December 2023: Domain Activity Highlights

Posted on January 11, 2024

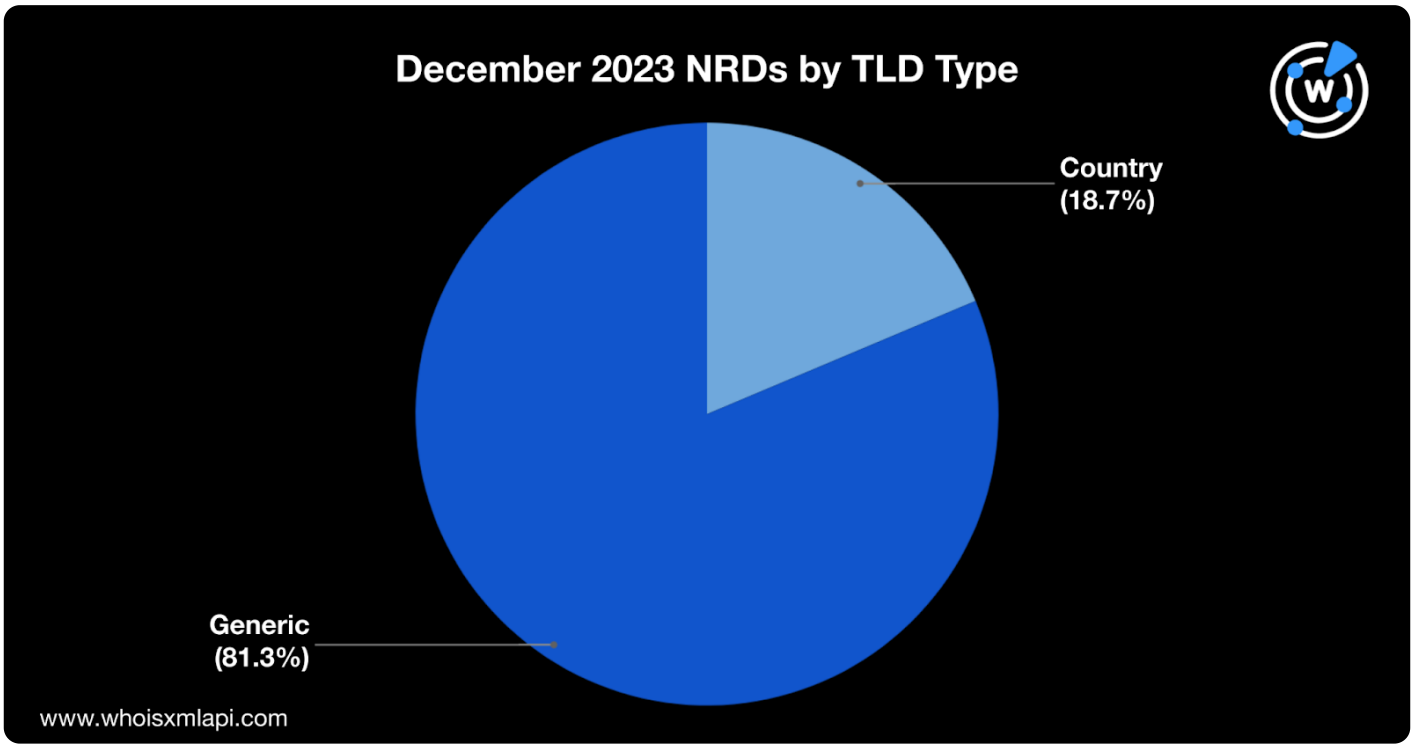
WhoisXML API researchers analyzed more than 9.6 million domains registered between 1 and 31 December 2023 to identify domain registration trends, including the most used top-level domain (TLD) extensions and registrars.

Our researchers also studied the TLD usage and threat type of about 1.5 million domains tagged as indicators of compromise (IoCs) in December. The findings are summarized below, along with links to the threat reports developed using DNS, IP, and domain intelligence sources.

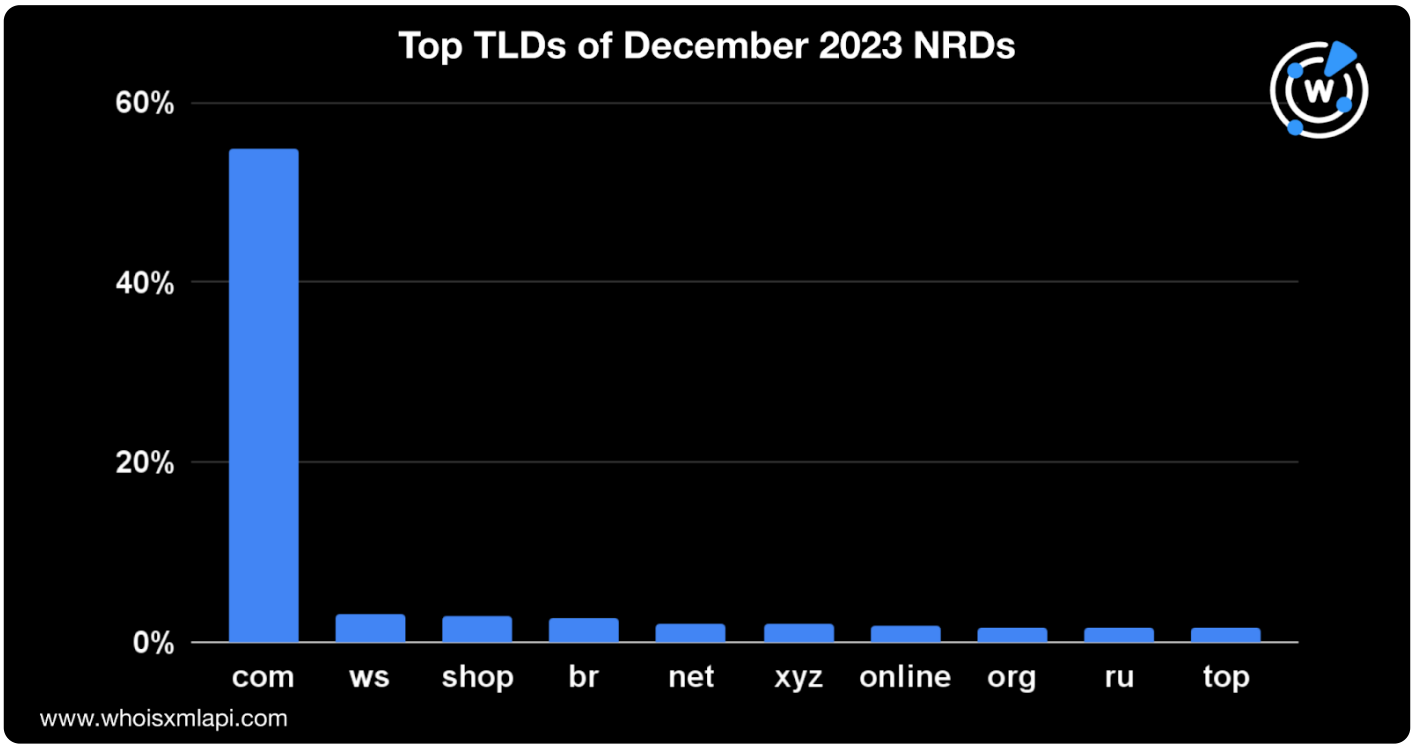
Zooming in on the December NRDs

TLD Distribution

About 81.3% of the total number of registered domains used generic TLDs (gTLDs), while 18.7% sported country-code TLDs (ccTLDs).

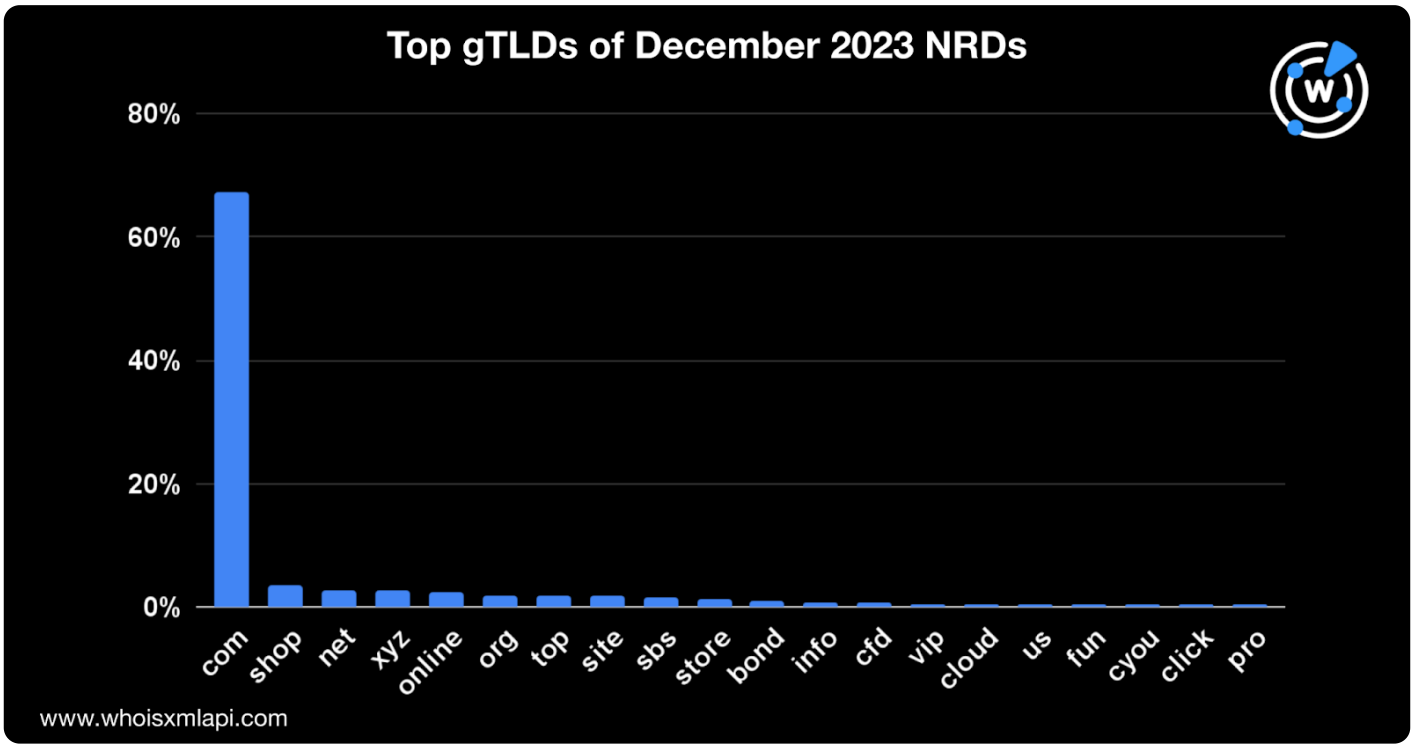


Overall, the top TLD was .com, accounting for 54.8% of the newly registered domains (NRDs), followed by .ws with a 3.1% share; .shop with 3%; .br with 2.7%; .net and .xyz with 2.1% each; .online with 1.9%; .org with 1.6%; and .ru and .top 1.5% each.

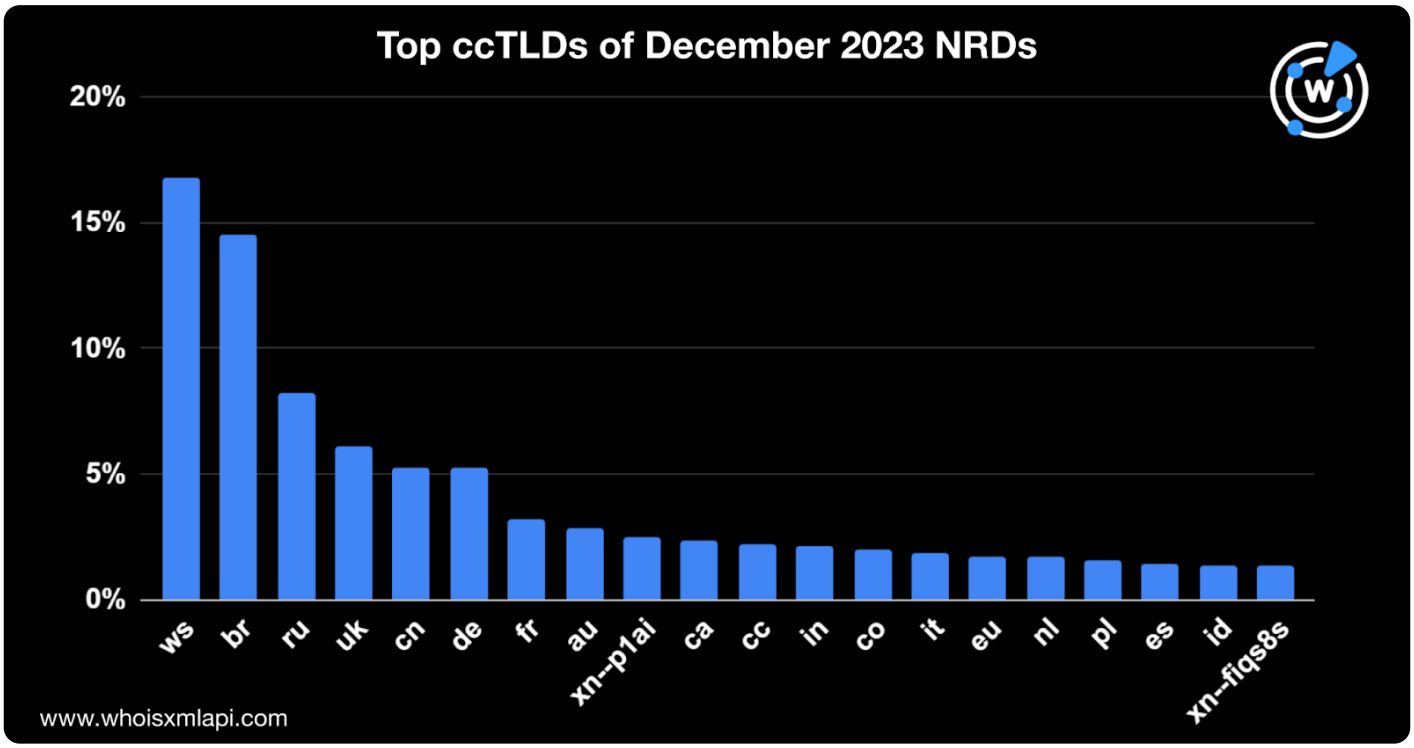


We then analyzed the usage of each TLD type to determine the most used gTLDs and ccTLDs, respectively.

Out of more than 625 gTLDs, .com remained the most popular gTLD extension, accounting for 67.3% of the total number of NRDs with gTLD extensions. The rest of the top 20 gTLDs had a substantial gap from .com. They included .shop (3.7%), .net and .xyz (2.6% each); .online (2.4%); .org and .top (1.9% each); .site (1.8%); .sbs (1.6%); .store and .bond (1.2% each); .info (0.9%); .cfd (0.7%); .vip, .cloud, .us, and .fun (0.5% each); and .cyou, .click, and .pro (0.4% each).

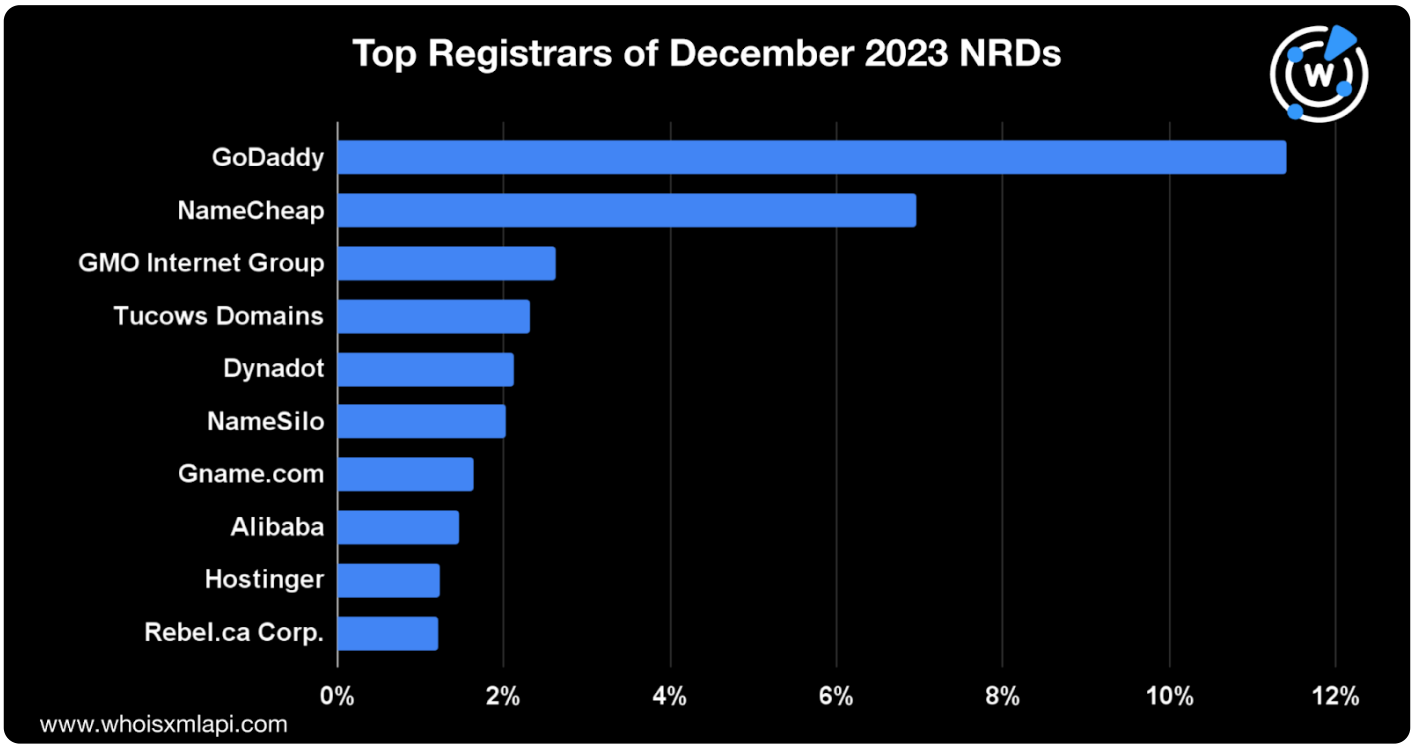


Meanwhile, .ws was the most popular out of more than 240 ccTLDs with a 16.8% share of the December NRDs. It was followed by .br (14.6%), .ru (8.3% each), .uk (6.1%), .cn and .de (5.2% each), .fr (3.2%), .au (2.8%), .xn--p1ai (2.5%), .ca (2.4%), and .cc (2.2%). The rest of the top 20 ccTLDs are shown in the graph below.



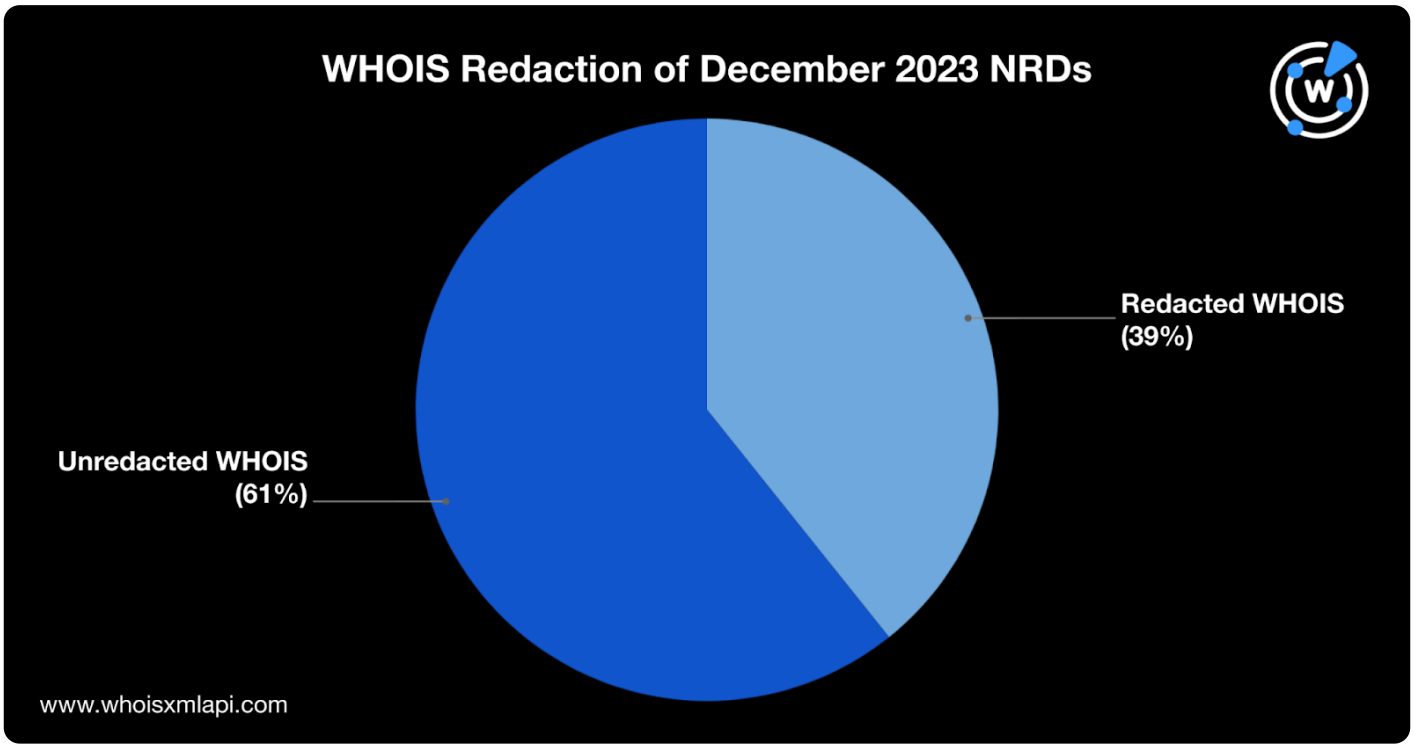
Registrar Distribution

GoDaddy remained the most used registrar among the December NRDs, accounting for 11.4% of the total domain registration volume. Namecheap followed with a 7% share, GMO Internet with 2.6%, Tucows with 2.3%, Dynadot with 2.1%, NameSilo with 2%, Gname with 1.6%, Alibaba Cloud Computing with 1.5%, and Hostinger and Rebel.ca with 1.2% each.



WHOIS Data Redaction

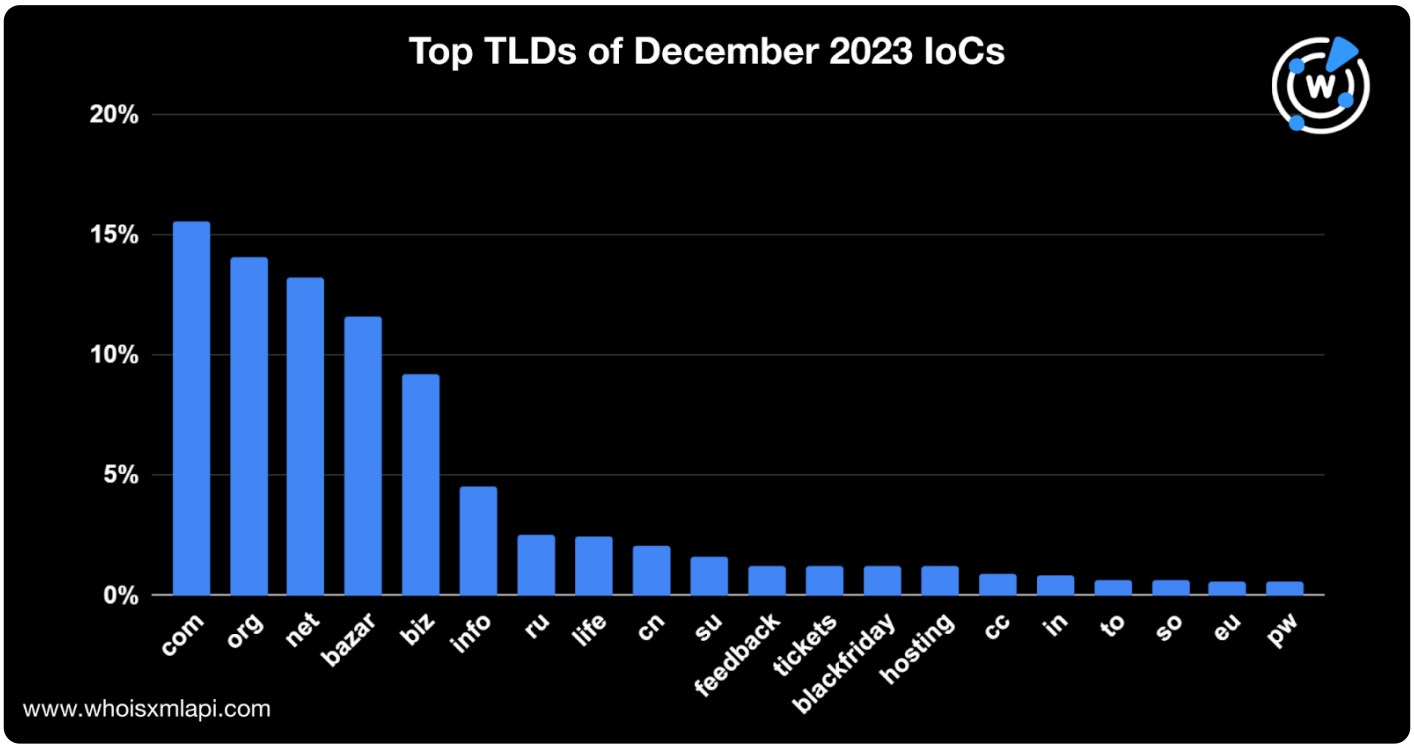
About 61% of the December NRDs had unredacted WHOIS records, while 39% used various WHOIS privacy redaction methods.



Cybersecurity through the DNS Lens

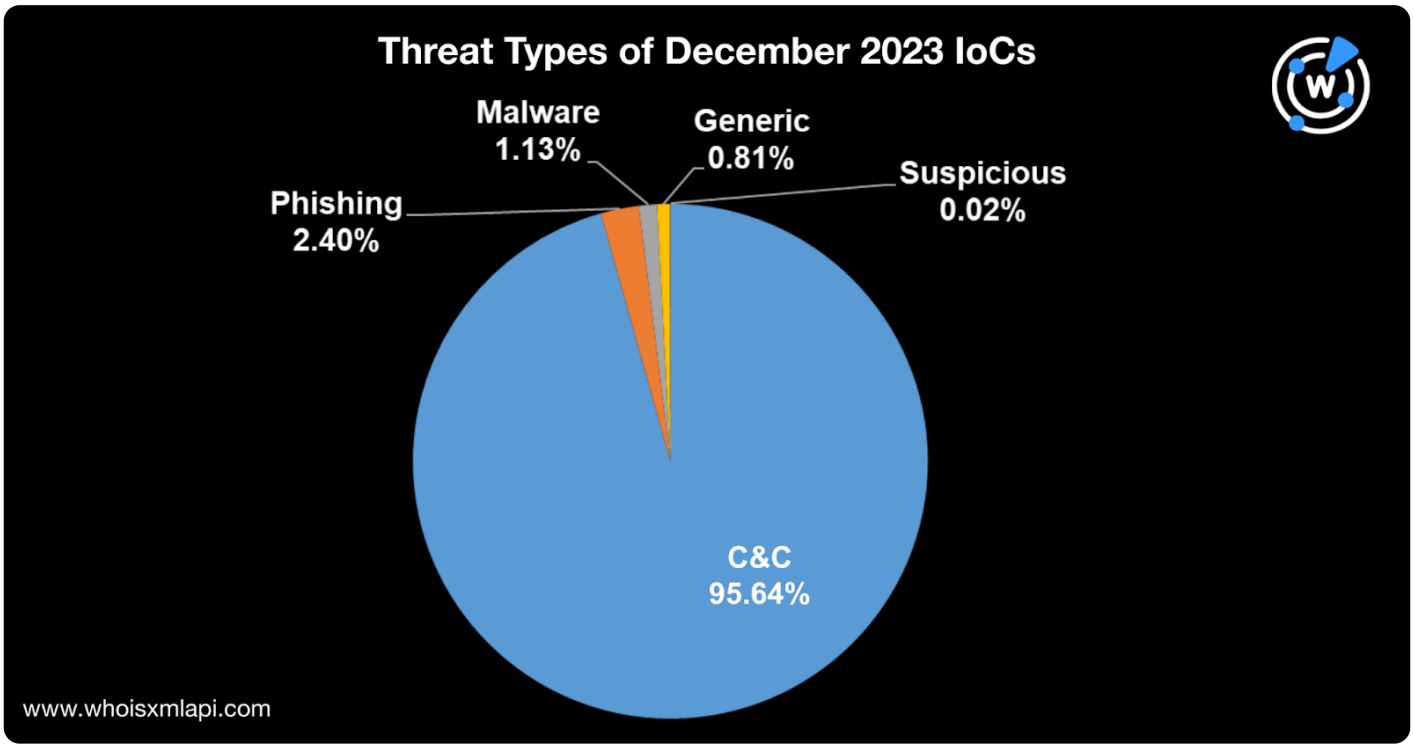
Top TLDs of the December IoCs

We analyzed nearly 1.5 million domains detected as IoCs in December and found that 16% used .com as their gTLD extension. Several IoCs used other major gTLDs, including .org (14%) and .net (13%). New gTLDs were also used. Approximately 12% used .bazar, 9% used .biz, 5% used .info, and 2% used .life. Others used ccTLDs, including .ru (3%%), .cn, and .su (2% each). The rest of the top 20 TLDs used by the IoCs are reflected in the graph below.



Threat Type Breakdown of the December IoCs

Our researchers categorized the IoCs detected in December into different threat types and discovered that most were tagged as command-and-control (C&C) servers (95.64%), while 2.4% figured in phishing campaigns and 1.13% in malware distribution. Approximately 0.8% were involved in other forms of cyber attacks, while 0.02% were tagged in suspicious activities. The threat type breakdown is reflected in the chart below.



Threat Reports

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

- **Unveiling Stealthy WailingCrab Aided by DNS Intelligence:** From a list of 24 IoCs involved in the distribution of the WailingCrab malware, our researchers uncovered 3,000+ potential artifacts.
- **A Peek Under the Hood of the Atomic Stealer Infrastructure:** WhoisXML API researchers dove into the IoCs connected to Atomic Stealer and found dozens of IP- and email-connected artifacts.
- **A Fake ID Marketplace under the DNS Lens:** After threat researcher Dancho Danchev found an email address belonging to a fake ID seller, our researchers performed an in-depth investigation and discovered several potential artifacts.

- **Behind the Genesis Market Infrastructure: An In-Depth DNS Analysis:** Our research team discovered several domains and IP addresses, possibly part of the Genesis Market cybercrime infrastructure.

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.