February 2023: New Domain Activity Highlights

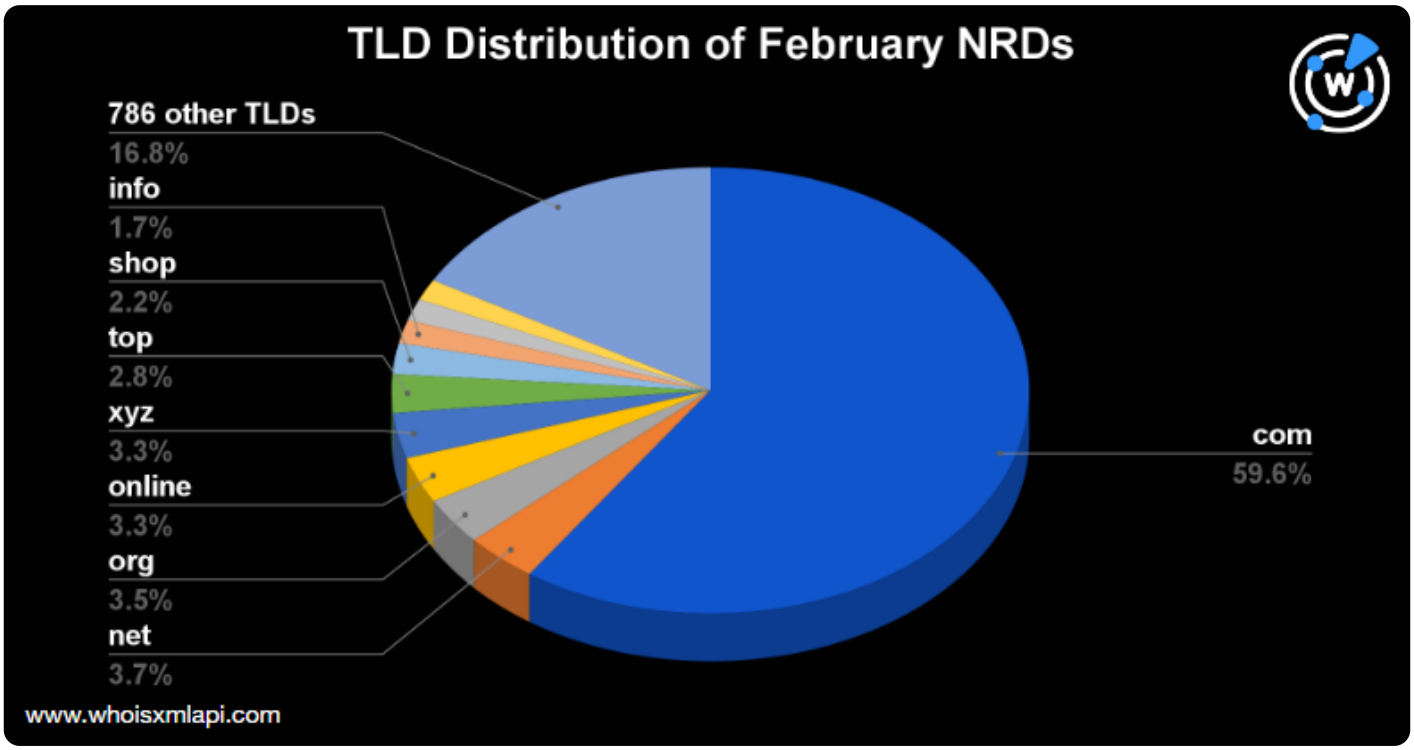
Posted on March 7, 2023

Of the millions of domains registered on 1–28 February 2023, WhoisXML API researchers analyzed a randomized sample of 28,000 domains to determine their top registrars, registrant countries, and TLD distribution. We also studied their text string usage to detect possible emerging trends. Check out our findings below, along with links to the threat reports our researchers put together using our domain, DNS, and IP intelligence sources.

Zooming in on the February NRDs

TLD Distribution

The TLD .com remained the most used, accounting for 59.6% of the domain registrations in February, followed by .net (3.7%), .org (3.5%), .online and .xyz (3.3% each), .top (2.8%), .shop (2.2%), and .info (1.7%). The rest of the domains sported 786 other TLDs. The distribution can be seen in the chart below.



Domain Registration Volumes for the Most-Abused TLDs

We also zoomed in on the domain registration volumes for the most-abused TLDs identified by Spamhaus on 3 March 2023. The table below shows these TLDs with the percentages of bad domains per TLD computed by Spamhaus and their registration volumes for February.

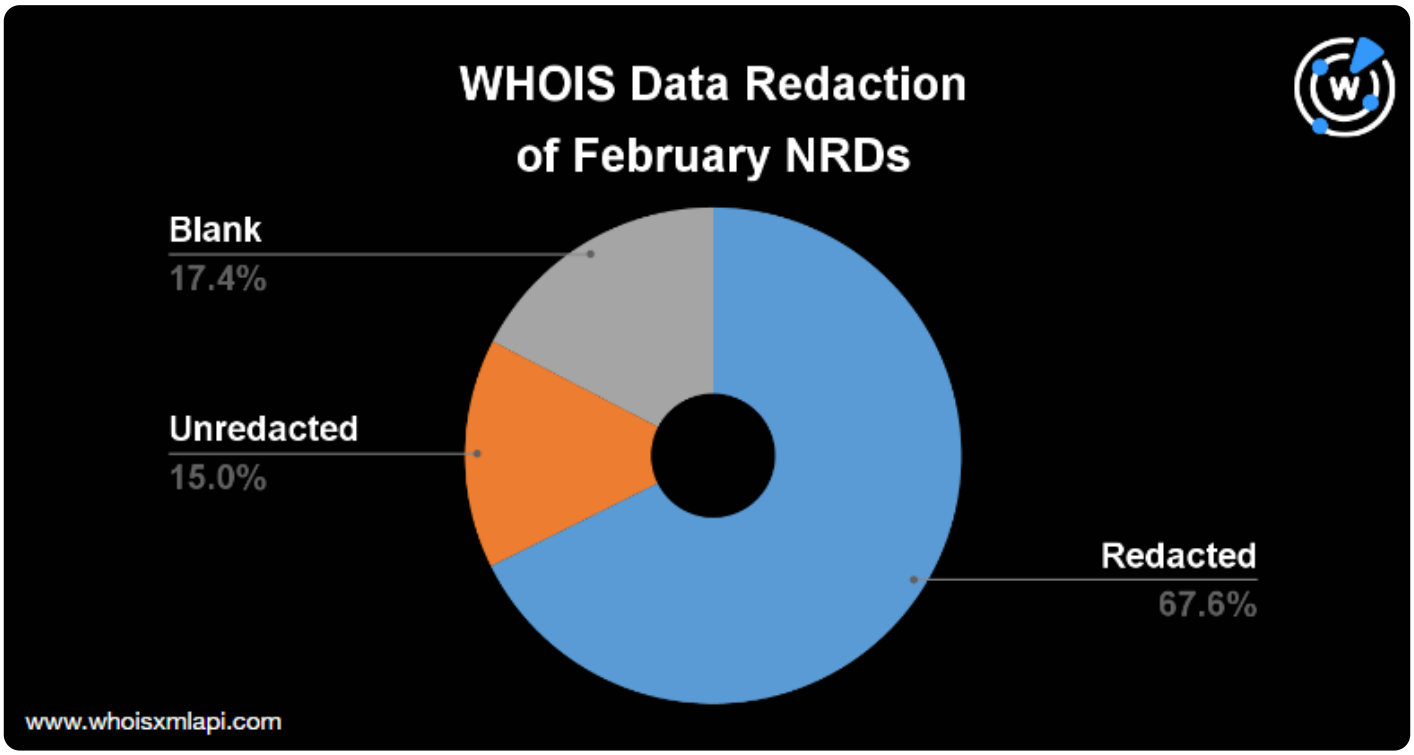
TLD	% of Bad Domains against Total Domains Seen by Spamhaus	Domain Registration Share against the Total February NRD Volume
.live	31.0%	0.542%
.beauty	25.1%	0.076%
.fyi	21.0%	0.063%

.fit	24.7%	0.029%
.zone	28.5%	0.015%
.bar	27.6%	0.012%
.rest	71.7%	0.005%
.okinawa	69.6%	0.001%

While the domain registration volumes accounted for less than 1% per TLD, they could still translate to thousands of NRDs that are likely to go bad since millions of domains were registered in February.

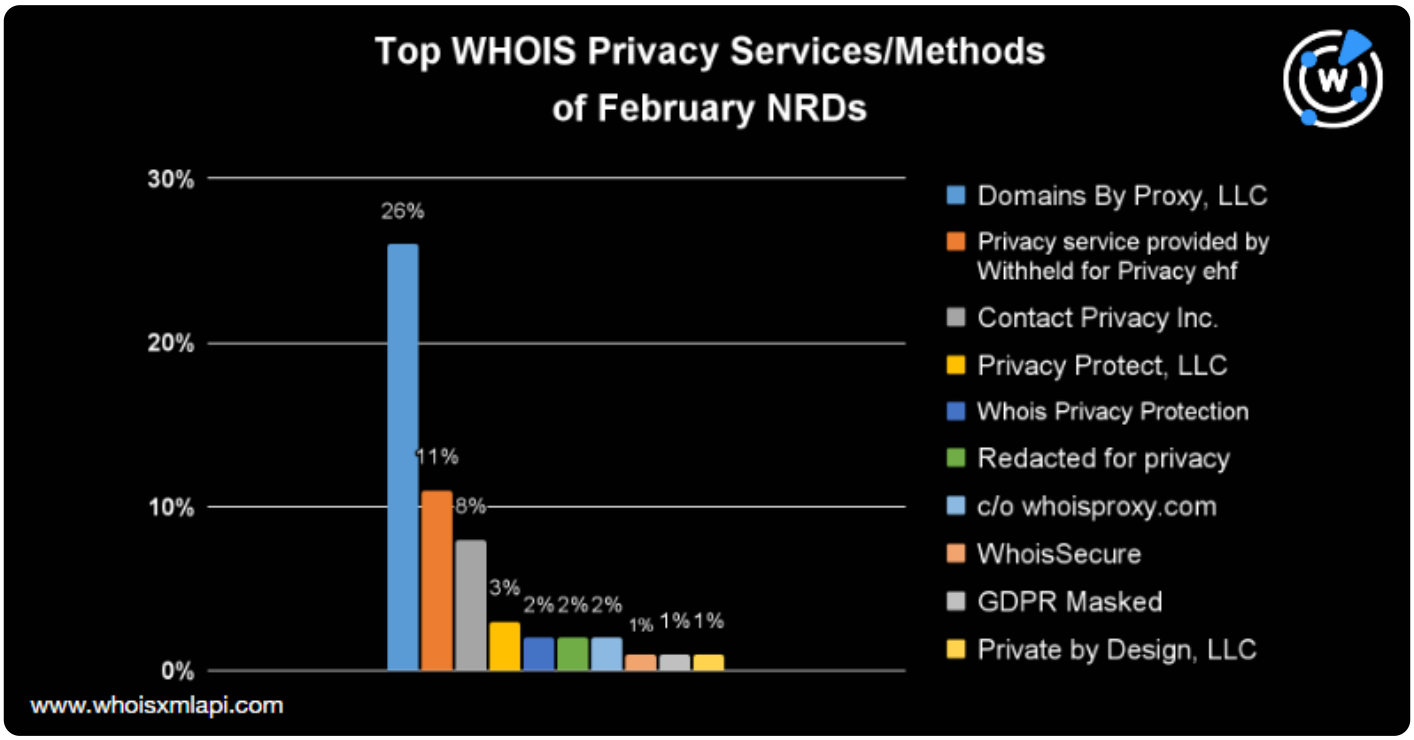
WHOIS Data Redaction

WHOIS data redaction has been massively implemented worldwide for years, and the February NRDs are no different. Only 15% of the domains had public WHOIS records, though even fewer publicized their email addresses.



About 67.6% of the domains employed the services of privacy protection companies based on their registrant organization fields. We tallied the top WHOIS privacy protection services and methods the registrants used. We discovered that Domains By Proxy, LLC was the most used, protecting the records of more than a quarter of the February NRDs.

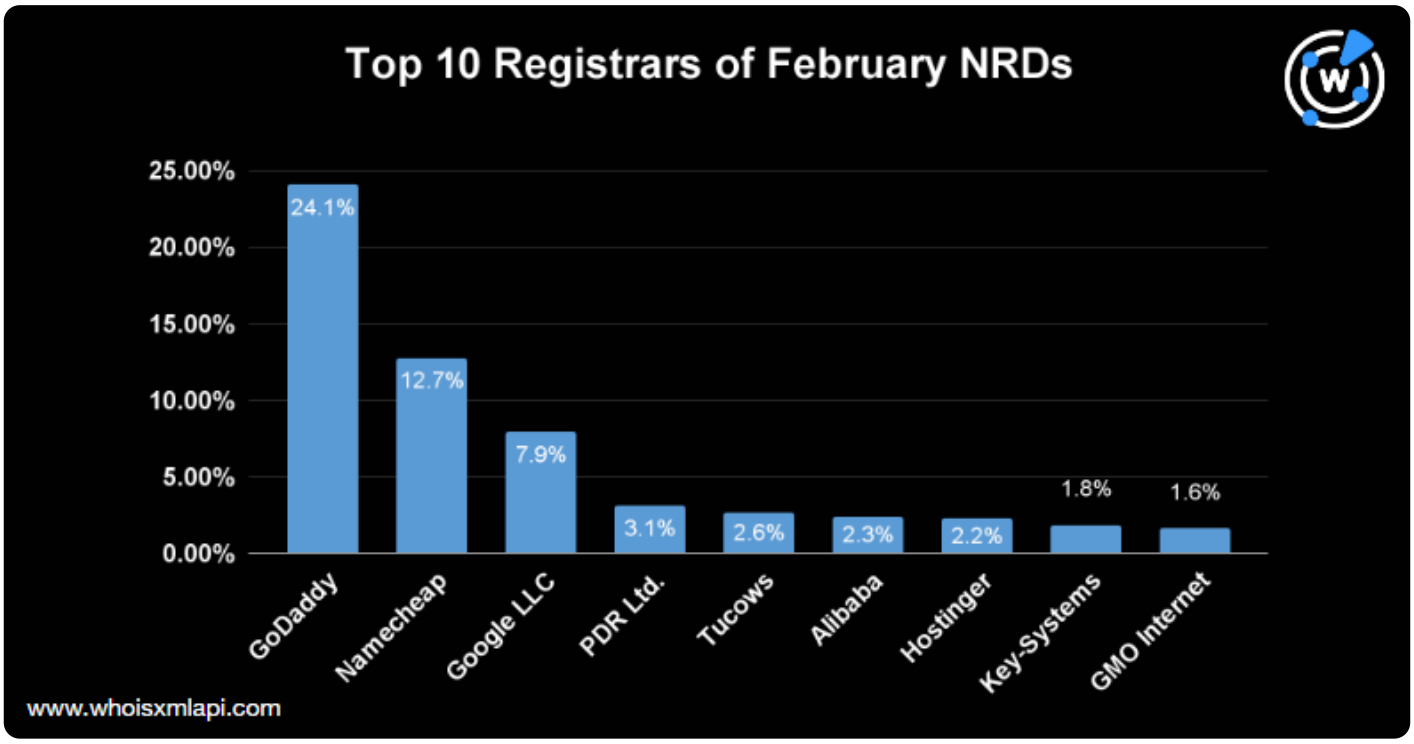
Withheld for Privacy ehf followed with an 11% share and Contact Privacy, Inc. with 8%. Other redaction methods and strings that appeared in the NRDs' registrant organization fields were Privacy Protect, LLC; Whois Privacy Protection Service by onamae.com; Redacted for privacy, c/o whoisproxy.com; WhoisSecure; GDPR Masked; and Private by Design, LLC. These are shown in the chart below.



Registrar Distribution

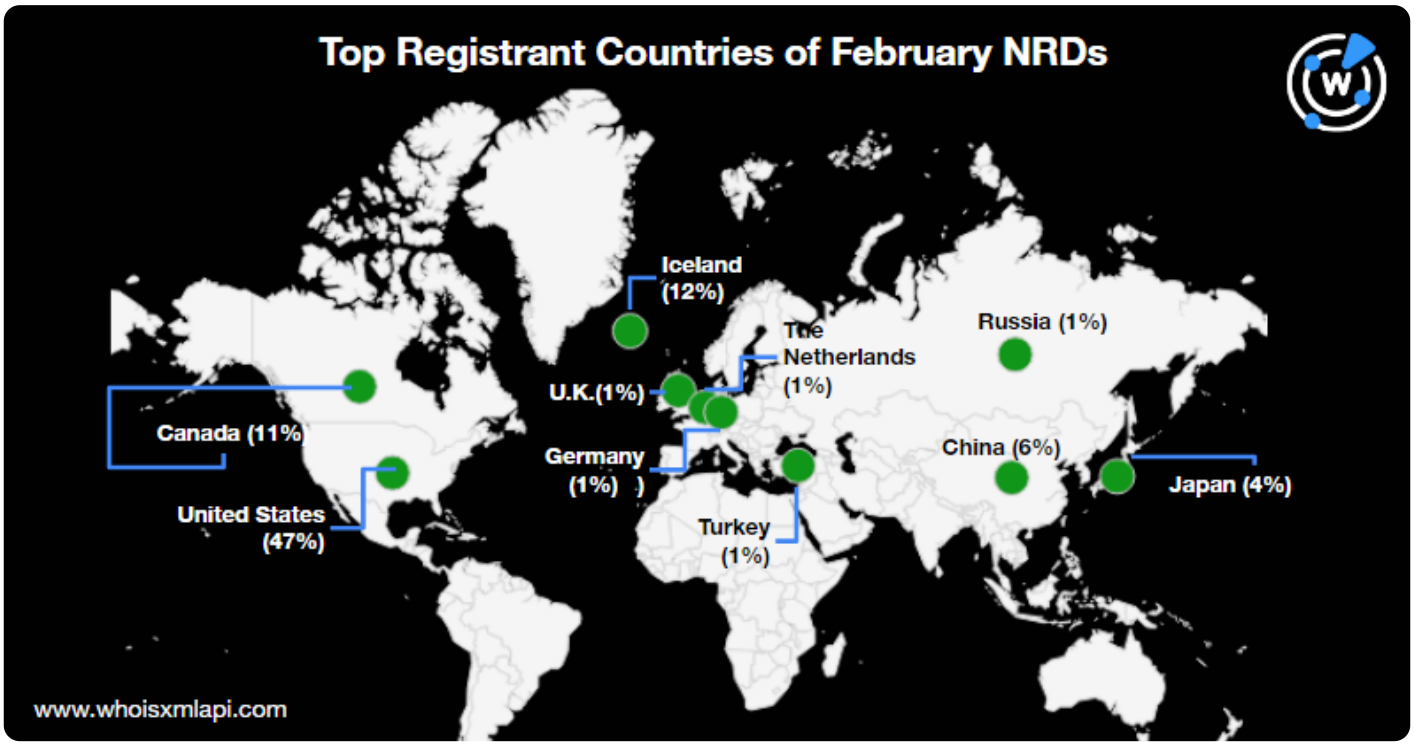
GoDaddy continued to account for most of the domain registrations with a share of about 24%. Namecheap followed with a 12.7% share, Google with 7.9%, PDR Ltd. with 3.1%, Tucows with 2.6%, Alibaba with 2.3%, Hostinger with 2.2%, Key-Systems with 1.8%, and GMO Internet with 1.6%.

Overall, the top 10 registrars were responsible for more than half of the domain registrations. The rest were distributed across 409 other registrars.



Top Registrant Countries

Almost half of the February NRDs were registered in the U.S., while 12% and 11% were registered in Iceland and Canada, respectively. The other top registrant countries included those that also appeared in the January list—China, Japan, the U.K., Russia, and Germany. However, the Netherlands and Turkey replaced Indonesia and India in February. The map below shows these countries and their corresponding registration volumes.



Appearance of Common Strings among the SLDs

Generic Internet terms remained common among the NRDs. Examples include ***online***, ***shop***, ***market***, ***info***, ***tech,*** and ***app***. We also noticed the repeated use of ***AI***.

Internationalized domain names (IDNs) continued to be popular, as reflected by the repeated usage of ***XN***. The word cloud below reflects these and other common text strings used in the February NRDs.

Cybersecurity through the DNS Lens

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

- **The Fight against Hive Ransomware May Not Be Done as Yet-Unidentified Artifacts Show:** Our researchers expanded six indicators of compromise (IoCs) used in Hive Ransomware Group activities and uncovered 950+ connected domains.
- **Expansion Analysis of a Known Cyber Jihad IoC List:** WhoisXML API threat researcher Dancho Danchev recently uncovered six email addresses connected to cyber jihadists. These IoCs led to 2,200+ email addresses and 5,551 IP addresses.
- **Catching Batloader Disguised as Legit Tools through Threat Vector Identification:** With 17 domains identified as Batloader IoCs as a starting point, we identified 5,000+ possible domain connections, several of which were confirmed malware hosts.

- **Gauging How Big a Threat Gigabud RAT Is through an IoC List Expansion Analysis:** We explored 10 Gigabud RAT IoCs and uncovered more than a thousand artifacts, hundreds of which contained organization names, such as Banco de Comercio, Advice, Thai Lion Air, Shopee Thailand, SUNAT, and Kasikornbank.

- **Tracing Connections to Rogue Software Spread through Google Search Ads:** Our researchers investigated a recent malicious campaign targeting users looking for open-source software download sites and found hundreds of artifacts based on a list of public IoCs.

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.