January 2023: New Domain Activity Highlights

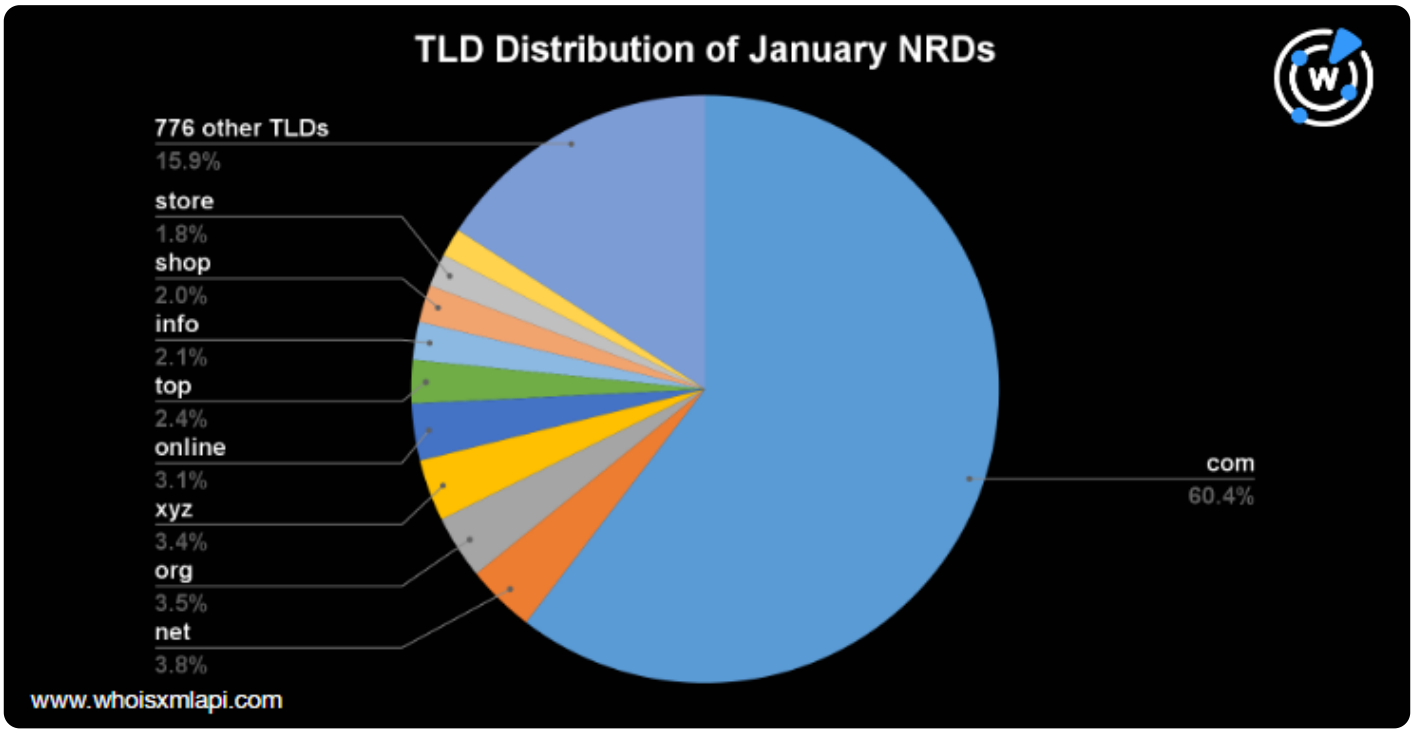
Posted on February 7, 2023

Out of millions of domains registered during 1–31 January 2023, WhoisXML API researchers analyzed a sample of 1 million domains to determine their top registrars, registrant countries, and TLD distribution. We also studied their text string usage 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 January NRDs

TLD Distribution

.com continued to amass huge domain volumes, with 60% of the January NRDs sporting the TLD. The rest of the top 10 TLDs only accounted for less than 5% each of the registration volume, but the top 10 TLDs shown in the chart below were responsible for about 84% of the registrations. The remaining 16% was distributed across 776 other TLDs.



Domain Registration Volumes for the Most-Abused TLDs

We also highlighted the domain registration volumes for some of the most-abused TLDs identified by Spamhaus on 2 February 2023. The table below shows these TLDs with their badness indexes and registration volumes for January.

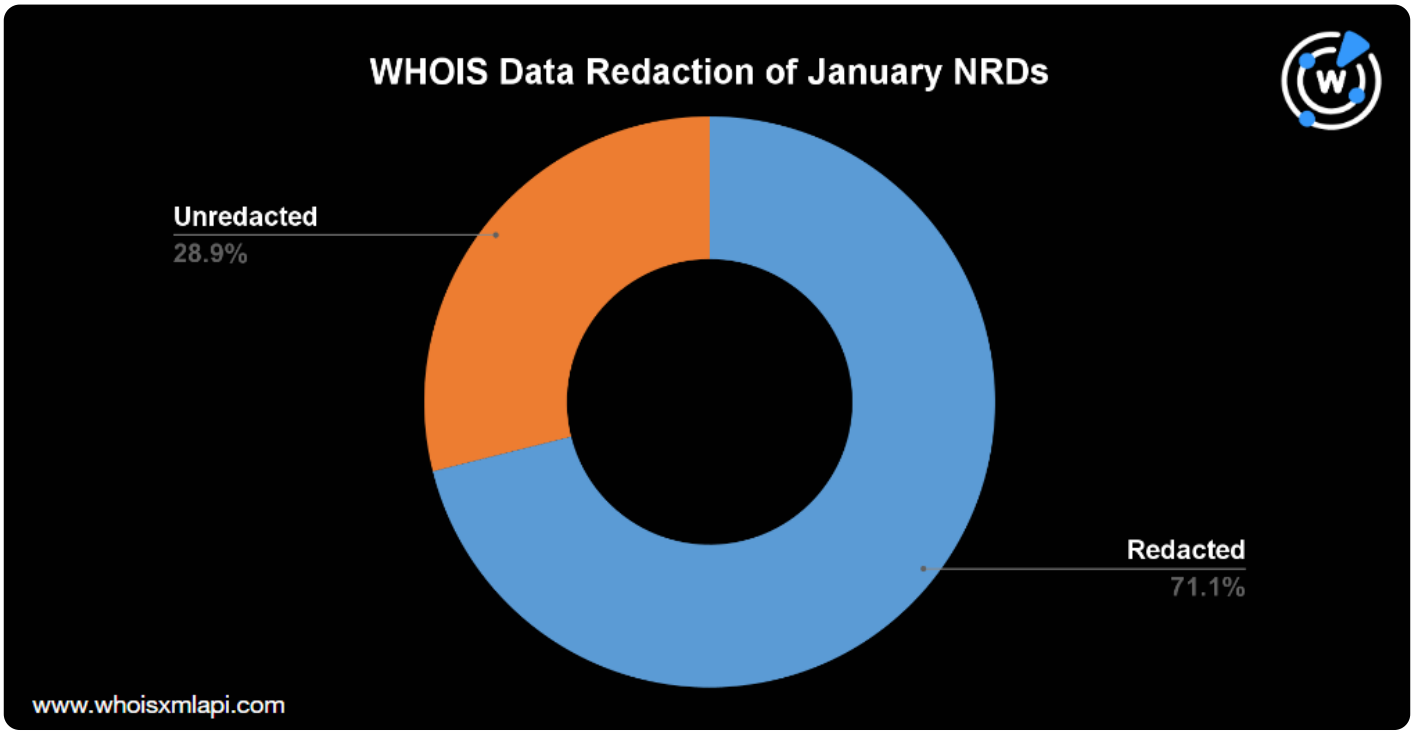
TLD	Badness Index	Domain Registration Share Against the Total January NRD Volume
.top	2.31	2.384%
.live	1.92	0.477%
.monster	1.65	0.008%
.beauty	1.98	0.002%

While the percentages may seem low, remember that there were millions of NRDs in January 2023. Therefore, the domains under these unreputable TLDs were registered by the thousands.

WHOIS Data Redaction

A majority of the NRDs had redacted WHOIS records. While some were covered by data privacy laws, most domain registrants employed the services of WHOIS privacy protection providers.

Less than one-third of the NRDs had unredacted WHOIS records, but less than that had public registrant email addresses.

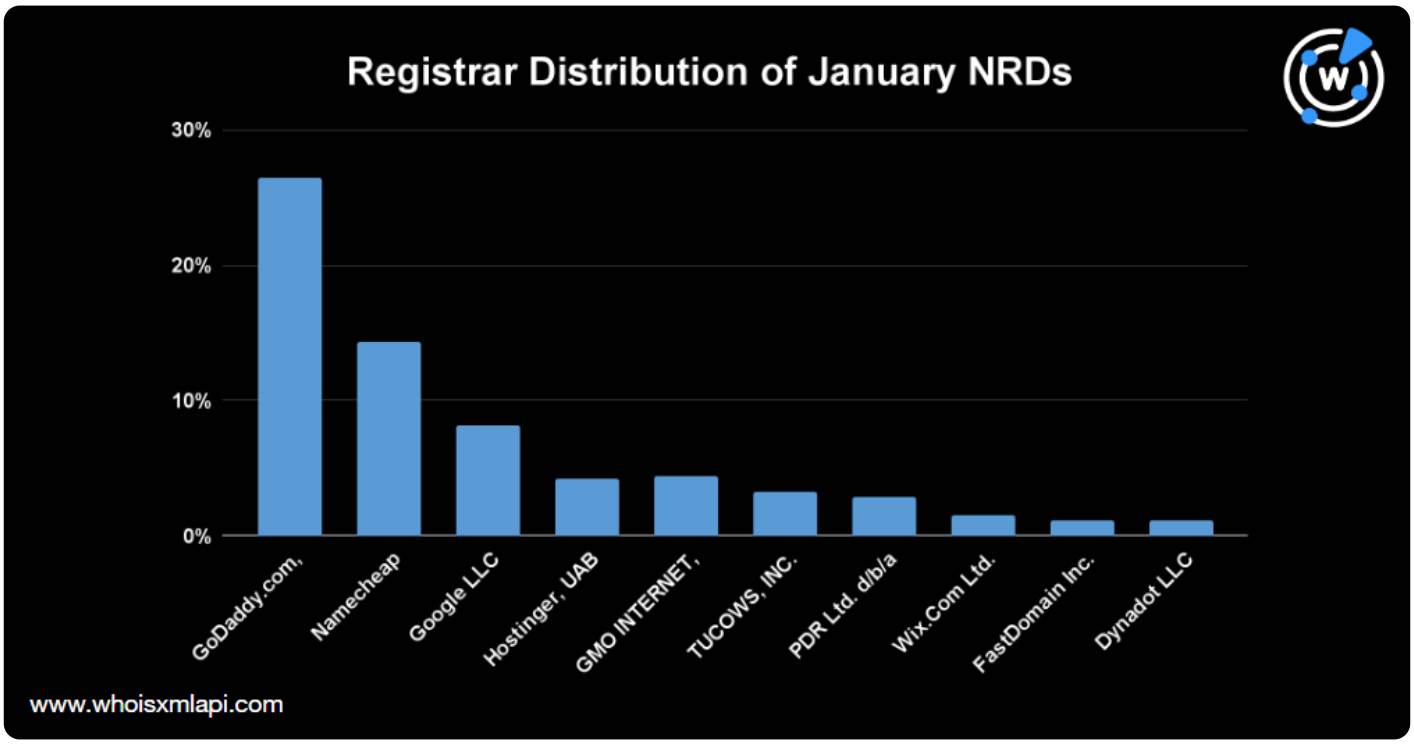


Registrar Distribution

GoDaddy took the lead as the top registrar, accounting for 26% of the domain registrations. Namecheap followed with a 14% share, Google with 8%, and Hostinger and GMO Internet with

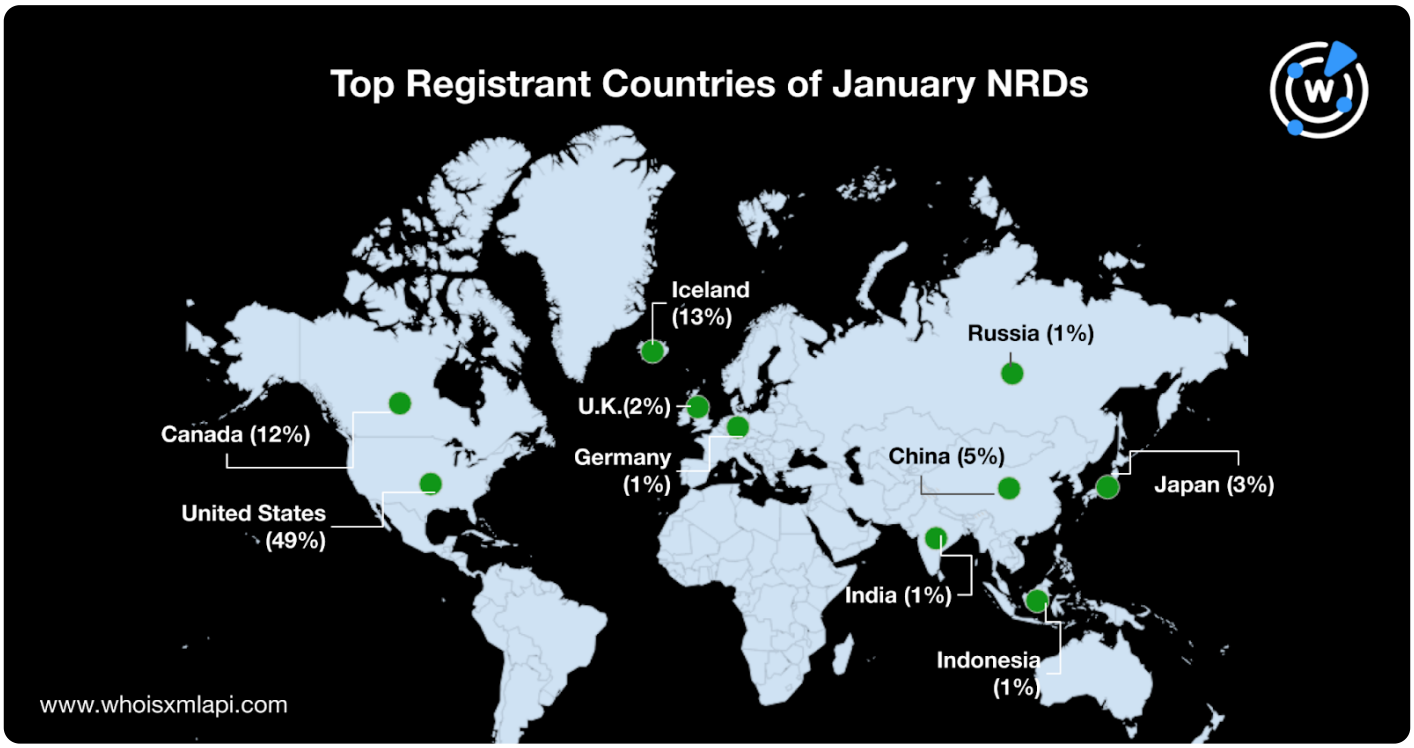
4% each. The rest of the top 10 registrars were Tucows (3%), PDR Ltd. (3%), Wix (2%), FastDomain (1%), and Dynadot (1%).

Overall, the 10 registrars were responsible for almost two-thirds of the January NRDs. The rest were distributed across 760 other registrars.



Top Registrant Countries

Half of the January NRDs were registered in the U.S., while 13% and 12% were registered in Iceland and Canada, respectively. The other top registrant countries included China, Japan, the U.K., Russia, Indonesia, Germany, and India. The map below shows these countries and their corresponding registration volumes.



About 88% of the January NRDs could be traced to the top 10 registrant countries. The remaining 12% were scattered across 138 other countries worldwide.

Appearance of Common Strings among the SLDs

Internet terms, such as ***online***, ***shop***, ***www***, and ***app***, remained common among the domains. We also saw the repeated usage of words related to emerging technologies, including ***AI*** and ***NFT***. The word cloud below reflects these and other common text strings used among the January NRDs.

Cybersecurity through the DNS Lens

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

- **Malware Persistence Versus Early Detection: AutoIT and Dridex IoC Expansion Analysis:** We looked into web properties involved in the distribution of AutoIT and Dridex malware and discovered 800+ artifacts connected to the threats via registrant email addresses, text strings, and IP hosts.

- **Sifting for Digital Breadcrumbs Related to the Latest Zoom Attack:** With Zoom repeatedly targeted in attacks, we decided to investigate the latest one that involved IceID malware-laced Zoom downloads. Our researchers found 20K+ Zoom-related cybersquatting domains, some of which were malicious.

- **Exposing Chat Apps Exploited for Supply Chain Attacks:** One of the lingering effects of

the pandemic is the popularity of chat applications. Threat actors didn't waste time exploiting this trend in supply chain attacks. We built on the list of IoCs related to this threat and we found thousands of connected domains.

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

Feel to contact us for more information about the products and capabilities used to analyze domain registration events or to support other use cases.