January 2024: Domain Activity Highlights

Posted on February 12, 2024

WhoisXML API researchers analyzed more than 7 million domains registered between 1 and 31 January 2024 to identify global domain registration trends, including the most popular registrars, registrant countries, and top-level domain (TLD) extensions.

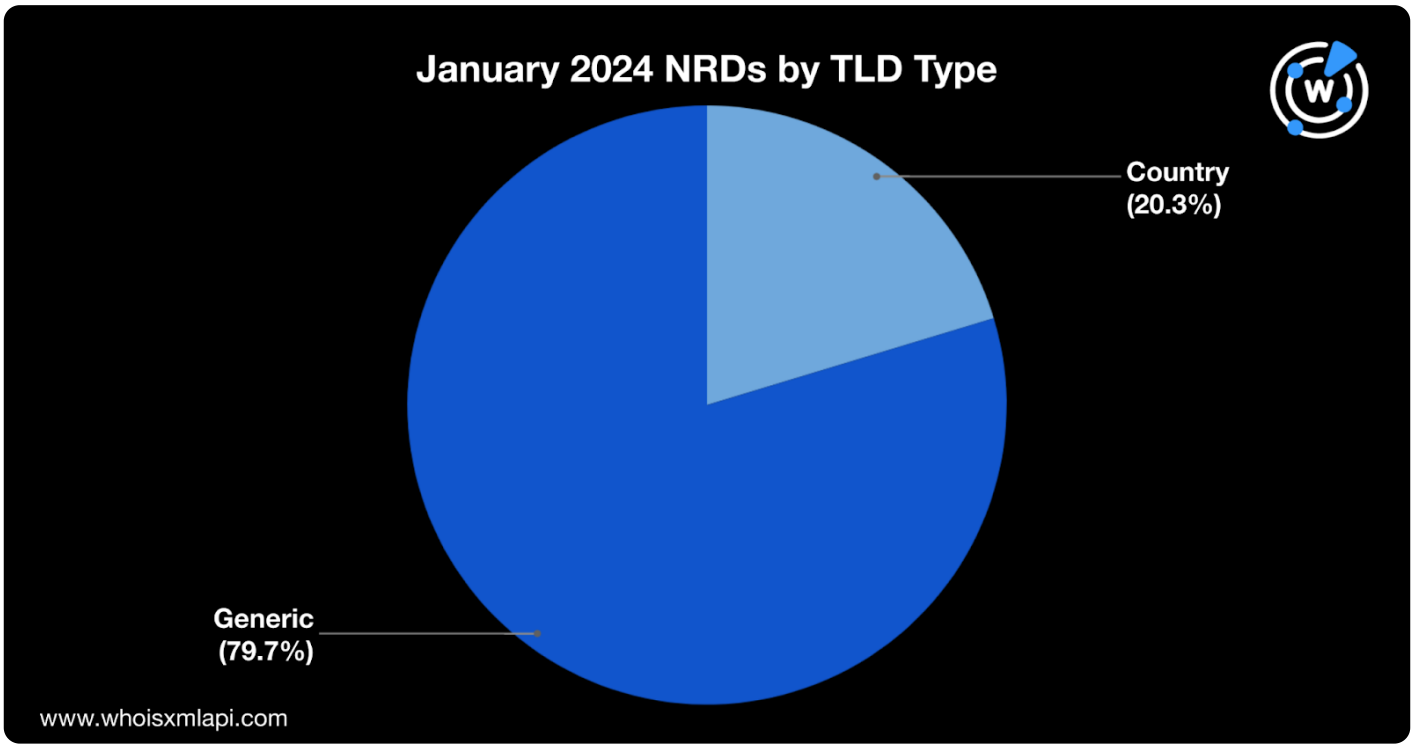
We also studied the TLD usage and threat type breakdown of more than 1.1 million domains detected as indicators of compromise (IoCs) in January.

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

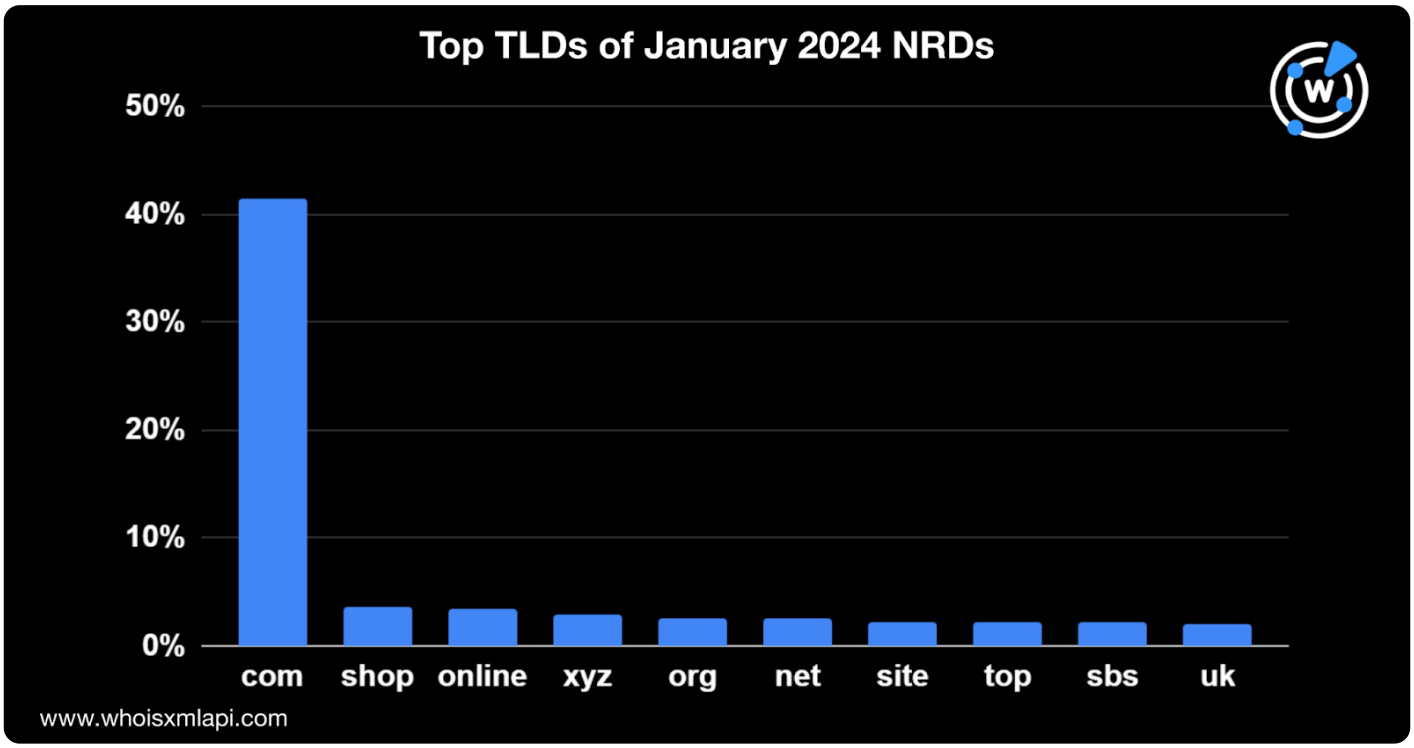
Zooming in on the January NRDs

TLD Distribution

Of the 7 million domains registered in January 2024, 79.7% used generic TLD (gTLD) extensions, while 20.3% used country-code TLDs (ccTLDs).



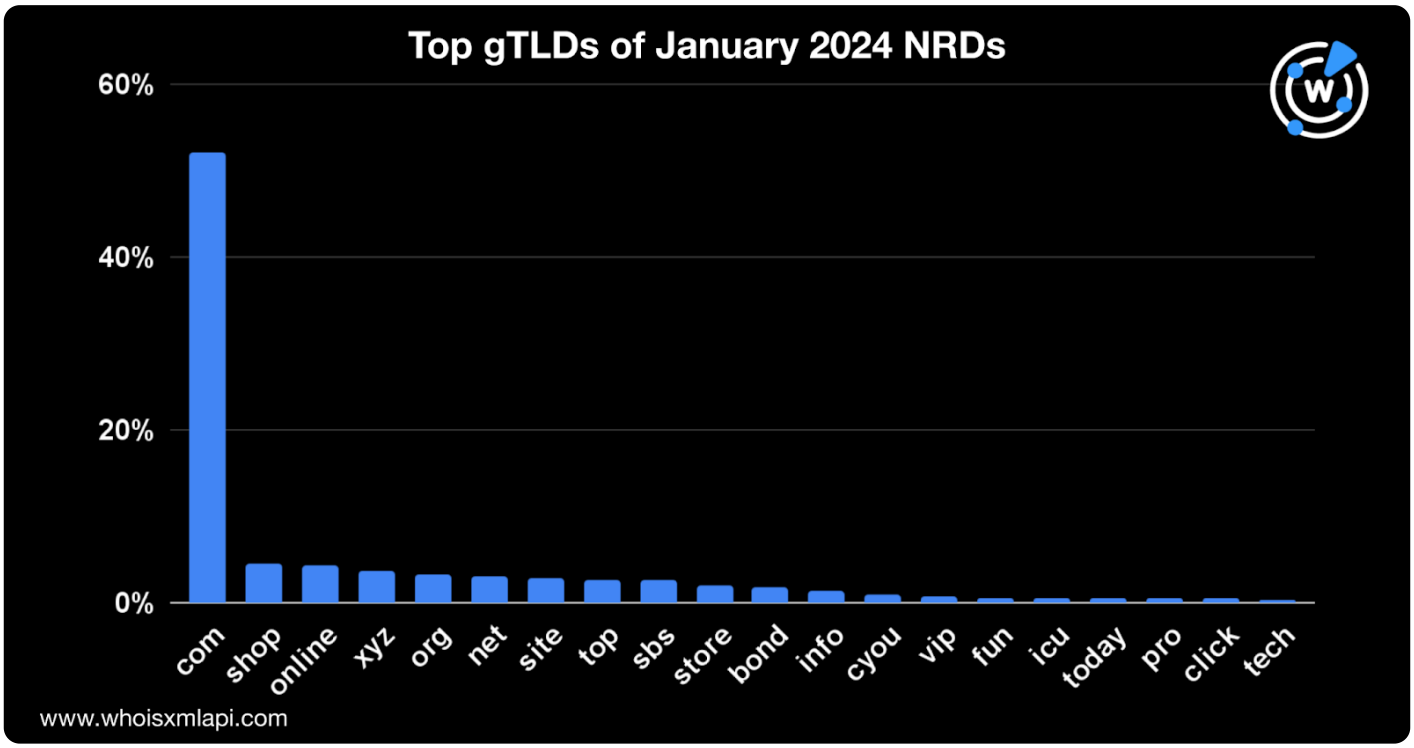
About 41.5% of the newly registered domains (NRDs) under gTLDs sported .com, making it the most used. It was followed by .shop with a 3.6% share; .online with 3.5%; .xyz with 3%; .org and .net with 2.5% each; .site and .top with 2.2% each; .sbs with 2.1%; and .uk with 2%.



We then deepened our TLD analysis to determine the most popular gTLDs and ccTLDs among the NRDs.

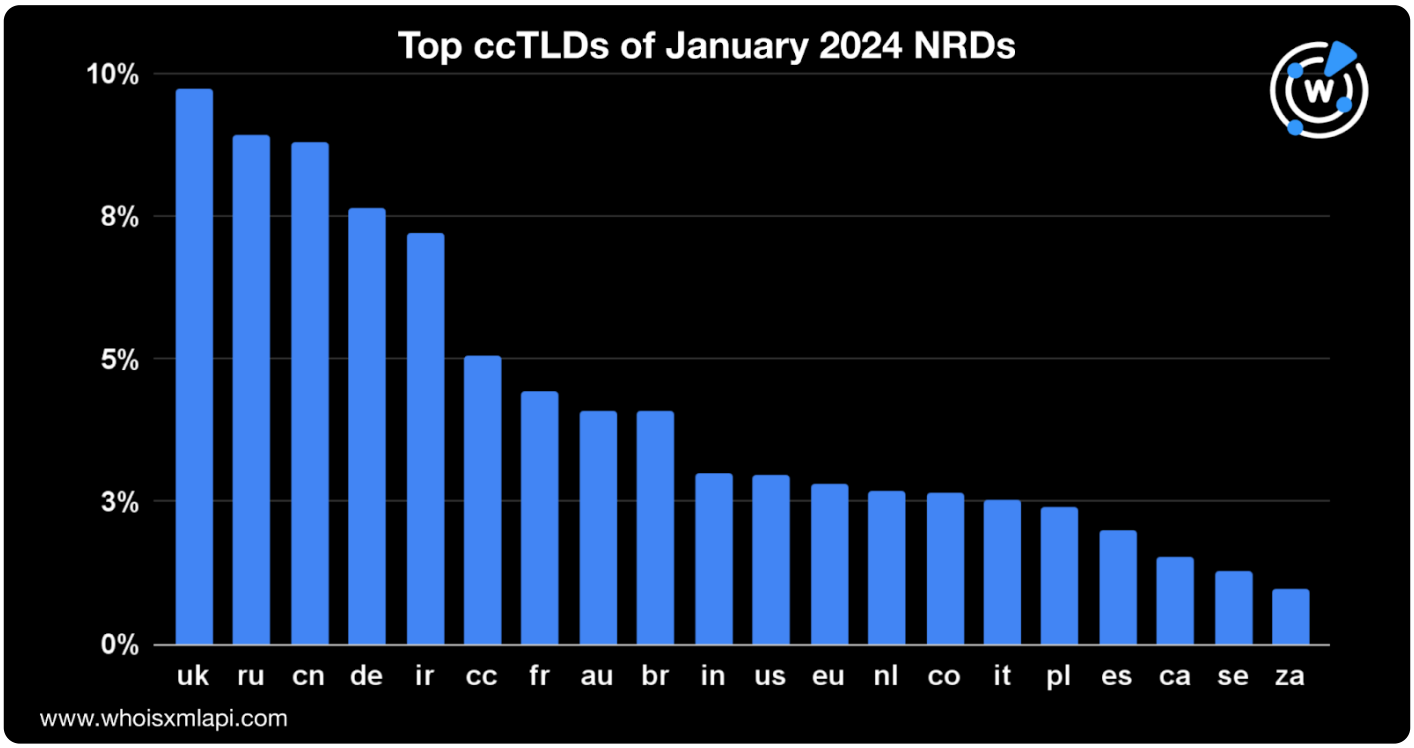
Out of more than 625 gTLDs, .com accounted for 52.1% of the new domain registrations sporting gTLDs and the rest of the top 20 TLDs followed with a significant gap.

In fact, e-commerce-related gTLD .shop came in second place with a 4.5% share; .online with 4.4%; .xyz with 3.8%; .org with 3.2%; .net with 3.1%; .site with 2.8%; .top and .sbs with 2.7% each; .store with 2%; .bond with 1.8%; .info with 1.4%; .cyou with 1%; .vip with 0.8%; .fun and .icu with 0.6% each; .today, .pro, and .click with 0.5% each; and .tech with 0.4%.



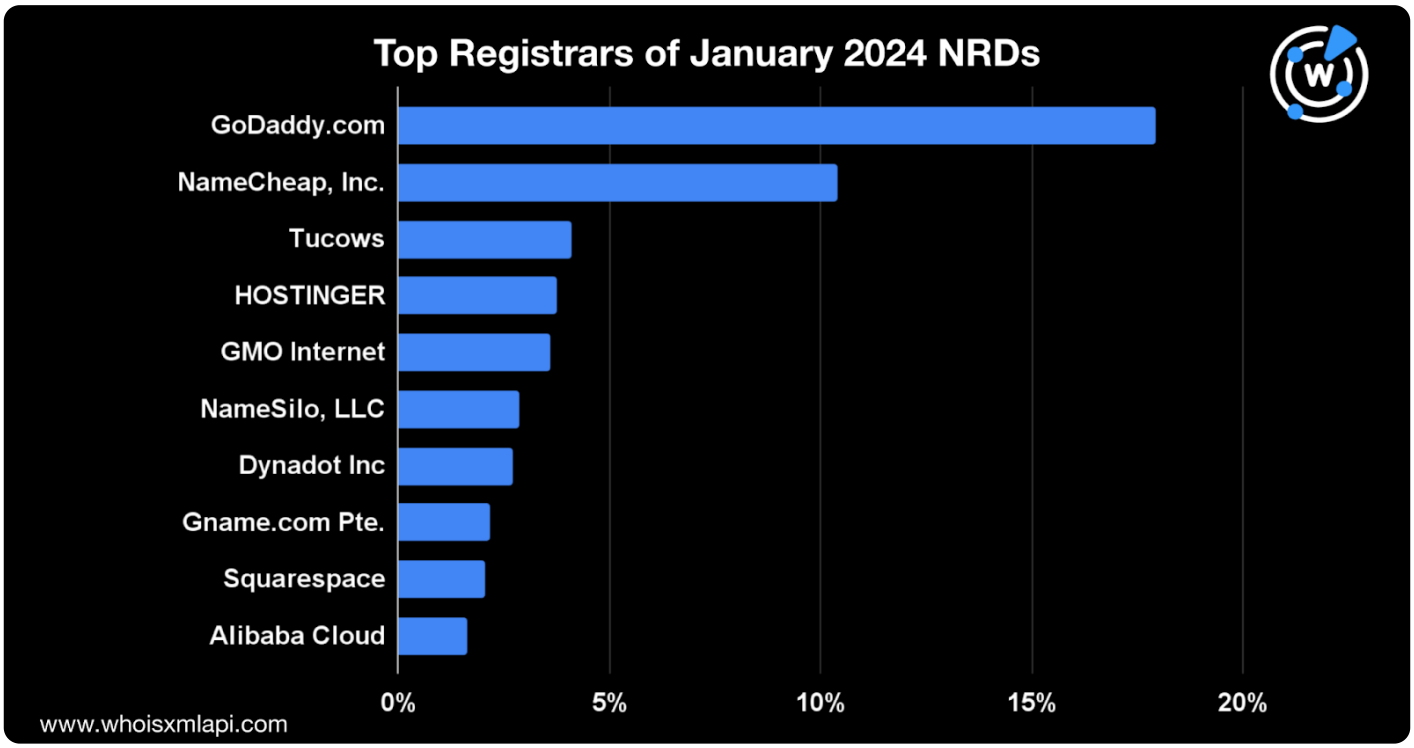
On the other hand, .uk was the most used ccTLD out of more than 230 ccTLDs, with a 9.7% share of the new domains sporting ccTLDs.

It was followed by .ru with an 8.9% share; .cn with 8.8%; .de with 7.7%; .ir with 7.2%; .cc with 5%; .fr with 4.4%; .au and .br with 4.1% each; .in and .us with 3% each; .eu with 2.8%; .nl and .co with 2.7% each; .it with 2.5%; .pl with 2.4%; .and .es with 2%. The rest of the top 20 were .ca (1.5%), .se (1.3%), .za (1%). Together, these ccTLDs accounted for 84.8% of the January NRDs under ccTLDs.



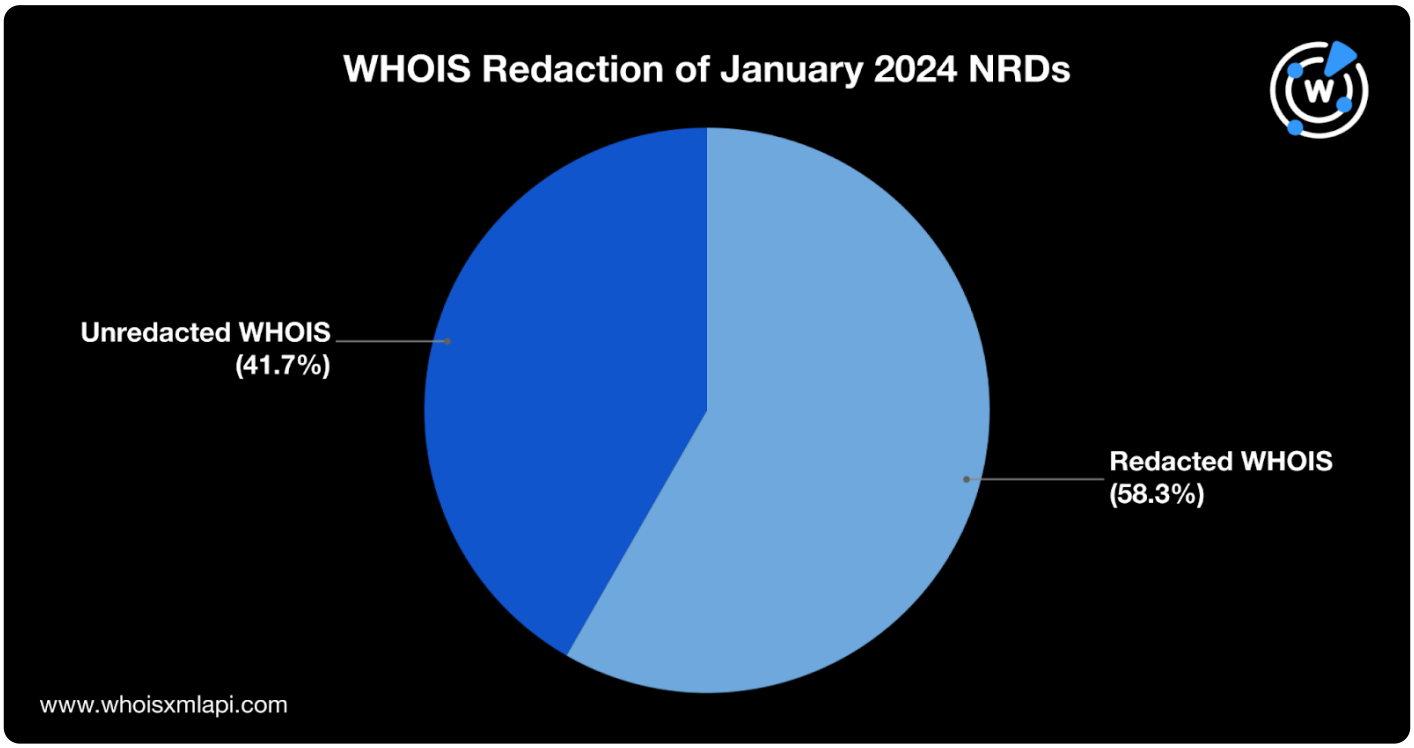
Registrar Distribution

Like in December, the most popular registrars were still GoDaddy and Namecheap, Inc., which accounted for 18% and 10.4% of the total domain registration volume, respectively. The rest of the top 10 registrars were Tucows (4.1%); HOSTINGER (3.8%); GMO Internet Group, Inc. (3.6%); NameSilo LLC (2.9%); Dynadot, Inc. (2.7%); Gname.com Pte. Ltd. (2.2%); Squarespace Domains LLC (2.1%); and Alibaba Cloud Computing Ltd. (1.6%).



WHOIS Data Redaction

A majority of the January NRDs, 58.3% to be exact, had redacted WHOIS records, while 41.7% had public WHOIS records.

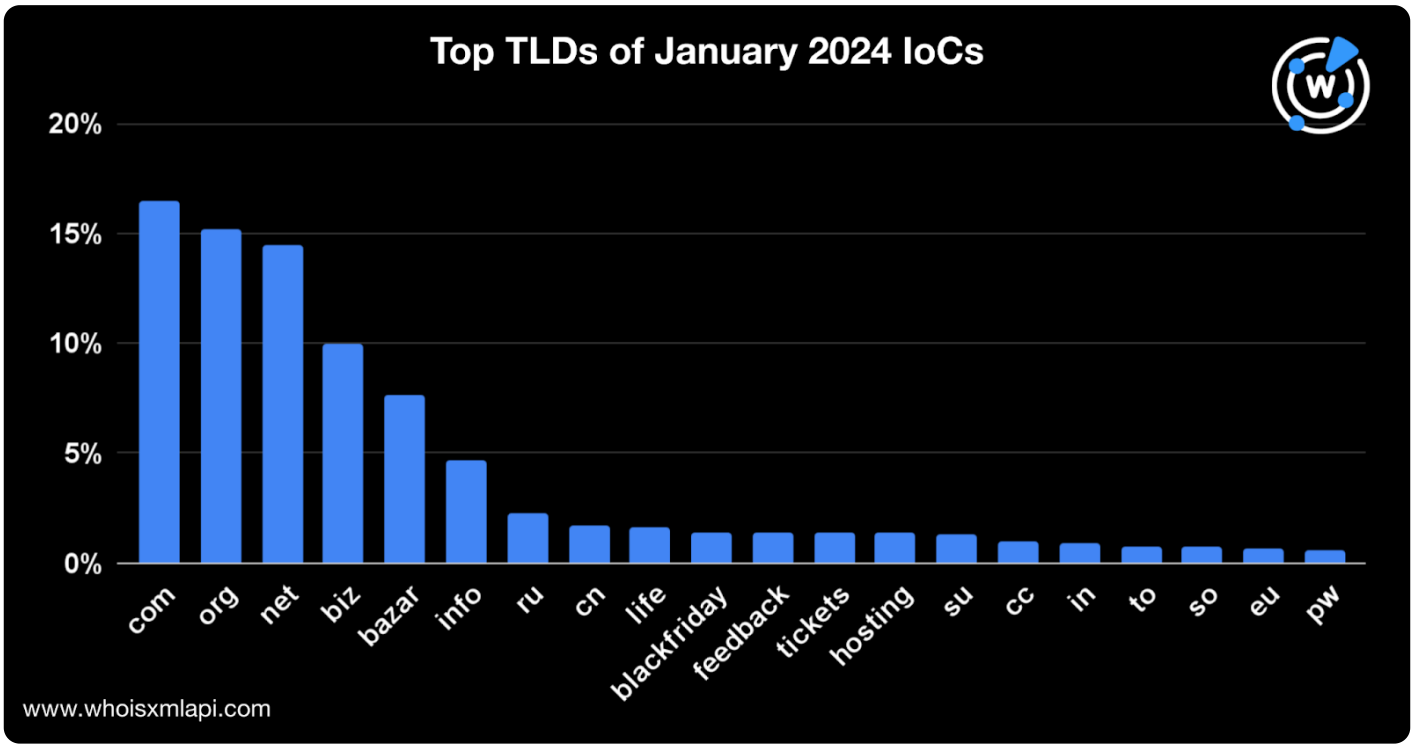


Cybersecurity through the DNS Lens

Top TLDs of the January IoCs

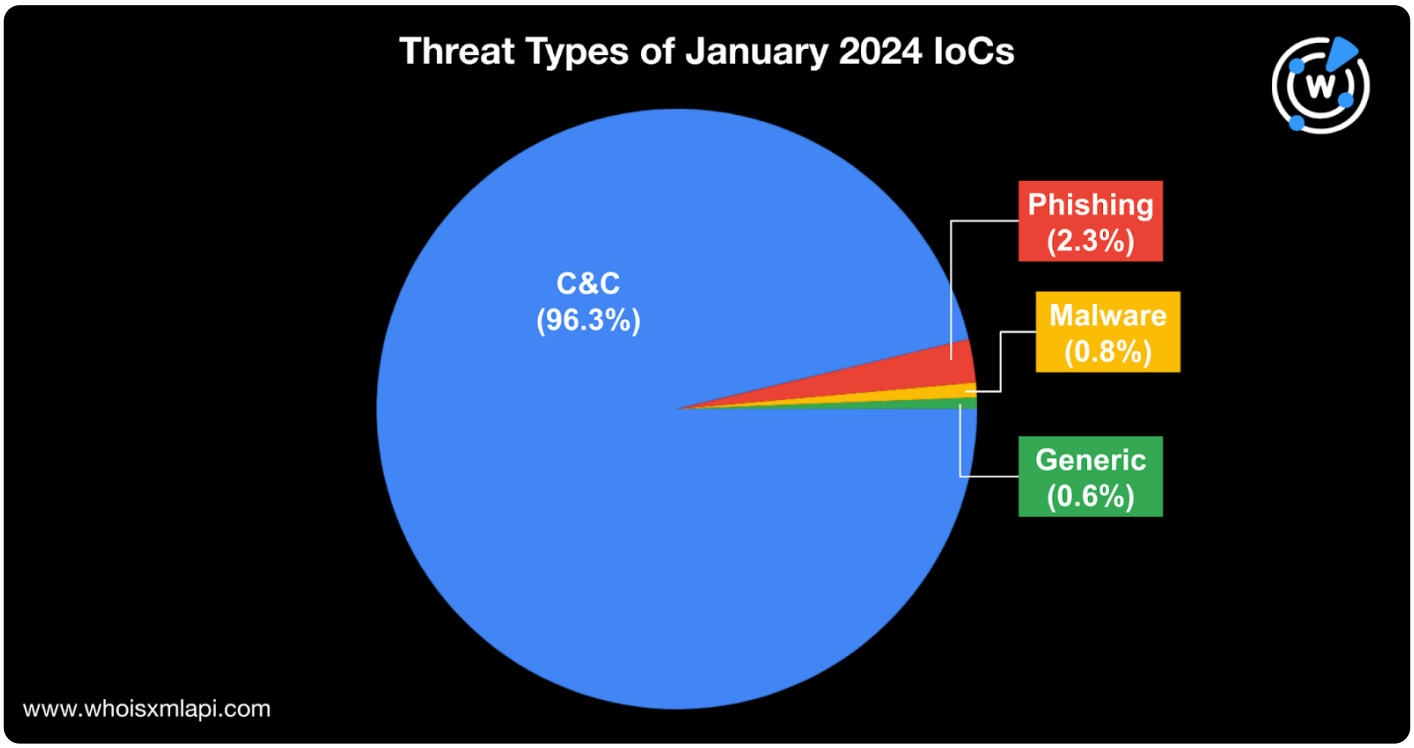
Our researchers then analyzed more than 1.1 million domains tagged as IoCs for various threats in January.

We found that .com was the most popular gTLD extension among the IoCs, accounting for 16.5% of the malicious domains. It was closely followed by other major gTLDs, namely, .org with a 15.2% share, .net with 14.4%, and .biz with 10%.Other IoCs used ccTLDs, including .ru (2.3%), .cn (1.7%), and .su (1.3%).



Threat Type Breakdown of the January IoCs

We also categorized the January IoCs based on the types of threats they were associated with. Most of them—a massive 96.3%—were tagged as command-and-control (C&C) servers. The rest figured in phishing campaigns (2.3%), malware distribution (0.8%), and other forms of cyber attacks (0.6%).



Threat Reports

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

- **Exploring Epsilon Stealer Traces Aided by DNS Intel:** The WhoisXML API research team extracted a list of 76 domains from the 133 indicators of compromise (IoCs) related to the Epsilon Stealer, uncovering 1,700+ potentially connected artifacts.
- **A Peek at the PikaBot Infrastructure:** From a list of 11 IoCs involved in the distribution of PikaBot through malvertising, our researchers discovered hundreds of email- and IP-connected artifacts.
- **Investigating the UNC2975 Malvertising Campaign Infrastructure:** We analyzed 28 IoCs associated with the UNC2975 malvertising campaign, which led to the discovery of 3,000+ potentially 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.