February 2024: Domain Activity Highlights

Posted on March 11, 2024

WhoisXML API researchers analyzed more than 6.6 million domains registered between 1 and 29 February 2024 to identify global domain registration trends, including the most popular registrars, registrant countries, and top-level domain (TLD) extensions.

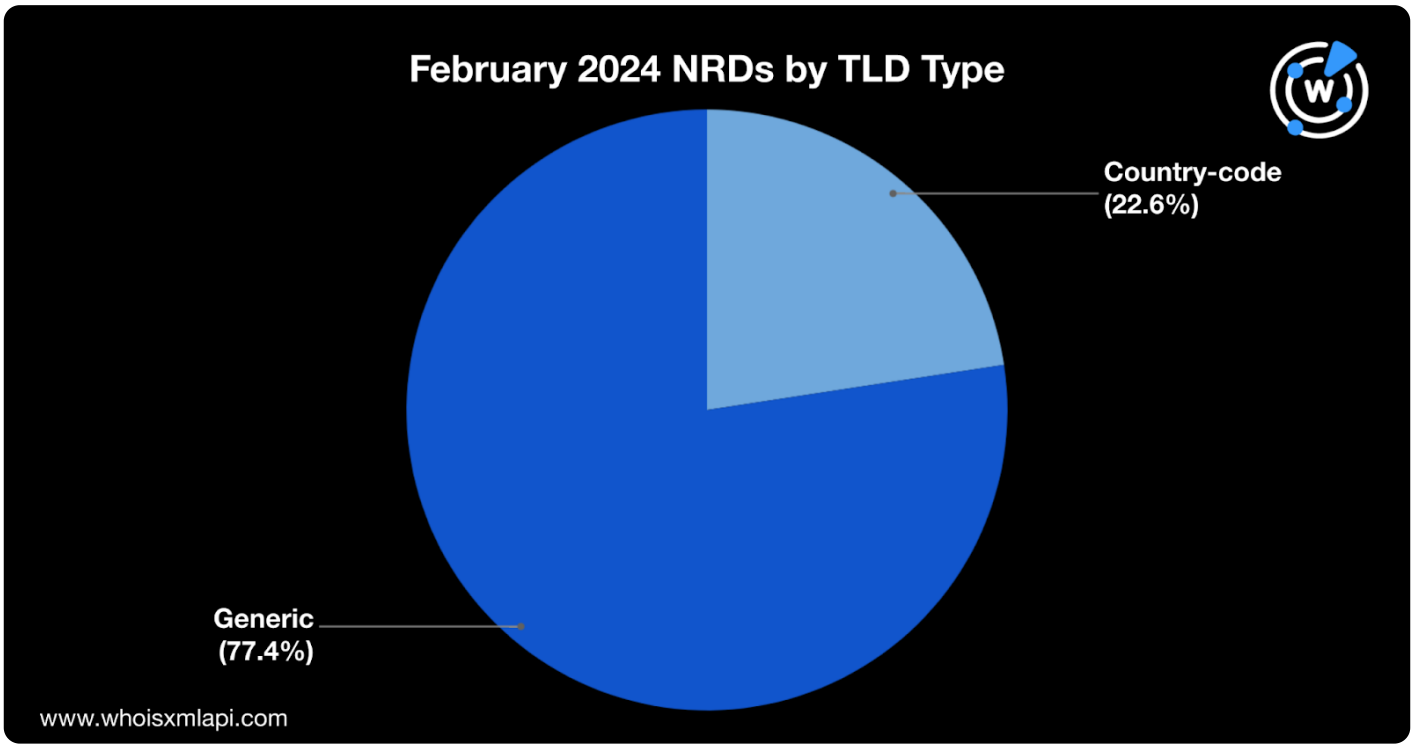
We also studied the TLD usage and associated threat type breakdown of more than 1 million domains detected as indicators of compromise (IoCs) in February.

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

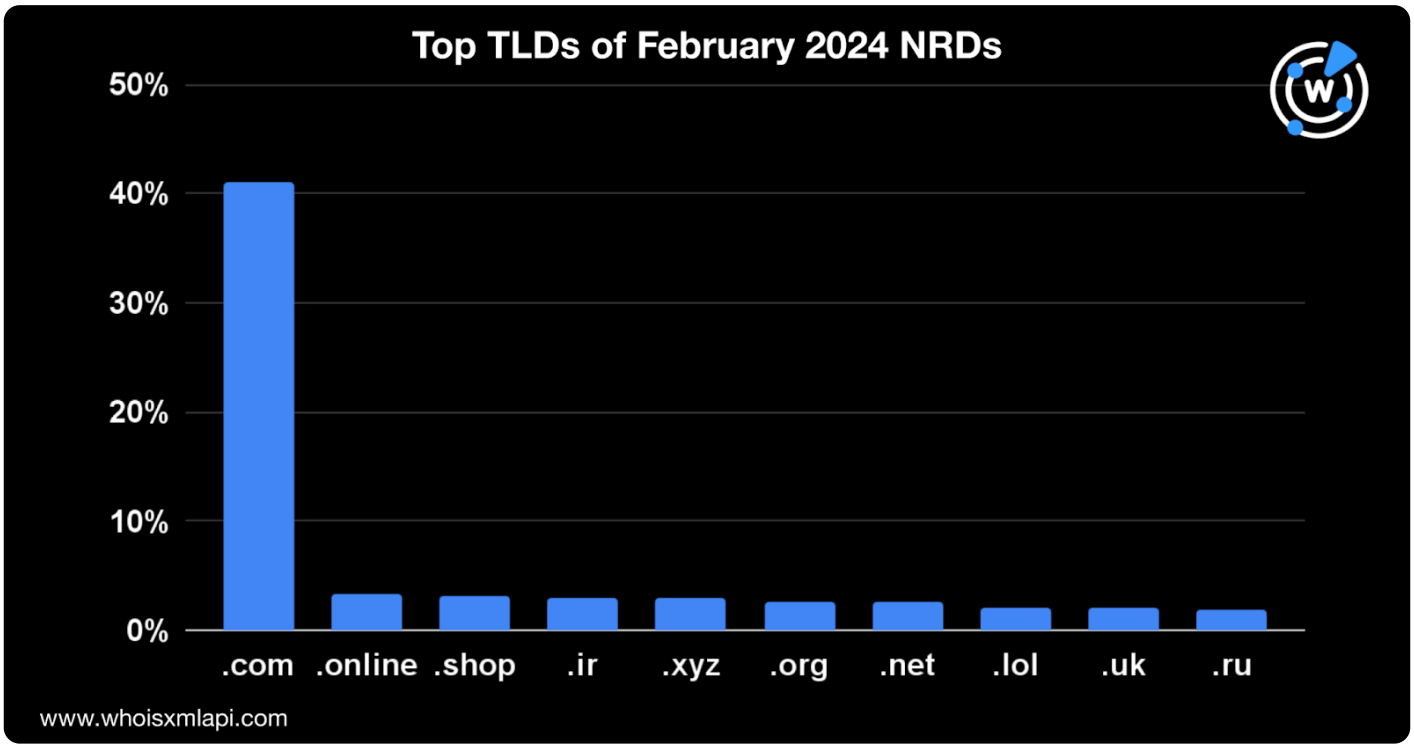
Zooming in on the February NRDs

TLD Distribution

Of the 6.6 million domains registered in February 2024, 77.4% used generic TLD (gTLD) extensions, while 22.6% used country-code TLDs (ccTLDs).



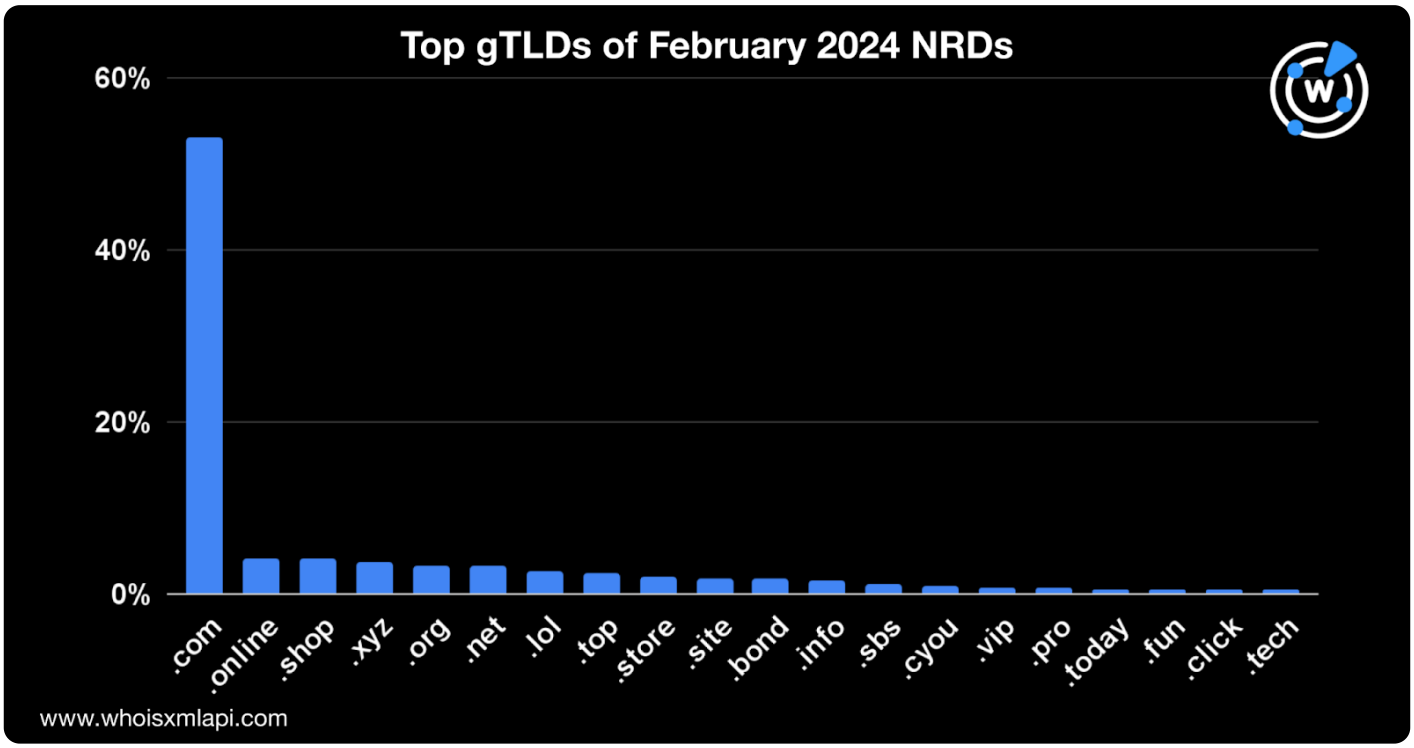
As in the previous months, .com continued to be the most used, accounting for about 41.1% of the NRDs. It was followed by .online with a 3.3% share; .shop with 3.2%; .ir with 3%; .xyz with 2.9%; .org with 2.6%; .net with 2.5%; and .lol, .uk, and .ru with 2% each.



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

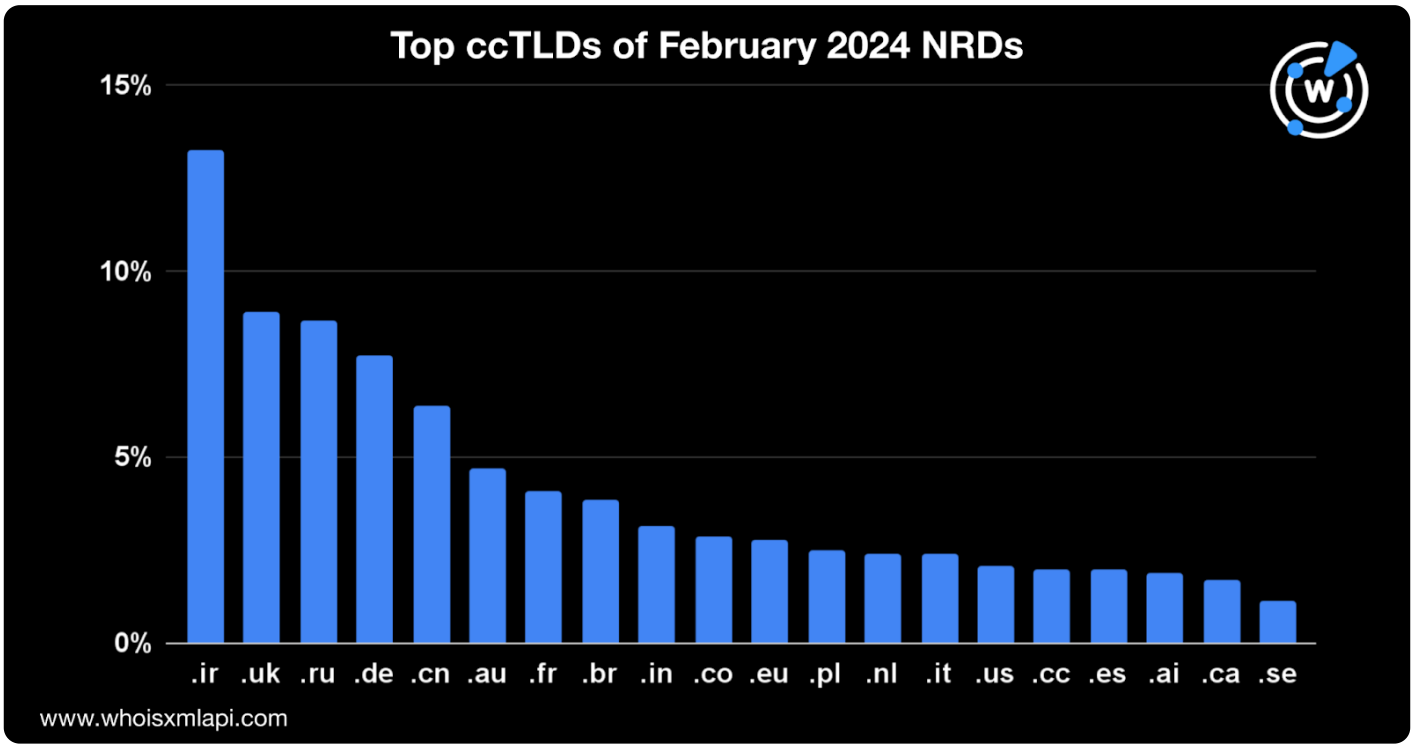
Out of more than 640 gTLDs, .com accounted for 53.1% of the NRDs sporting gTLDs and the rest of the top 20 followed with a significant gap.

For instance, e-commerce-related gTLDs .online and .shop came in second place with a 4.2% share each; .xyz with 3.7%; .org with 3.4%; .net with 3.3%; .lol with 2.6%; .top with 2.5%; .store with 2.1%; .site with 1.9%; .bond with 1.8%; .info with 1.5%; .sbs with 1.1%; .cyou with 1%; .vip with 0.8%; .pro with 0.7%; .today, .fun, and .click with 0.5% each; and .tech with 0.4%.



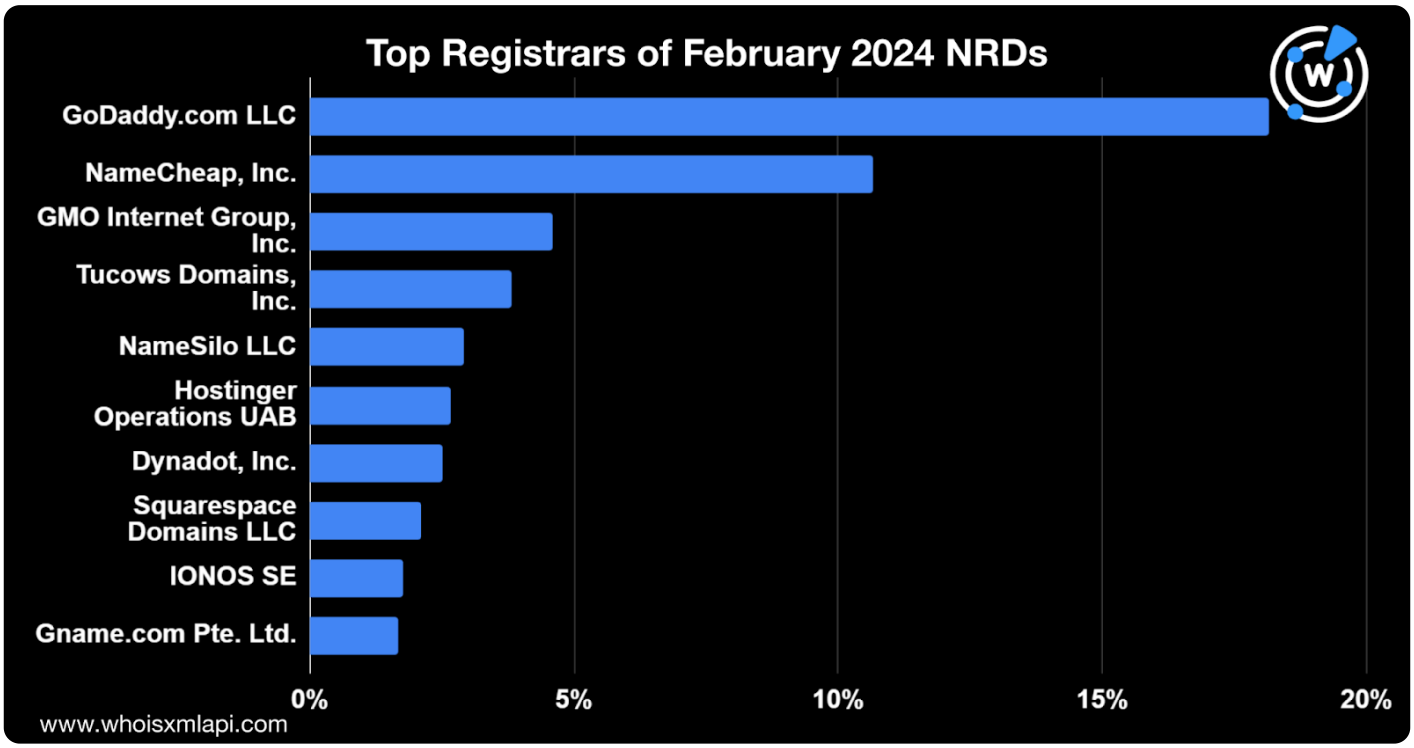
On the other hand, .ir was the most used ccTLD out of more than 230 ccTLDs, with a 13.2% share of the new domains sporting ccTLDs.

It was followed by .uk with an 8.9% share; .ru with 8.7%; .de with 7.7%; .cn with 6.4%; .au with 4.7%; .fr with 4.1%; .br with 3.8%; .in with 3.2%; .co with 2.9%; .eu with 2.8%; .pl with 2.5%; and .nl and .it with 2.4% each. The rest of the top 20 were .us (2.1%), .cc (2%), .es (2%), .ai (1.9%), .ca (1.7%), and .se (1.1%). Together, these ccTLDs accounted for 84.8% of the February NRDs under ccTLDs.



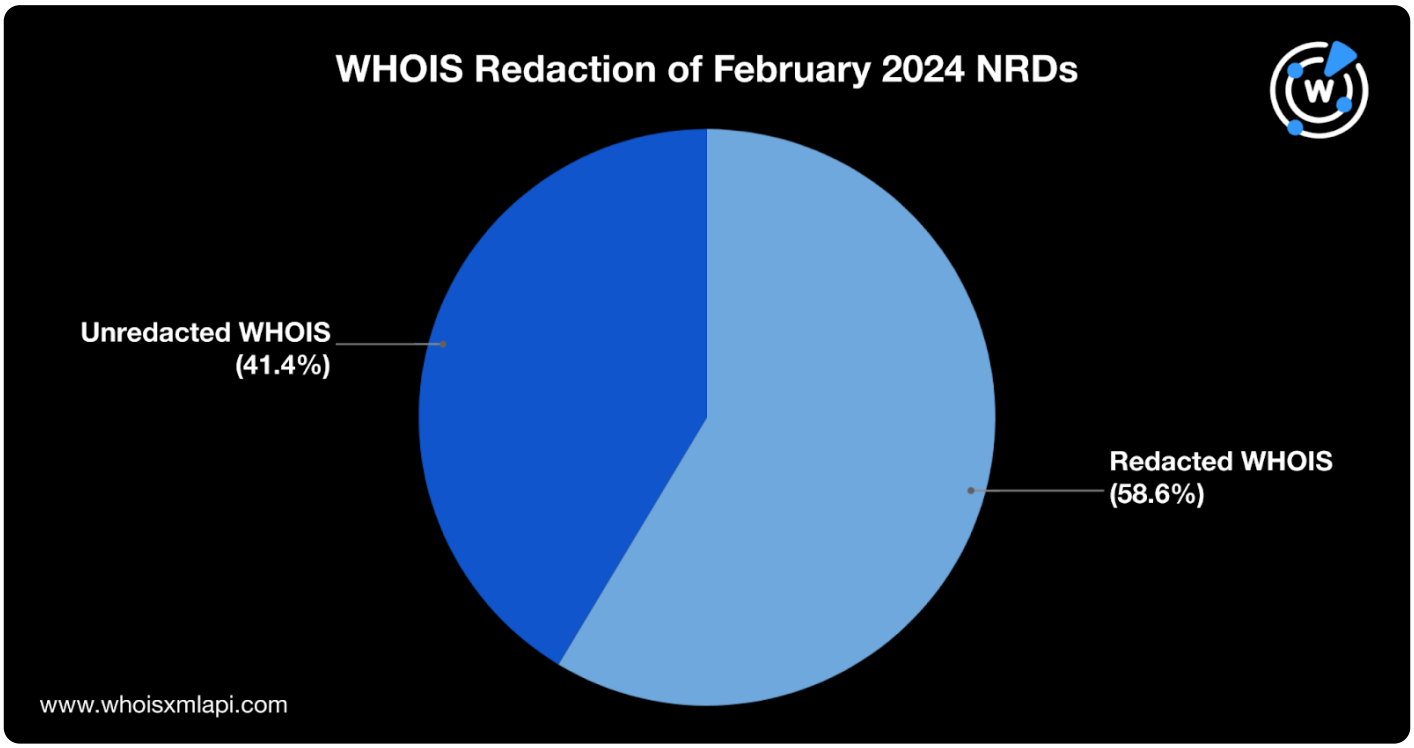
Registrar Distribution

The most popular registrar was GoDaddy.com LLC, accounting for an 18.1% share, followed by Namecheap, Inc. with 10.7%; GMO Internet Group, Inc. with 4.6%; and Tucows Domains, Inc. with 3.8%. The rest of the top 10 registrars in February were NameSilo LLC (2.9%); Hostinger Operations UAB (2.7%); Dynadot, Inc. (2.5%); Squarespace Domains LLC (2.1%); IONOS SE (1.8%); and Gname.com Pte. Ltd. (1.7%).



WHOIS Data Redaction

WHOIS record redaction was common among the February NRDs. About 58.6% of the NRDs had privacy-protected WHOIS data, while 41.4% had public WHOIS records.

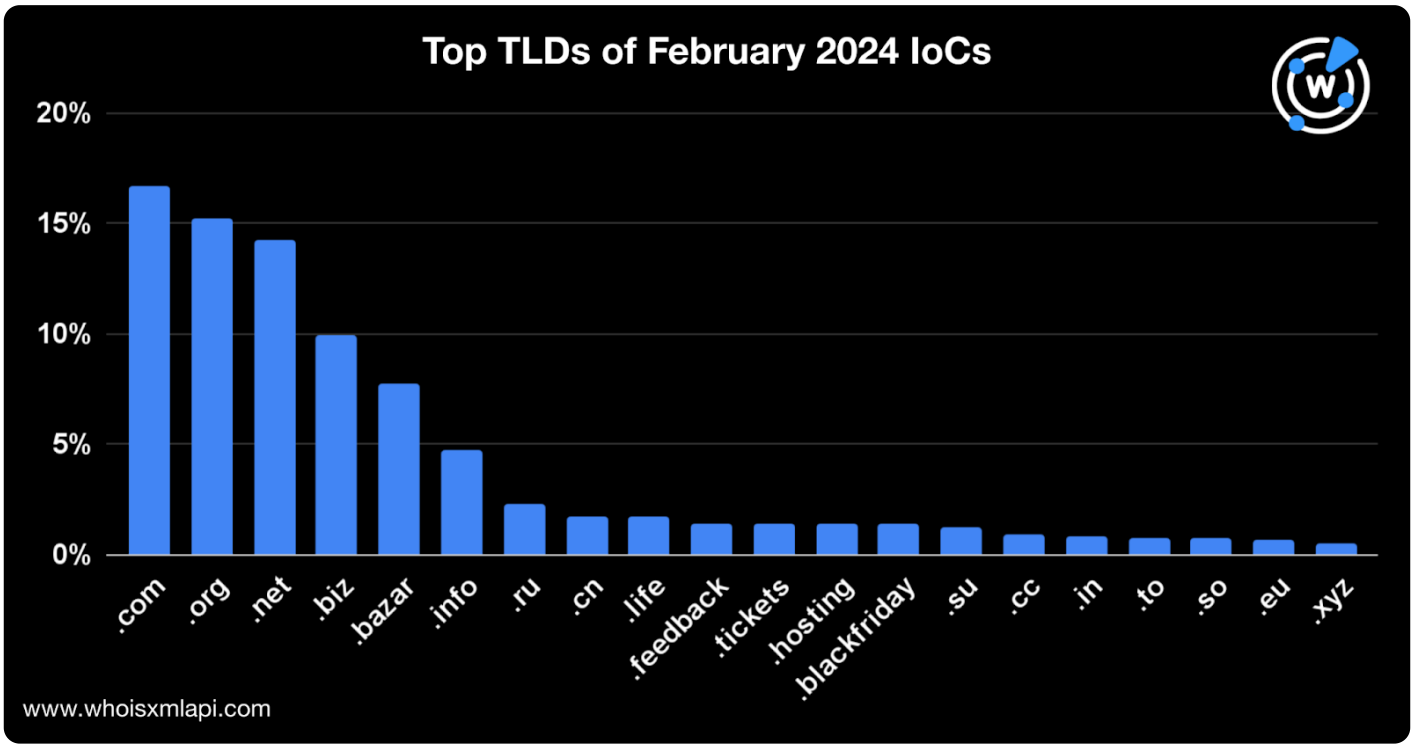


Cybersecurity through the DNS Lens

Top TLDs of the February IoCs

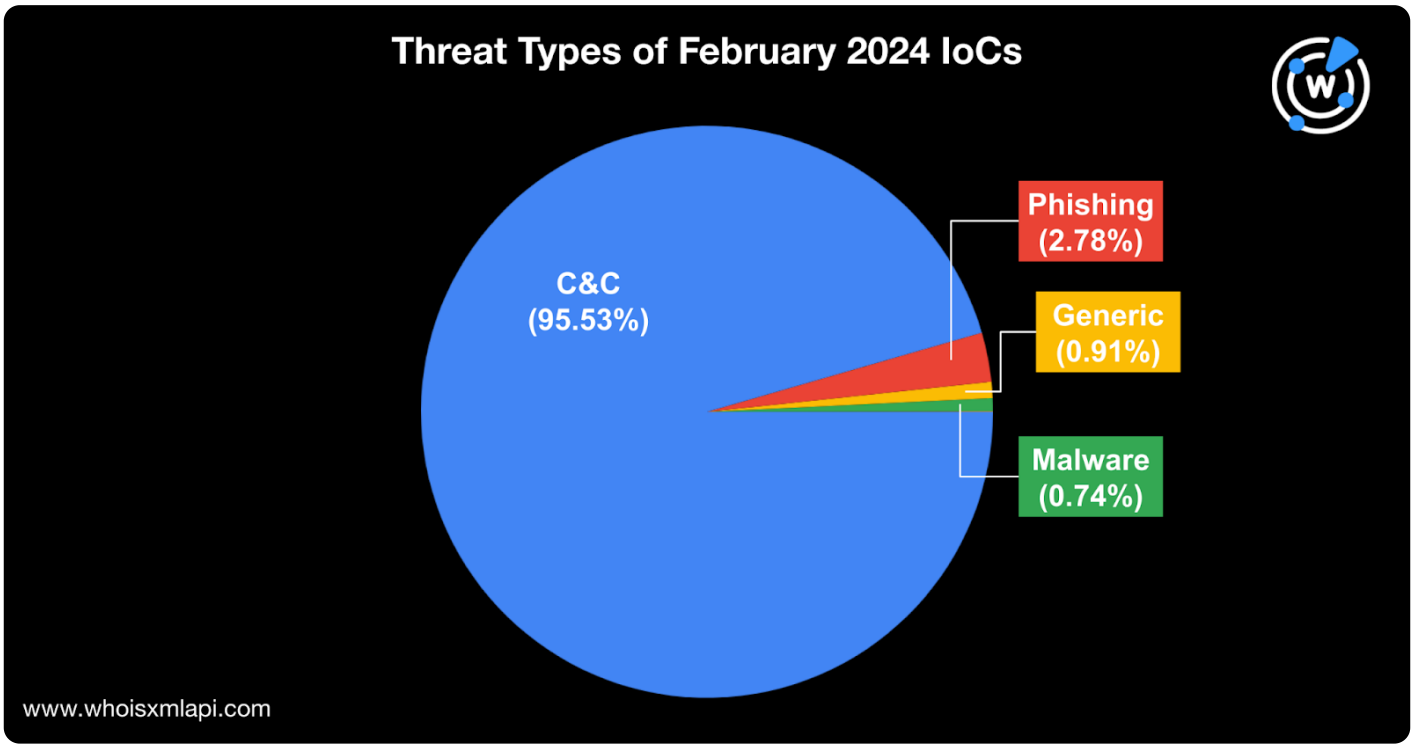
Our researchers then analyzed more than 1 million domains tagged as IoCs for various threats in February.

We discovered that 16.6% of the IoCs used .com, making it the most popular gTLD. Other major gTLD extensions followed, including .org with a 15.2% share, .net with 14.3%, and .biz with 10%. Some ccTLDs were also used, such as .ru with a 2.3% share, .cn with 1.7%, and .su with 1.2%, among others.



Threat Type Breakdown of the February IoCs

We then grouped the February IoCs based on the types of threats they were associated with. Most of them, 95.53% to be exact, were related to command-and-control (C&C) servers. The rest figured in phishing campaigns (2.78%), malware distribution (0.74%), and other forms of cyber attacks (0.91%).



Threat Reports

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

- **Tracing Ivanti Zero-Day Exploitation IoCs in the DNS:** From a list of 20 IoCs related to the vulnerability exploitation of Ivanti products, our research team uncovered 397 potential artifacts that share the IoCs' email addresses, IP resolutions, and string usage.
- **DNS Investigation: Is xDedic Truly Done for After Its Takedown?:** The WhoisXML API research team's expansion of 19 xDedic IoCs led to the discovery of 150 email-, IP-, and string-connected artifacts even after law enforcers took down the cybercrime-as-a-service (CaaS) marketplace.
- **DNS Deep Diving into Pig Butchering Scams:** We looked into the new scam dubbed "pig butchering" by analyzing eight IoCs, leading us to identify 141 connected artifacts.

- **The New RisePro Version in the DNS Spotlight**: Our researchers investigated 10 IoCs related to the newly detected RisePro variant, enabling us to discover hundreds of potential artifacts, many of which were malicious.

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.