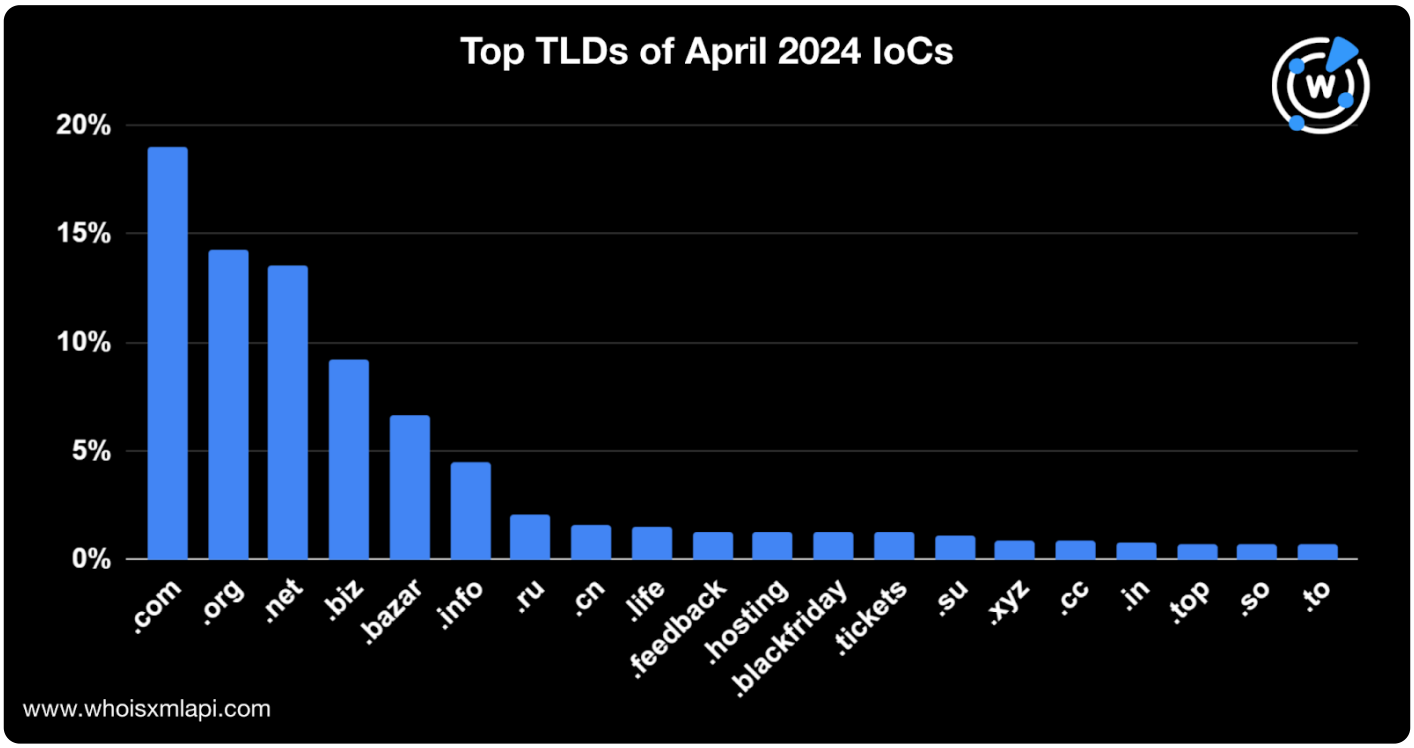


Cybersecurity through the DNS Lens

Top TLDs of the April IoCs

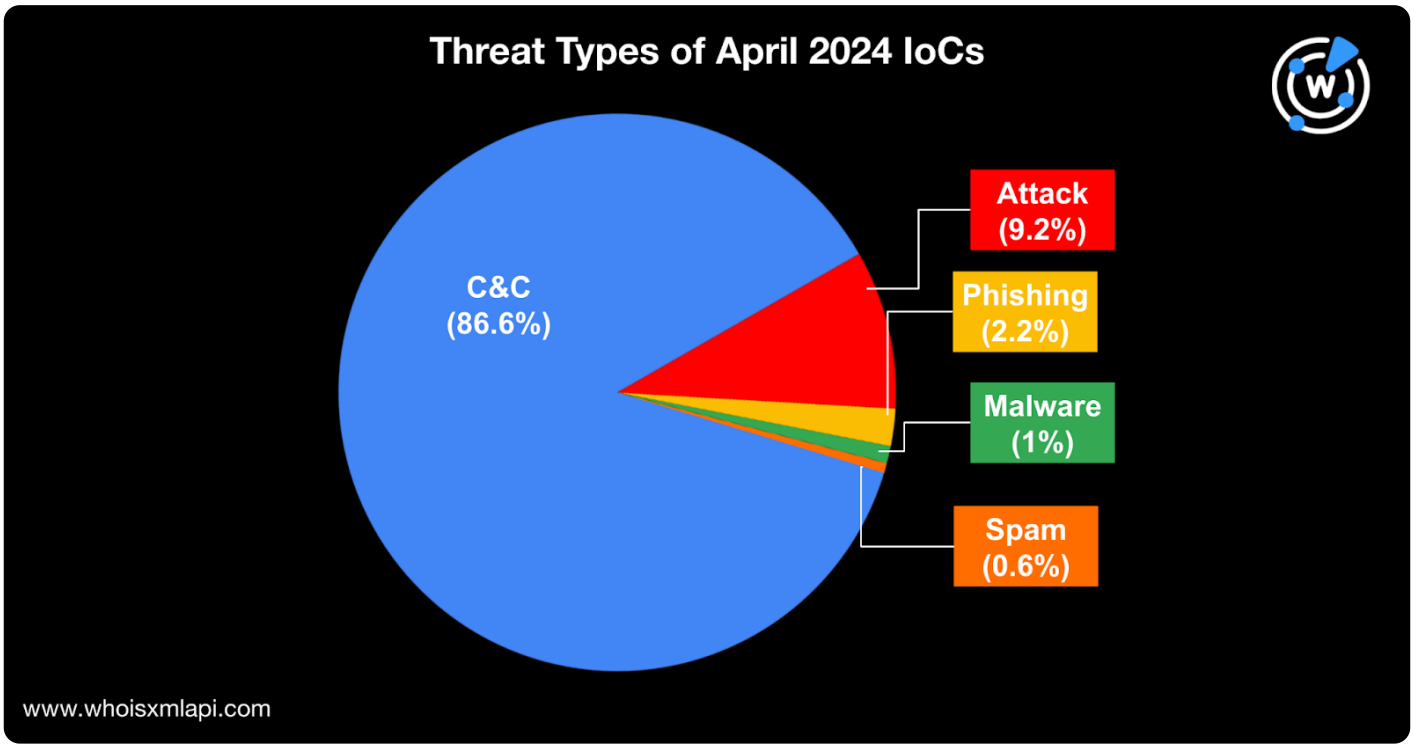
We then analyzed more than 1.1 million domains tagged as IoCs for various threats in April, leading us to discover that .com was also the most popular gTLD used for malicious domains in our dataset with a 19% share of the IoCs.

Other major gTLD extensions were also used, such as .org with a 14.3% share, .net with 13.5%, and .biz with 9.2%. Some malicious domains also sported ccTLD extensions, such as .ru with a 2.1% share, .cn with 1.6%, and .su with 1.1%, among others.



Threat Type Breakdown of the April IoCs

We then grouped the April IoCs based on the threat types they were associated with. A massive 86.6% of the IoCs were associated with command and control (C&C). This number went down from 95% in March. The rest were related to other forms of cyber attacks (9.2%), phishing (2.2%), malware distribution (1%), and spamming (0.6%).



Threat Reports

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

- **Stately Taurus APT Group Targets Asian Countries: What Do the Campaign IoCs Reveal?:** Building on two lists comprising 30 IoCs, WhoisXML API researchers found more than 130 artifacts connected to the decade-old APT group recently observed targeting ASEAN countries, particularly Japan, Myanmar, the Philippines, and Singapore.

- **Examining a U.S. Tax Scammer's Web Infrastructure through the DNS Lens:** We investigated a U.S. tax scammer reportedly victimizing small businesses and self-employed individuals, leading us to other web properties that could be part of the threat actor's attack infrastructure.

- **Hunting for TimbreStealer Malware Artifacts in the DNS:** WhoisXML API researchers investigated 152 IoCs tagged in a campaign distributing TimbreStealer, an information stealer, through finance-themed lures. The analysis found 19,000+ potential artifacts.

- **Uncovering Suspicious Download Pages Linked to App Installer Abuse:**We performed an IoC expansion analysis on IoCs related to Microsoft App Installer abuse, leading us to uncover 1,100 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.