March 2024: Domain Activity Highlights

Posted on April 10, 2024

WhoisXML API researchers analyzed more than 7.3 million domains registered between 1 and 31 March 2024 to identify global domain registration trends, including the most popular registrars, registrant countries, and top-level domain (TLD) extensions.

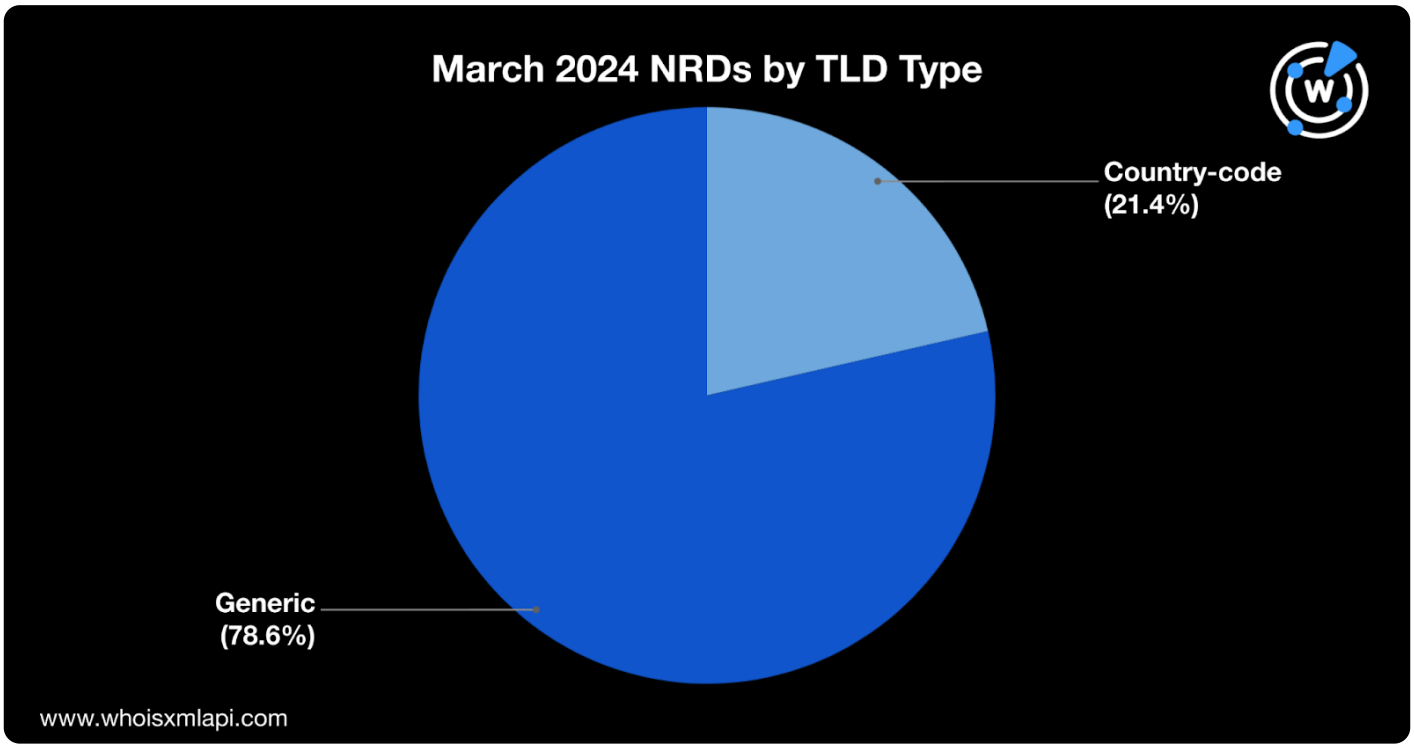
We also studied the TLD usage and associated threat type breakdown of more than 1.1 million domains detected as indicators of compromise (IoCs) in March.

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.

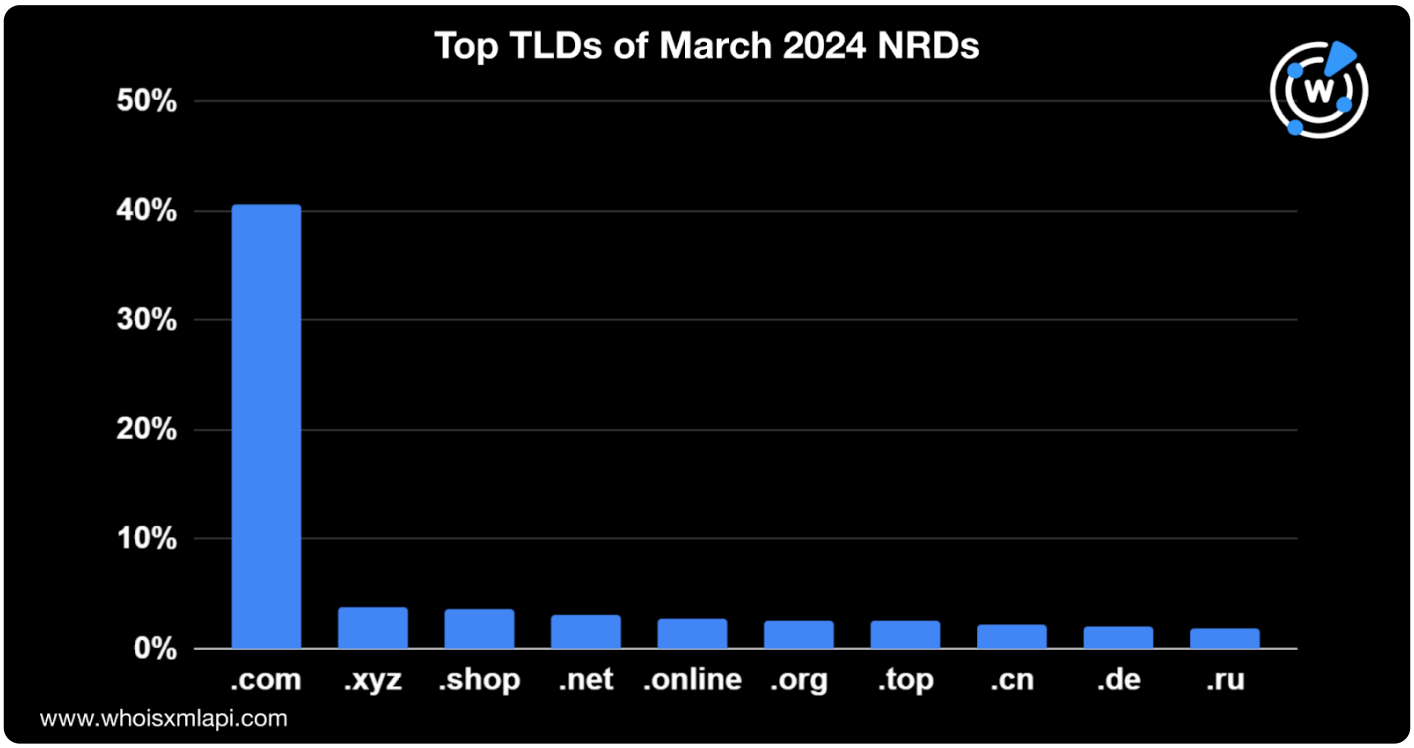
Zooming in on the March NRDs

TLD Distribution

About 78.6% of the 7.3 million domains registered in March used generic TLD (gTLD) extensions, while 21.4% used country-code TLDs (ccTLDs).



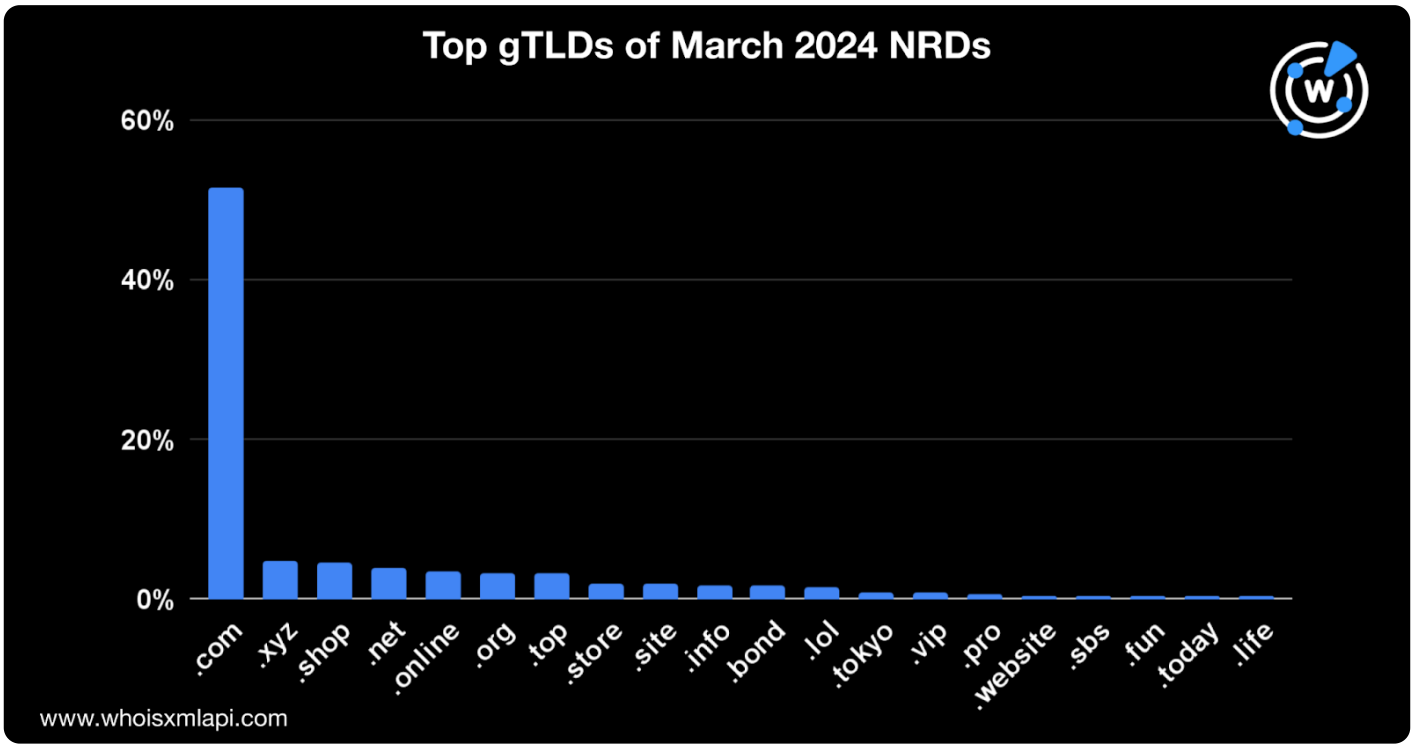
As in the previous months, .com continued to be the most popular, with a 40.5% share of the NRDs. The other TLDs on the top 10 most used TLDs lagged behind with a significant gap. They include .xyz (3.8%), .shop (3.7%), .net (3%), .online (2.7%), .org (2.6%), .top (2.5%), .cn (2.2%), .de (2.1%), and .ru (1.9%).



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

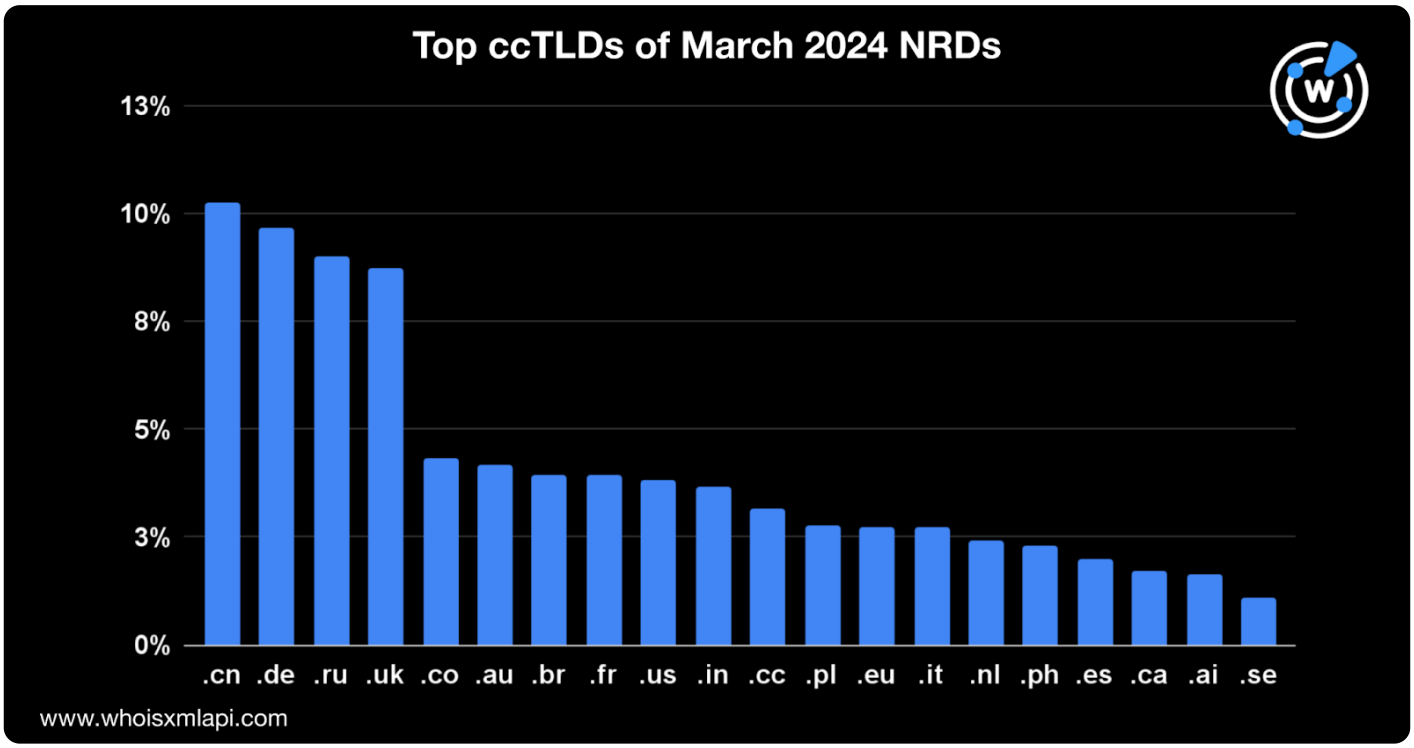
More than half of the NRDs sporting gTLDs, 51.6% to be exact, used .com out of more than 650 gTLDs. The rest of the top 20 followed far behind.

For instance, .xyz came in second place with a 4.9% share, while e-commerce-related gTLD .shop had a 4.7% share. They were followed by .net with 3.9%; .online and .org with 3.4% each; .top with 3.2%; .store and .site with 1.9% each; .info with 1.8%; .bond with 1.7%; .lol with 1.5%; .tokyo with 0.9%; .vip with 0.8%; .pro with 0.6%; and .website, .sbs, .fun, .today, and .life with 0.5% each.



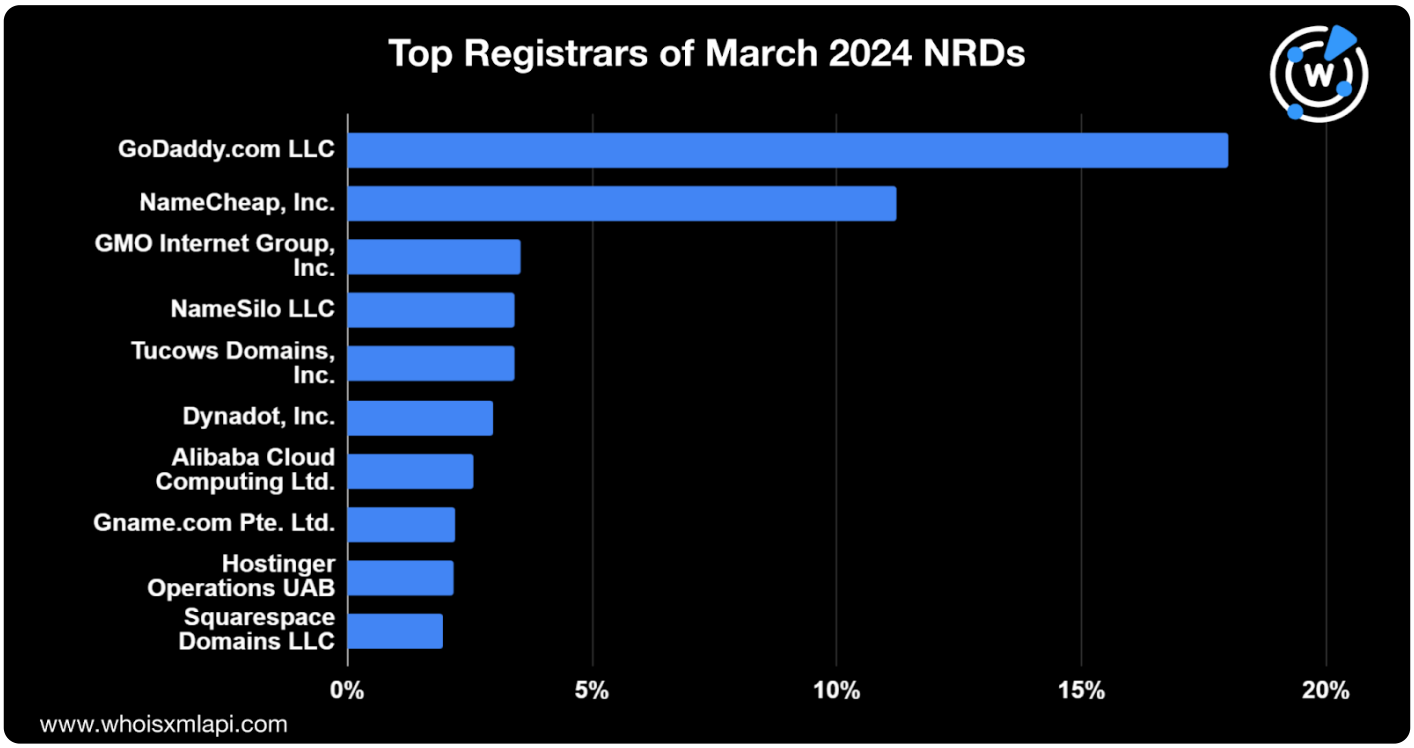
On the other hand, .cn was the most used out of more than 230 ccTLDs, with a 10.3% share of the new domains.

It was followed by .de with a 9.7% share, .ru with 9%, .uk with 8.7%, .co with 4.3%, .au with 4.2%, .br with 4%, .fr with 3.9%, .us with 3.8%, .in with 3.7%, .cc with 3.2%, .pl and .eu with 2.8% each, .it with 2.7%, .nl with 2.4%, .ph with 2.3%, .es with 2%, .ca and .ai with 1.7%, and .se with 1.1%. These extensions accounted for 84.2% of the March NRDs sporting ccTLDs.



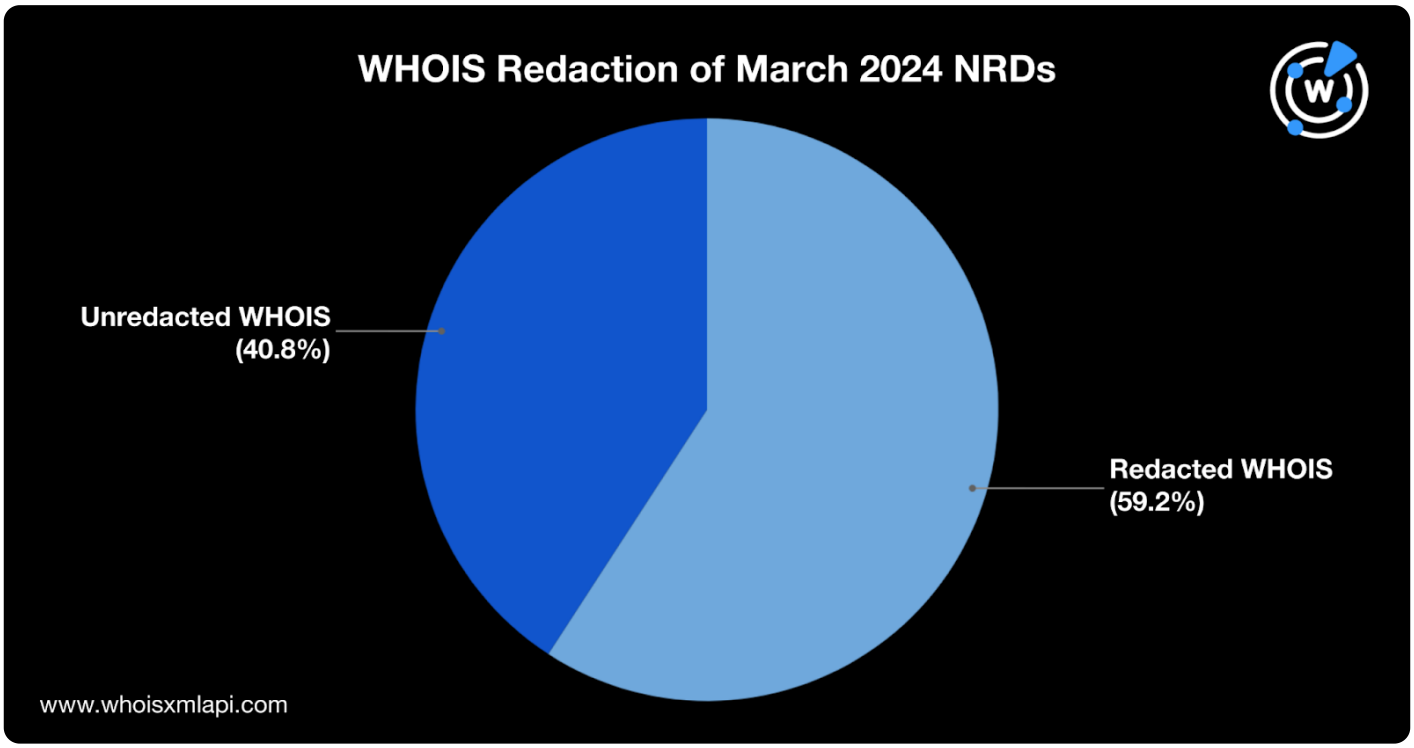
Registrar Distribution

GoDaddy.com LLC remained the most popular registrar with an 18% share, followed by Namecheap, Inc. with 11.2%; GMO Internet Group, Inc. with 3.6%; and NameSilo LLC and Tucows Domains, Inc. with 3.4% each. Completing the top 10 registrars for March were Dynadot, Inc. (3%), Alibaba Cloud Computing Ltd. (2.6%), Gname.com Pte. Ltd. and Hostinger Operations UAB (2.2% each), and Squarespace Domains LLC (1.9%).



WHOIS Data Redaction

WHOIS record redaction increased. From 58.6% in February, the NRDs with privacy-redacted WHOIS details rose to 59.2% in March, while 40.8% had public WHOIS records.

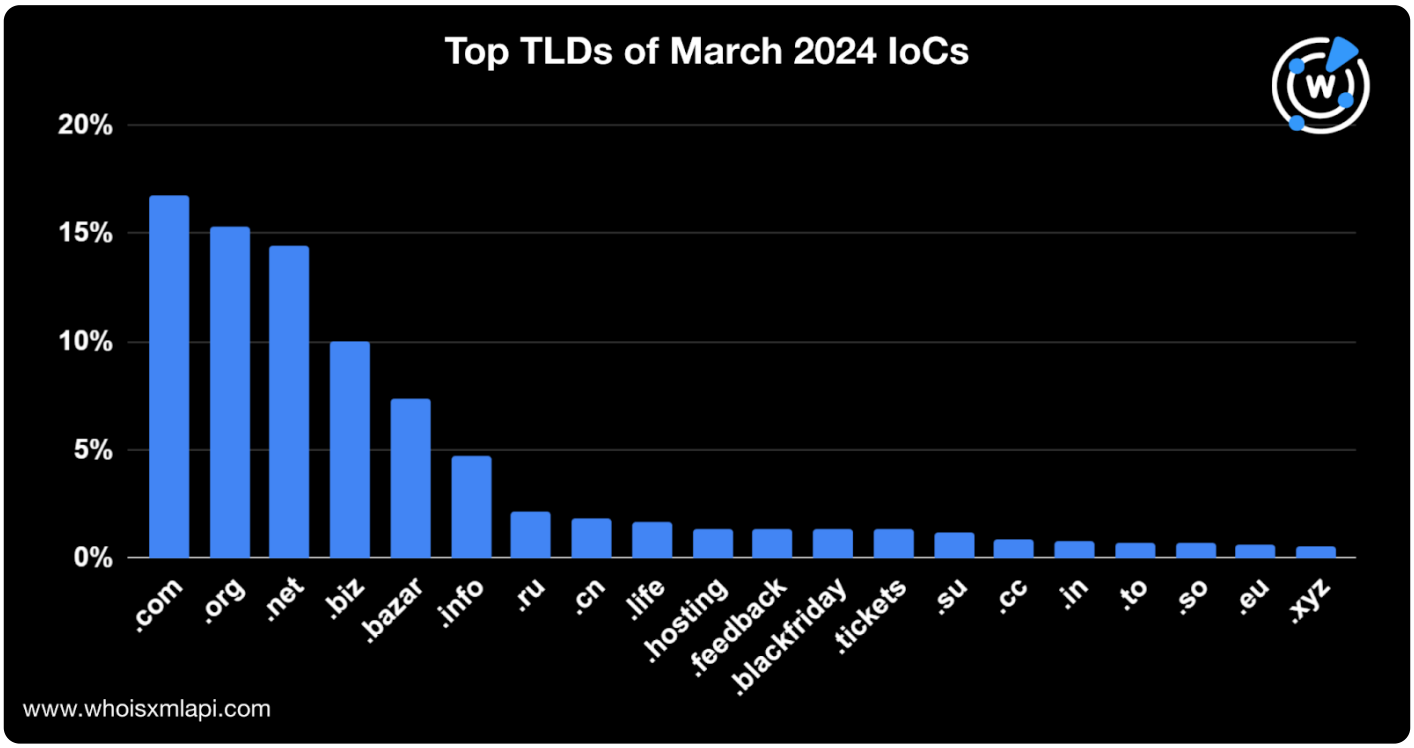


Cybersecurity through the DNS Lens

Top TLDs of the March IoCs

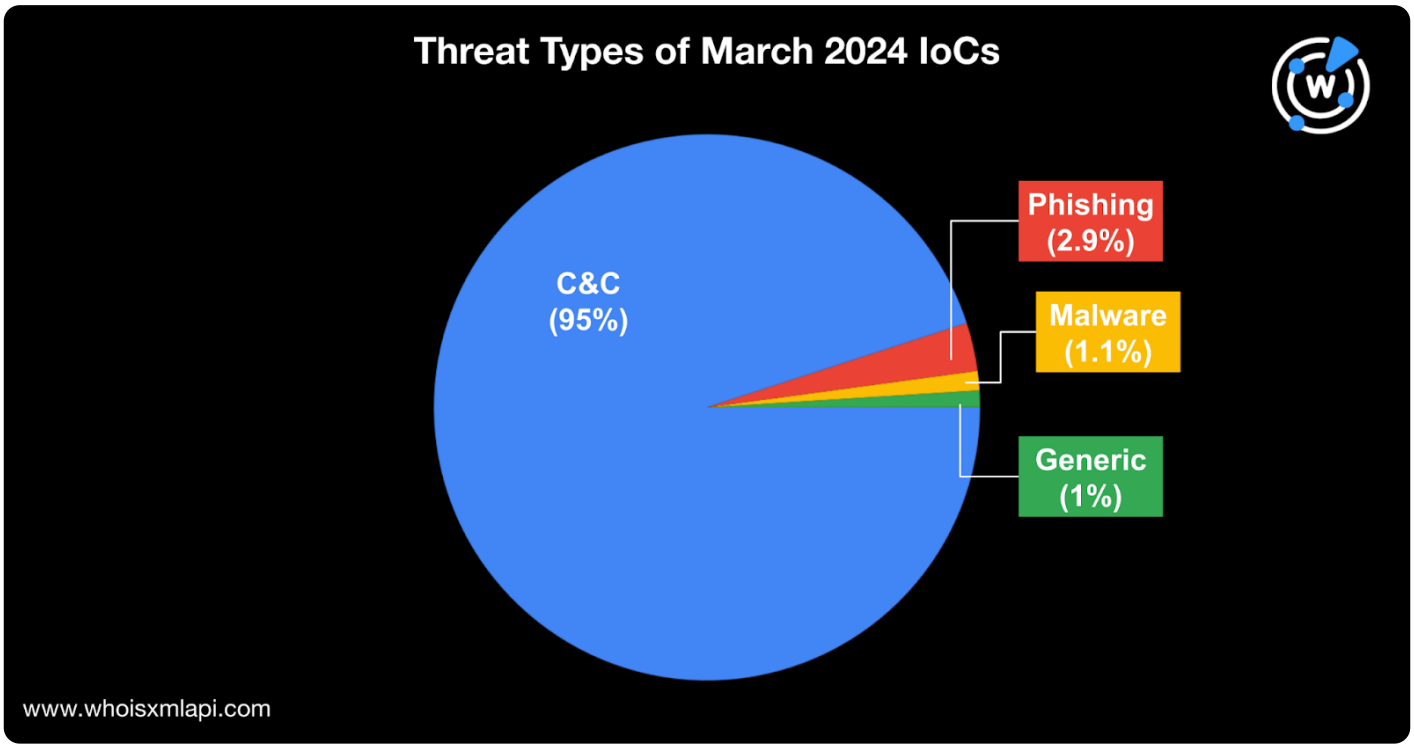
Our researchers then analyzed more than 1.1 million domains tagged as IoCs for various threats in March.

We discovered that 16.8% of the IoCs sported .com, making it the most used gTLD. Other major gTLD extensions followed, including .org with a 15.3% share, .net with 14.4%, and .biz with 10%. Some malicious domains also used ccTLDs, such as .ru with a 2.2% share, .cn with 1.8%, .su with 1.2%, and .in with 0.8%, among others.



Threat Type Breakdown of the March IoCs

We then grouped the March IoCs based on the threat types they were associated with. A massive 95% of the IoCs were associated with command and control (C&C). The rest were related to phishing campaigns (2.9%), malware distribution (1.1%), and other forms of cyber attacks (1%).



Threat Reports

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

- **Uncovering Suspicious Download Pages Linked to App Installer Abuse:** From a list of domains and subdomains tagged as IoCs in a campaign abusing Microsoft's App Installer, WhoisXML API researchers found more than 1,100 potentially connected artifacts.

- **Checking Out the DNS for More Signs of ResumeLooters:** We investigated the ResumeLooters campaign by analyzing 15 IoCs, which led us to hundreds of connected artifacts.

- **On the DNS Trail of the Rise of macOS Backdoors:** Our research team analyzed IoCs related to two macOS backdoors, RustDoor and KandyKorn, and found five email addresses

and 32 IP-connected domains.

- **Searching for Potential Propaganda Vehicle Presence in the DNS:** We performed an IoC expansion on 132 PAPERWALL IoCs that allowed us to uncover 681 email-connected domains and other 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.