December 2022: New Domain Activity Highlights

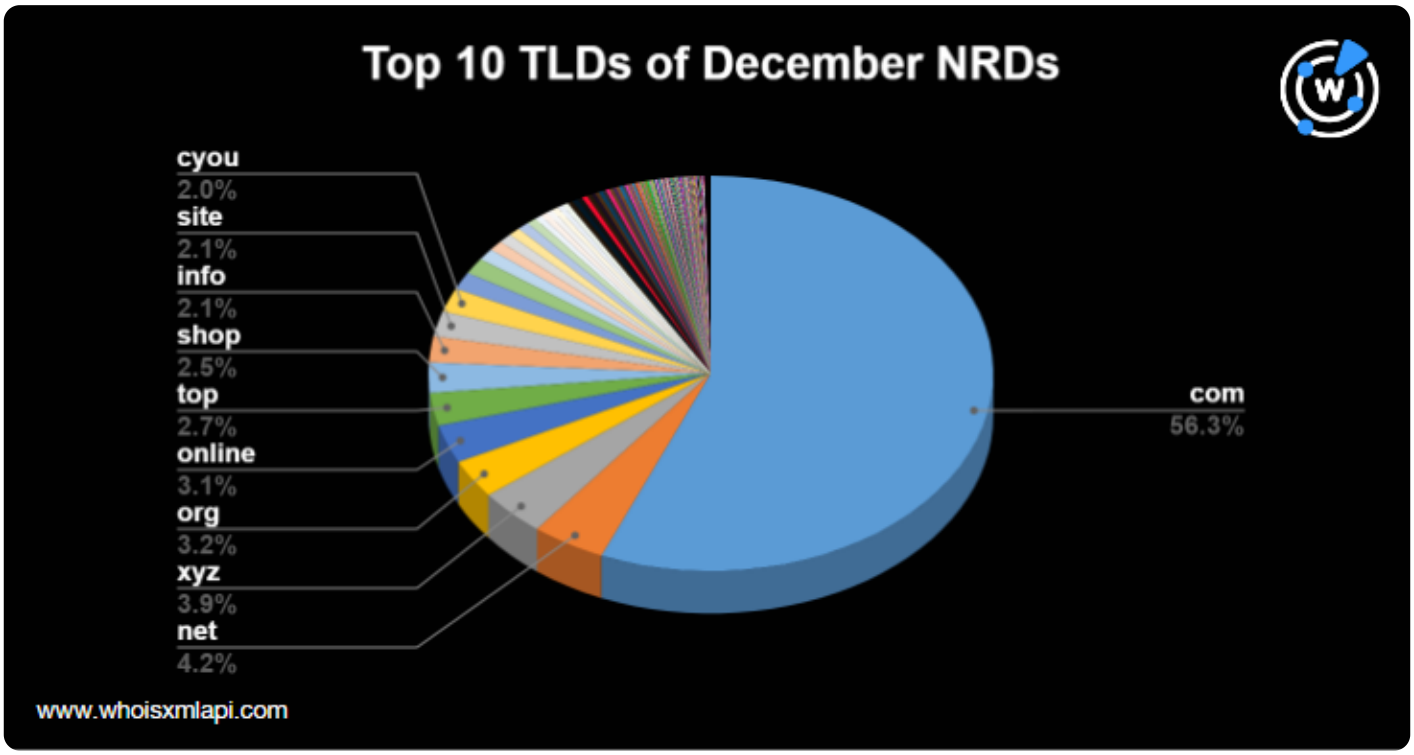
Posted on January 10, 2023

Using our extensive collection of domain intelligence, WhoisXML API researchers analyzed several millions of newly registered domains (NRDs) added on 1–31 December 2022. We studied their top-level domain (TLD), registrar, and registrant country distribution. We also looked at their text string usage as part of the effort to detect emerging trends. Check out our findings below, along with links to threat reports our researchers put together using our domain, DNS, and IP intelligence sources.

Zooming in on the December NRDs

TLD Distribution

More than half of the December NRDs fell under the .com TLD, while the rest were distributed across 700+ other TLDs. The other TLDs that made it to the top 10 list of most-used TLDs in December accounted for 25.73% of the total registration volume. They comprised generic TLDs (gTLDs) like .net, .info, and .org, and new gTLDs (ngTLDs) like .xyz, .online, .top, .shop, .site, and .cyou. See the chart below for the top 10 TLD NRD distribution.



These TLDs were also the top 10 in November, except for .cyou, which replaced .store.

Domain Registration Volume for the Most-Abused TLDs

We also analyzed how the most-abused TLDs were represented in December based on Spamhaus's list of most-abused TLDs as of 5 January 2023. The table below shows these TLDs with their corresponding badness indexes, percentage of bad domains against the total number of domains observed, and number of December NRDs that could potentially go bad based on the former percentage.

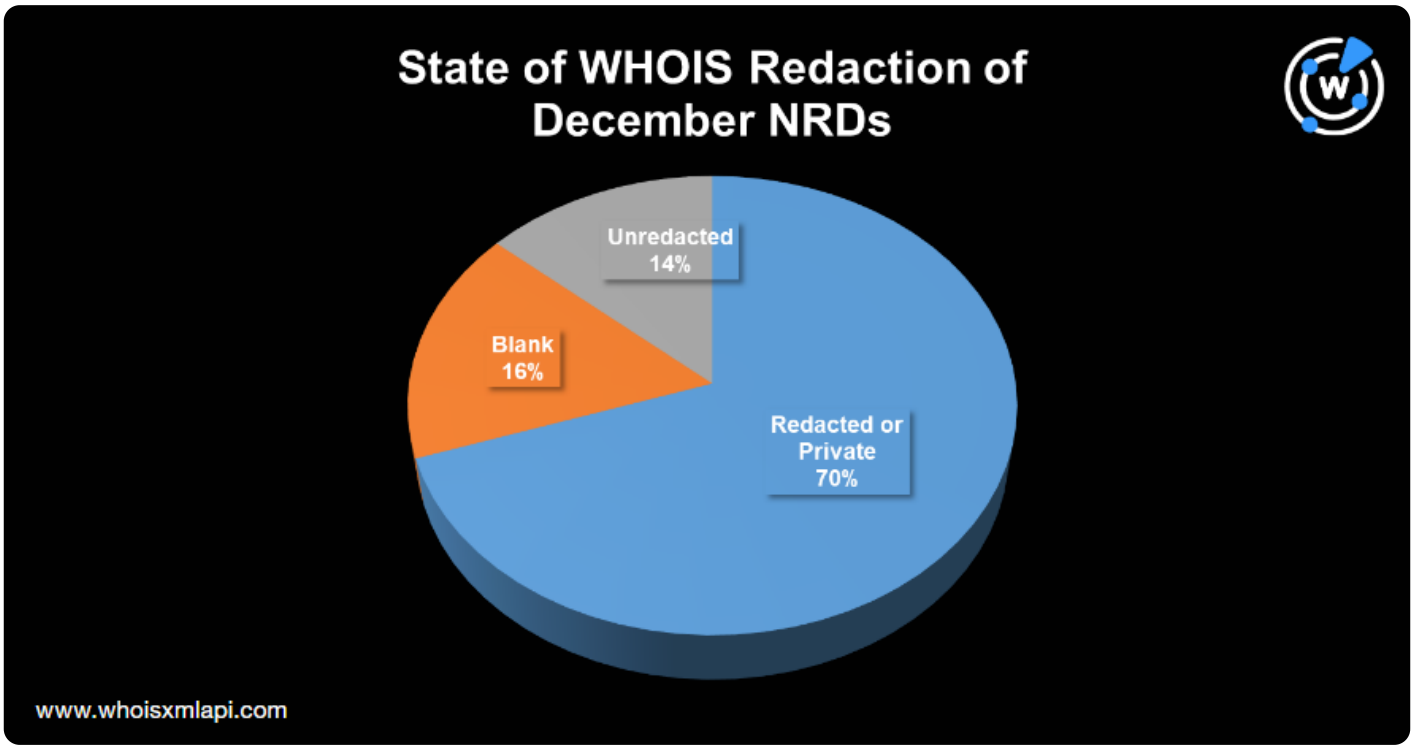
The TLD with the highest badness index was .surf at 4.49. Of the total number of domains observed, 77.3% were malicious. Note that this percentage can change over time and can't be universally applied. But theoretically speaking, that means about 53 domains of the December NRDs using .surf had the potential to be weaponized.

Bad TLDs as of 5 January 2023	Badness Index	Percentage of Observed Domains That Turned Out to Be Bad	Number of December NRDs Using the TLD	Number of December NRDs That Could Go Bad
surf	4.49	77.30%	69	53.34
fit	2.49	36.70%	2,448	898.42
live	2.33	25.50%	26,435	6,740.93
beauty	2.18	31.80%	2,640	839.52
top	1.88	19.50%	125,856	24,541.92
monster	1.35	20.10%	3,384	680.18

Overall, 3% of the December NRDs fell under the most-abused TLDs.

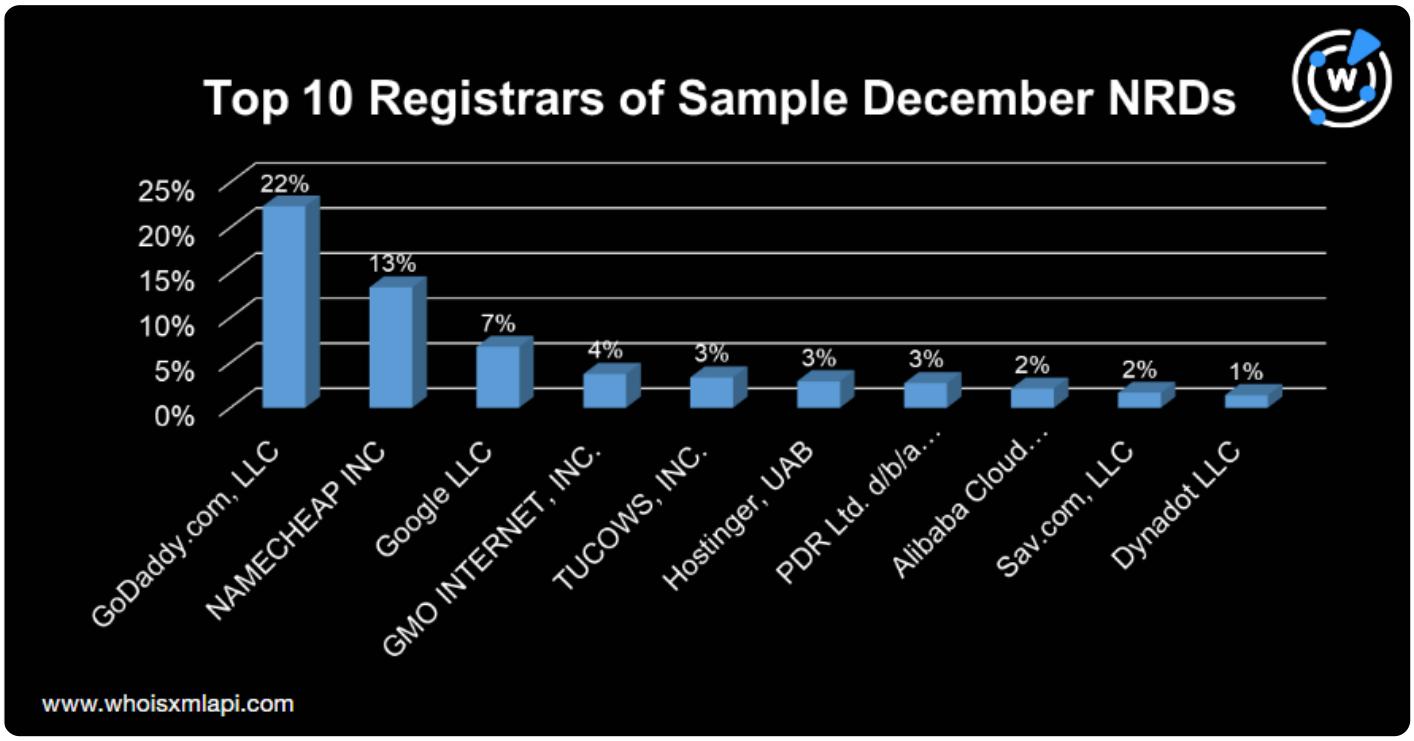
WHOIS Data Redaction

We also analyzed the state of WHOIS privacy redaction for the month using a sample of nearly 21,000 domains. About 70% of the NRDs had redacted or privacy-protected WHOIS records based on their identified registrant names. Only 14% had unredacted registrant names, but even fewer publicized their email addresses. The rest of the sample left the registrant name field blank, which translated to keeping their registration private.



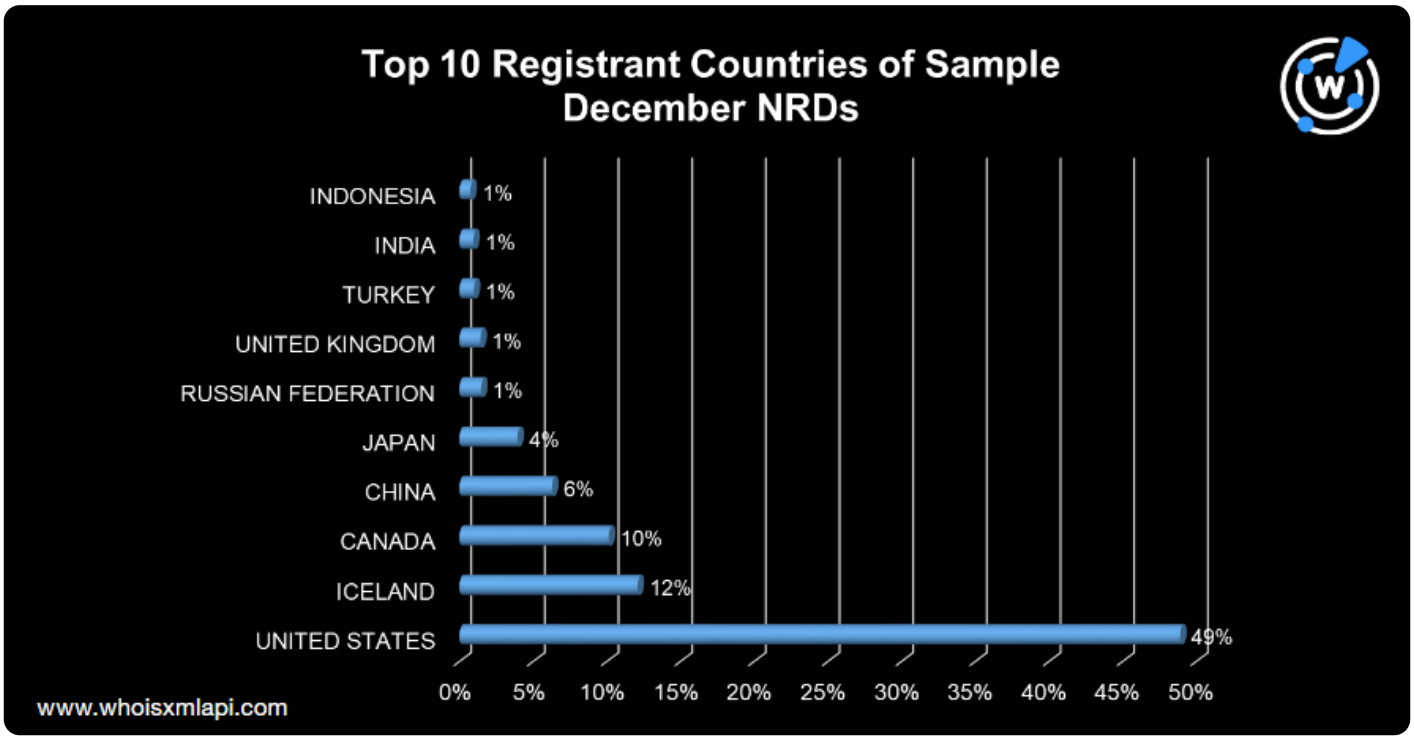
Registrar Distribution

We tallied the top registrars based on the same sample used in the previous analysis. GoDaddy accounted for a majority of the domain registrations with a 22% share. It was followed by Namecheap (13%), Google (7%), and GMO Internet (4%). The rest of the top 10 registrars and their shares are found in the chart below.



Top Registrant Countries

The domains were registered across 139 countries worldwide, but the U.S. accounted for most of the registrations. Iceland followed with a 12% share and Canada with 10%. The chart below shows the distribution of the domains across the top 10 registrant countries.



Appearance of Common Strings among the SLDs

Internationalized domain names (IDNs) continued to be popular since the most-recurring text string among our sample domains was *xn*. Generic tech terms, such as *online*, *shop*, *app*, and *web* were also common among our December NRD sample. These and other recurring strings are shown in the word cloud below.

Cybersecurity through the DNS Lens

In December, we traced the digital footprints of ransomware attack IoCs, scrutinized the persistence of money mule recruitment, and discovered thousands of typosquatting properties that could serve as vehicles for Royal Ransomware.

Below are some of the threat reports we published.

- **From Counties to Banks: Tracing the Footprint of Ransomware Attack IoCs:** Our researchers did a two-part investigation of a U.S. county attack where the Cryxos trojan was believed to be involved. The study led us to 1,400+ typosquatting properties targeting Chase Bank.

- **Why Domain Seizure May Not Stop Money Mule Recruitment Campaigns:** When we heard the news about U.S. law enforcement agencies seizing 18 domains believed to be part of money mule recruitment campaigns, we decided to expand the list of IoCs. We found

hundreds of properties related to the seized domains through registrant email addresses, unique text strings, and IP resolutions.

- **Exposing the New Potential Ways Royal Ransomware Gets Delivered:** A threat actor called “DEV-0569” has been using typosquatting domains to deploy Royal ransomware. Our researchers found 3,000+ typosquatting properties targeting the same companies impersonated by DEV-0569.

You can find more reports created in the past months here.

Please do not hesitate to contact us for more information about the domain registration events and analyses mentioned above or any inquiries about enterprise commercial solutions.