November 2023: Domain Activity Highlights

Posted on December 13, 2023

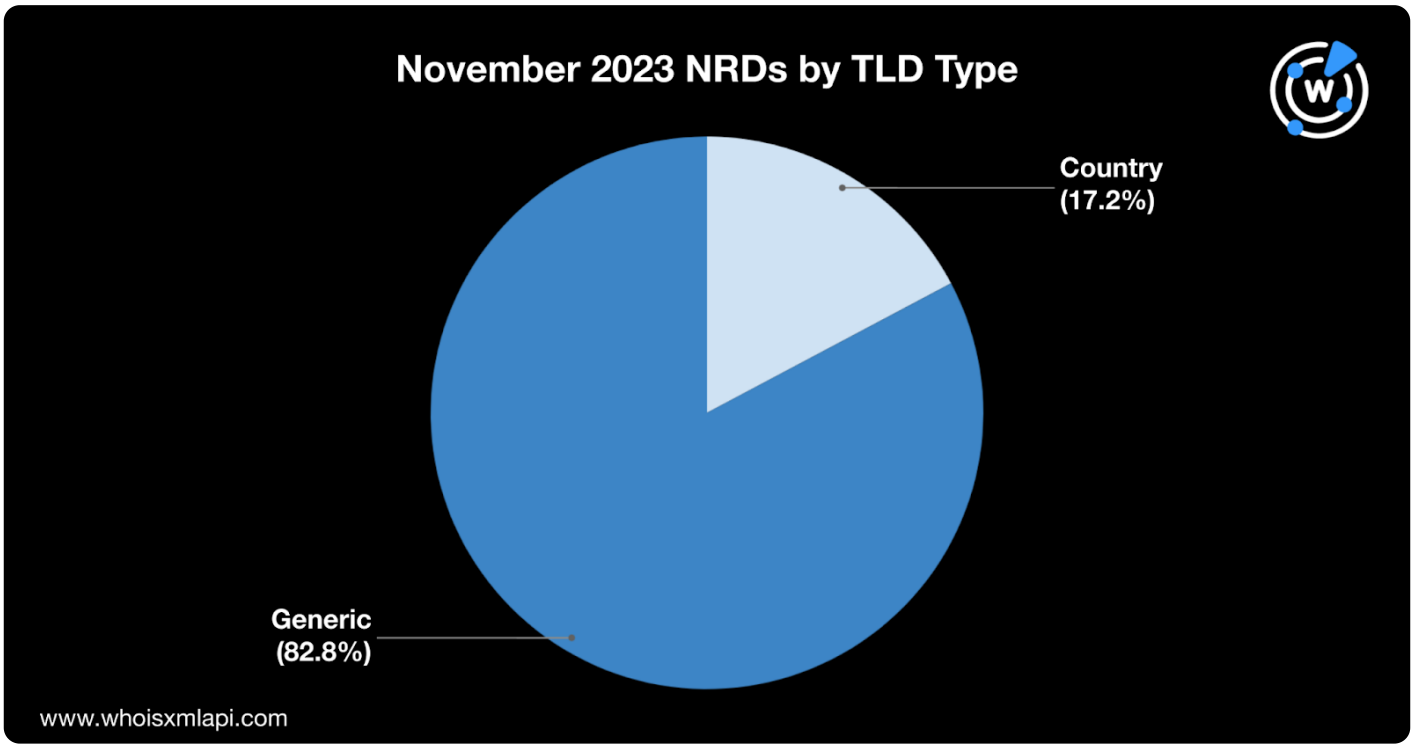
WhoisXML API researchers analyzed more than 8.7 million domains registered between 1 and 30 November 2023 to identify trends, such as the most used top-level domain (TLD) extensions and registrars.

We also studied the TLD usage and threat types of 1.1 million domains tagged as indicators of compromise (IoCs) in November. The findings and links to the threat reports we developed using DNS, IP, and domain intelligence sources are summarized below as well.

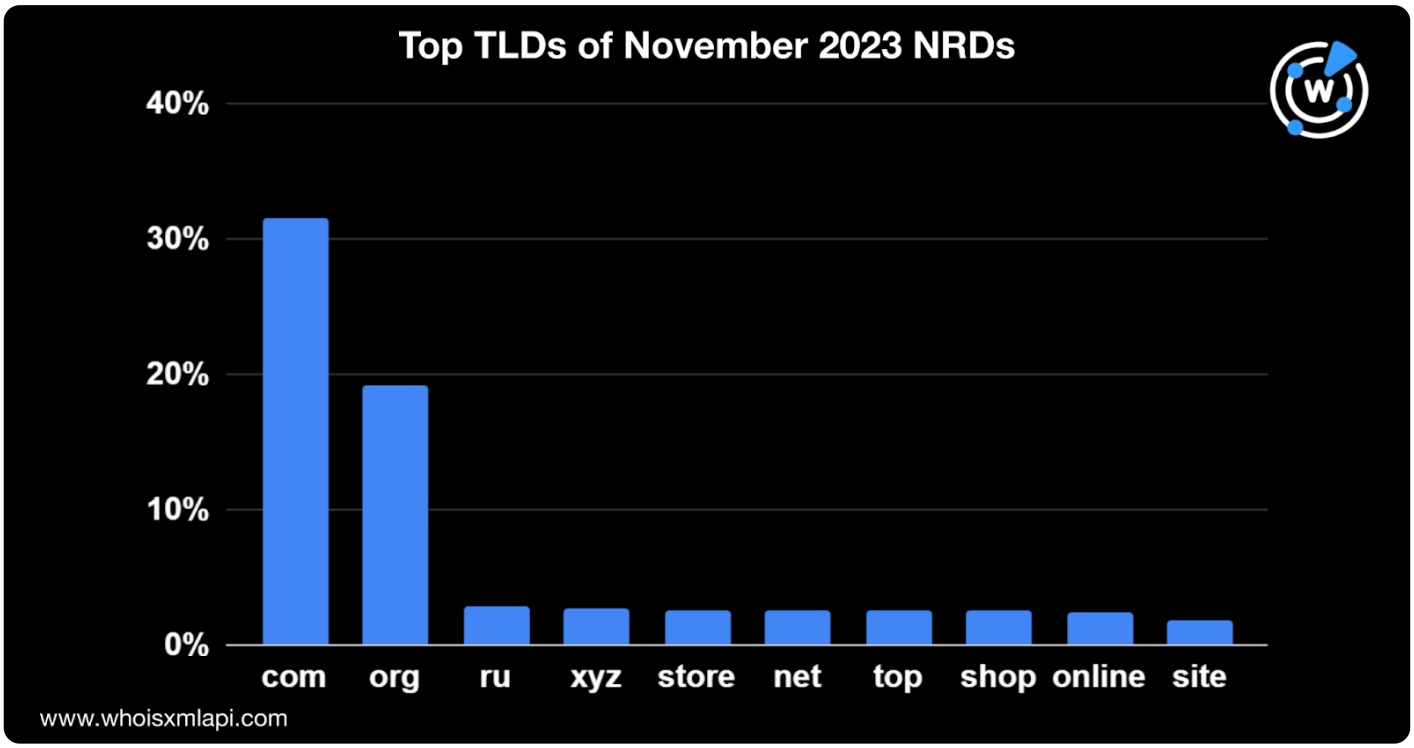
Zooming in on the November NRDs

TLD Distribution

Generic TLDs (gTLDs) were used by 82.8% of the total number of registered domains, while country-code TLDs (ccTLDs) accounted for 17.2%.

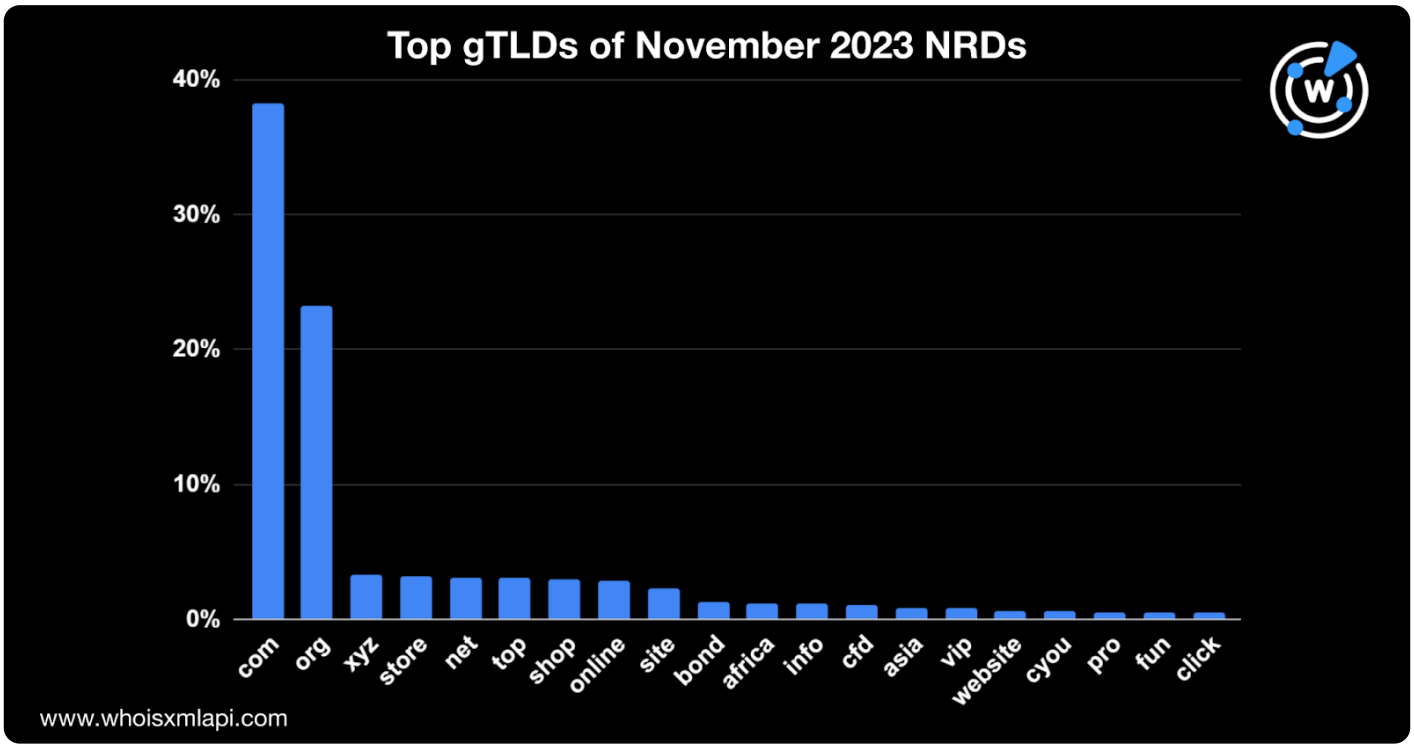


Overall, the top TLD was .com, accounting for 31.6% of the new domain registrations, followed by .org with a 19.2% share; .ru with 2.8%; .xyz with 2.7%; .store with 2.6%; and .net, .top, and .shop with 2.5% each. Completing the top 10 TLDs were .online and .site with 2.4% and 1.9% shares, respectively.

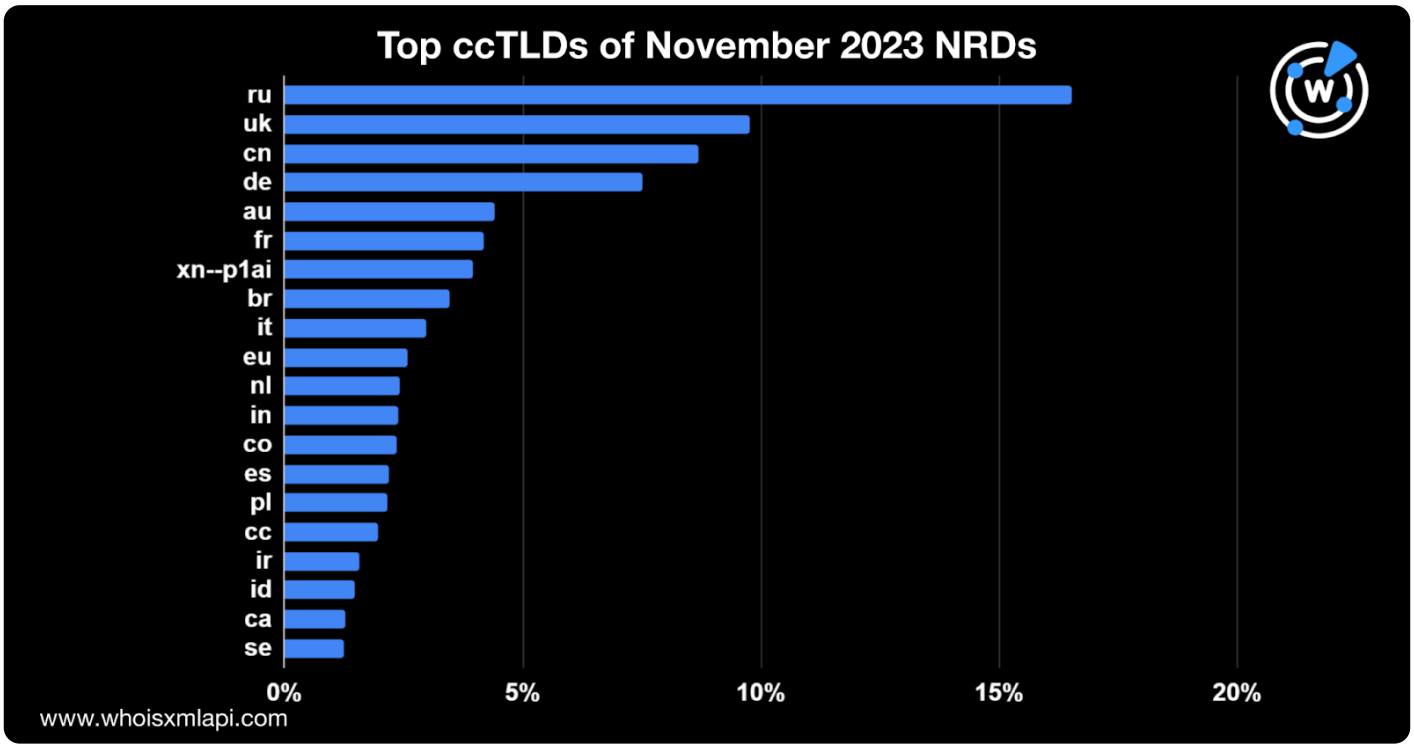


We then performed separate analyses for gTLD and ccTLD usage among the newly registered domains (NRDs) to identify the most popular TLDs by type.

Out of more than 635 gTLDs, .com emerged as the most used gTLD extension, accounting for 38.2% of the total number of NRDs using gTLDs. It was followed by .org, with a 23.2% share. The rest of the top 20 gTLDs had a considerable gap from .com and .org. The gTLDs .xyz (3.3%), .store (3.2%), .net (3.1%), .top (3%), and .shop (3%) ranked third to seventh, respectively. Other significant players were .online (2.9%), .site (2.3%), and .bond (1.3%). The chart below shows these and the rest of the top 20 gTLDs.

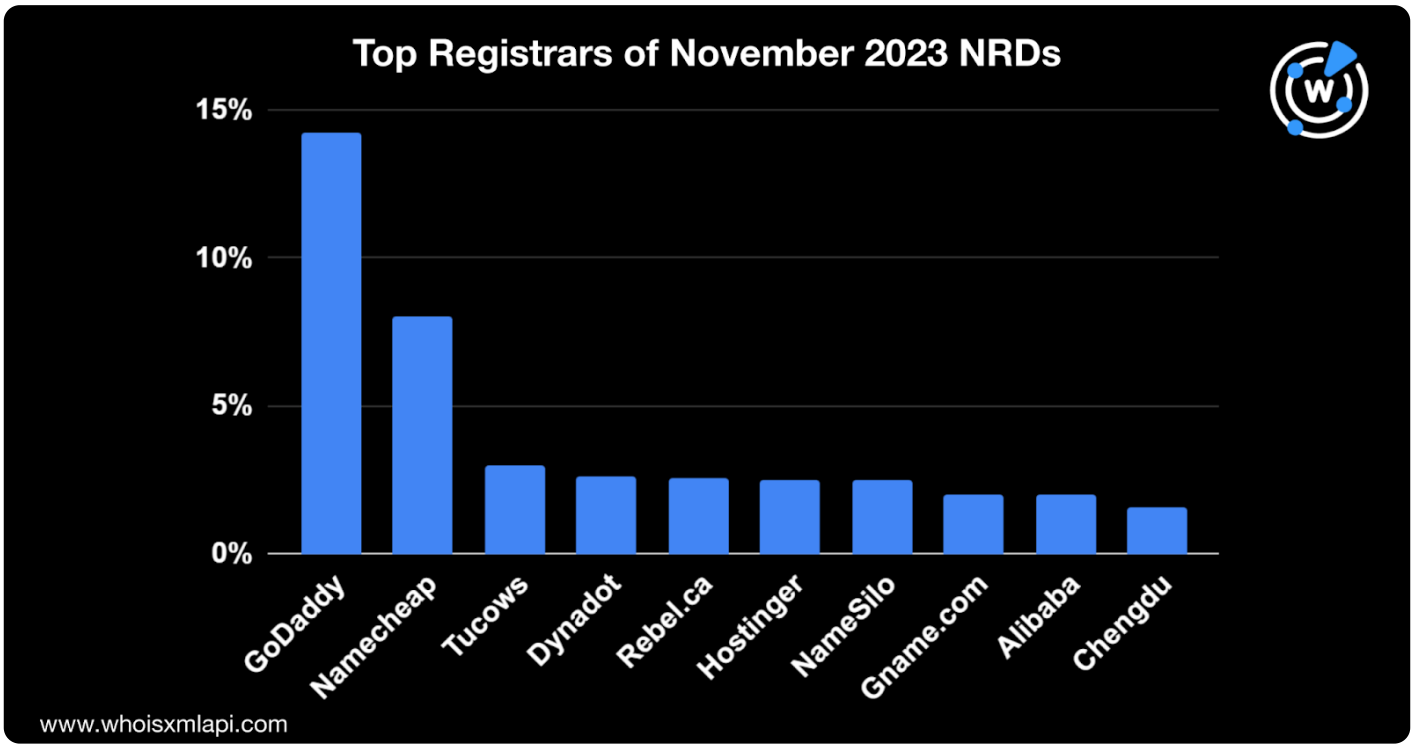


Meanwhile, .ru was the most popular out of more than 240 ccTLDs, with a 16.5% share of the November NRDs with ccTLD extensions. It was followed by .uk (9.8%), .cn (8.7%), .de (7.5%), .au (4.4%), .fr (4.2%), .xn--p1ai or .?? (4%), .br (3.5%), .it (3%), and .eu (2.6%). The rest of the top 20 ccTLDs are shown in the graph below.



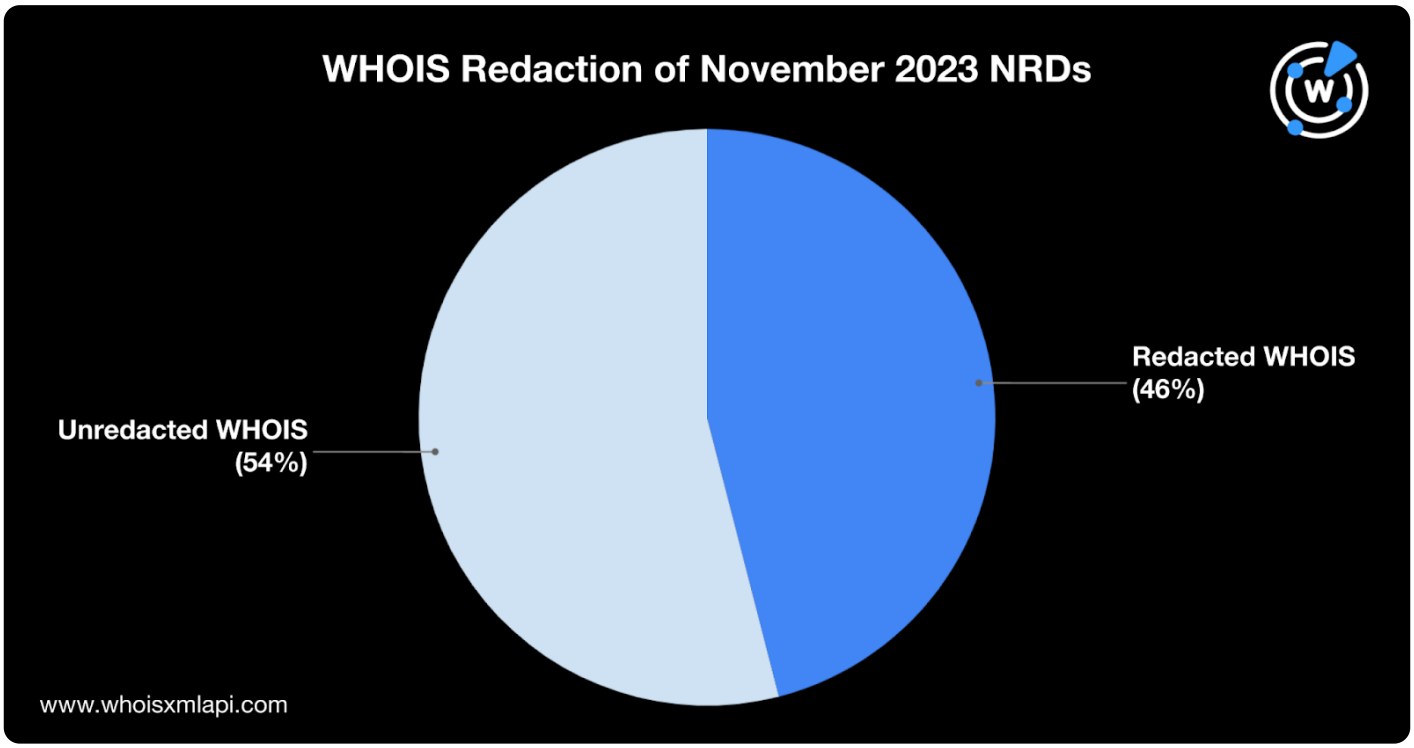
Registrar Distribution

GoDaddy emerged as the top registrar among more than 2,900 others, accounting for 14.2% of the NRDs. Namecheap, Inc. followed with an 8.1% share; Tucows Domains, Inc. with 3%; Dynadot, Inc. and Rebel.ca Corp. with 6% each; and Hostinger Operations, UAB, and NameSilo, LLC with 2.5% each. Other registrars that made it to the top 10 were Gname.com Pte. Ltd., Alibaba Cloud Computing Ltd. (2% each), and Chengdu West Dimension Digital Technology Co. Ltd. (1.6%).



WHOIS Data Redaction

More than half of the November NRDs had public or unredacted WHOIS records, while 46% used various privacy redaction methods.

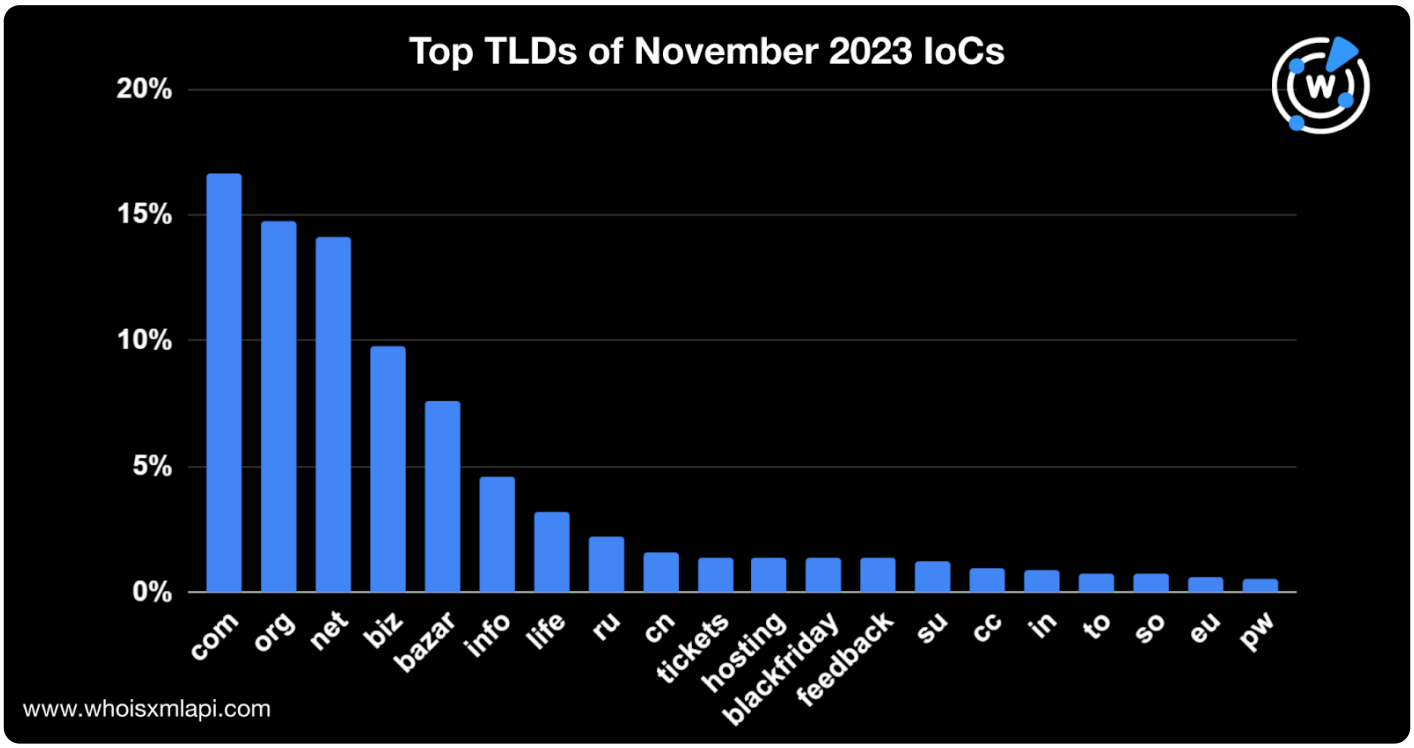


Cybersecurity through the DNS Lens

Top TLDs of November IoCs

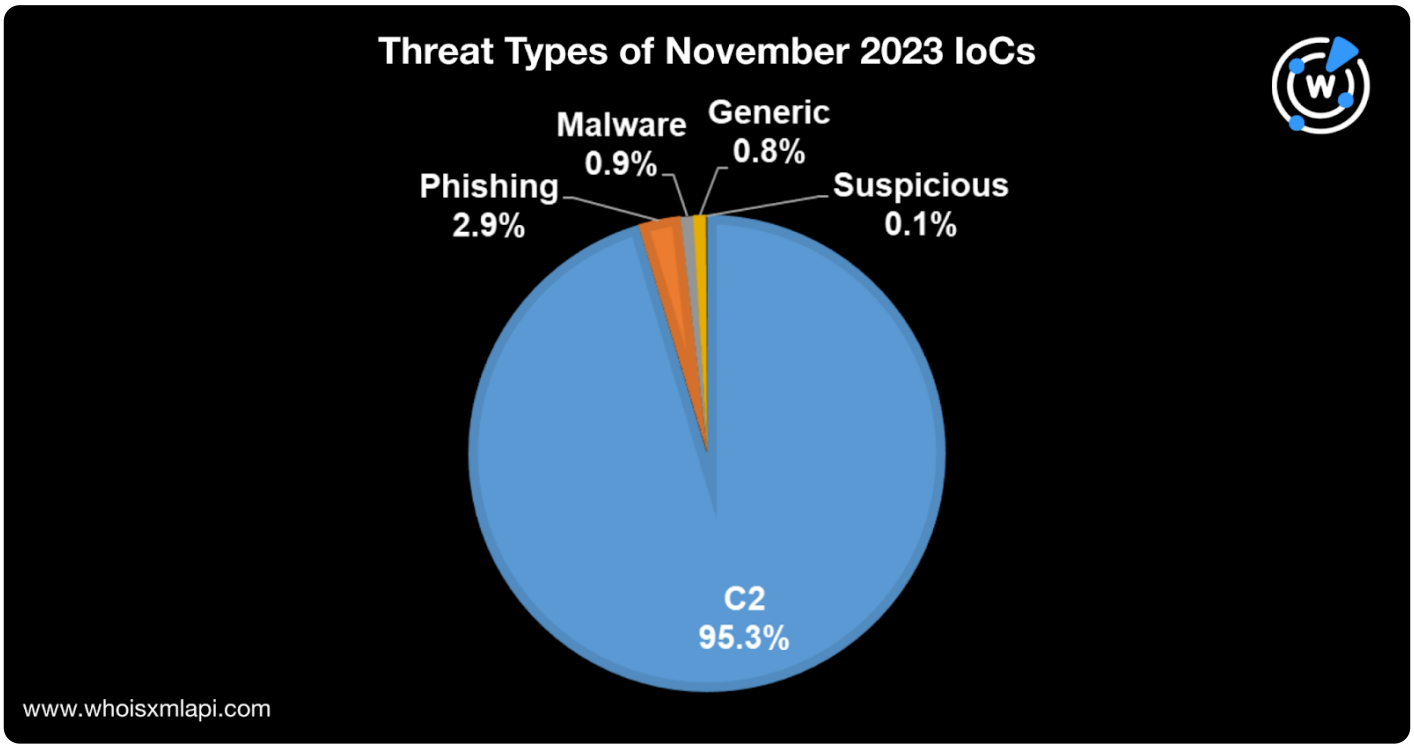
Our researchers analyzed the TLD usage of more than 1.1 million domains detected as IoCs in November and found that .com was the top TLD, with a 16.6% share of the IoCs.

Approximately 14.8% used .org, while 14.1% used .net. Several IoCs used new gTLDs (ngTLDs), such as .biz (9.8%), .bazar (7.6%), .info (4.6%) .life (3.2%), and .tickets (1.4%). Meanwhile, others used ccTLDs, most notably .ru (2.2%) and .cn (1.6%). The rest of the top 20 TLDs used in the IoCs were mostly ccTLDs and ngTLDs.



Threat Type Breakdown of the November IoCs

WhoisXML API threat intelligence enabled us to categorize the 1.1 million IoCs based on threat type. Most IoCs were tagged as command-and-control (C&C) servers (95.3%), while 2.9% figured in phishing campaigns and 0.9% in malware distribution. About 0.8% were involved in other forms of cyber attacks, while 0.1% 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 November.

- **Rogue Bulletproof Hosts May Still Be Alive and Kicking as DNS Intel Shows:** Our researchers dove into domains connected to rogue bulletproof hosting service providers, leading us to 130+ public email addresses and 5,000+ email- and IP-connected artifacts.
- **Carding, Still in Full Swing as DNS Intel Shows:** From a list of 220 email addresses believed to be owned by carders, WhoisXML API researchers uncovered 1,700+ potential artifacts.
- **A DNS Deep Dive into BreachForums Domains:** Threat researcher Dancho Danchev found 570+ domains believed to belong to BreachForums members. We expanded this to investigate reports saying that the forum taken down by the FBI in March 2023 was back online.

- **Tracing BlackNet RAT's History through a DNS Deep Dive:** Our researchers gathered lists of BlackNet RAT IoCs and analyzed them using DNS intelligence. The investigation led to 5,800+ email- and IP-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.