WhoisXMLAPI

Global Domain Activity Report

Q1 2024

Dear Reader,

I'm thrilled to unveil the latest edition of the Global Domain Activity Report that dives deep into global trends related to newly registered domains (NRDs) and verified malicious indicators of compromise (IoCs) in Q1 2024.

Staying on top of global domain registrations and emerging DNS trends is crucial for robust security in today's complex digital ecosystem.

Dive into the data, share valuable findings with your team, and together, let's tackle known and emerging cybersecurity risks.

Jonathan Zhang

CEO of WHOIS API, Inc.,
doing business as WhoisXML API

Find me on LinkedIn

Executive Summary

In Q1 2024, we detected more than 21 million NRDs, down by 32.3% from Q4 2023. This trend shows the sometimes erratic and evolving nature of domain registration.

Leveraging domain intelligence, this report unveils key domain registration trends, including the prevalence of popular gTLDs and ccTLDs among the legitimate and malicious domains.

1. **Newly Registered Domains by TLD Type**
   - Check out the breakdown of domains registered by top TLD type.
2. **New Domain Activity: gTLD Trends**
   - Uncover the most widely used gTLDs during the quarter.
3. **New Domain Activity: ccTLD Trends**
   - Discover the most widely used ccTLDs during the quarter.
4. **New Domain Activity: Most Popular Registrars**
   - Identify the most popular registrars during the quarter.

5. **Decoding Malicious Domain TLD Usage**
   - Analyze the TLD usage trends for newly found IoCs during the quarter.

6. **Analyzing the Malicious gTLD Domains**
   - Determine the prevalence of malicious gTLD domains.

7. **Analyzing the Malicious ccTLD Domains**
   - Determine the prevalence of malicious ccTLD domains.

Methodology

This quarterly report draws insights from WhoisXML API's comprehensive domain and cyber threat intelligence sources.

We began by examining the global domain activity related to Q1 2024 NRDs under the lens of our newly registered domains (NRD) solution.

Our analysis explored domain registration trends, including the use of specific TLDs and TLD types, registrar distribution, and WHOIS data redaction.

To gain further insights, we incorporated data from Threat Intelligence Data Feeds (TIDF), allowing us to scrutinize confirmed malicious IoCs that emerged between between 1 January and 31 March 2024.

Q1 2024 Findings

Newly Registered Domains by TLD Type

There has been a significant decline in the Q1 2024 new domain registrations. Compared with the previous quarter, the overall volume shrunk by roughly 32.3%. This decrease affected both gTLDs and ccTLDs although the ccTLD registration posted a steeper decline of 42.7%, while the gTLD registration decreased by only 28.7%.

The number of gTLD registrations significantly outnumbered that of ccTLDs in Q1. In fact, the gTLD registration was 3.67 times more than that of ccTLDs. Altogether, the average daily registration volume in Q1 amounted to 233,452 domains.

TLD Type	January	February	March	Q1 2024 Total	Q4 2023 Total
gTLD	5,589,751	5,148,142	5,770,968	16,508,861	23,169,691
ccTLD	1,426,045	1,502,976	1,572,765	4,501,786	7,854,883
TOTAL	**7,015,796**	**6,651,118**	**7,343,733**	**21,010,647**	**31,024,574**

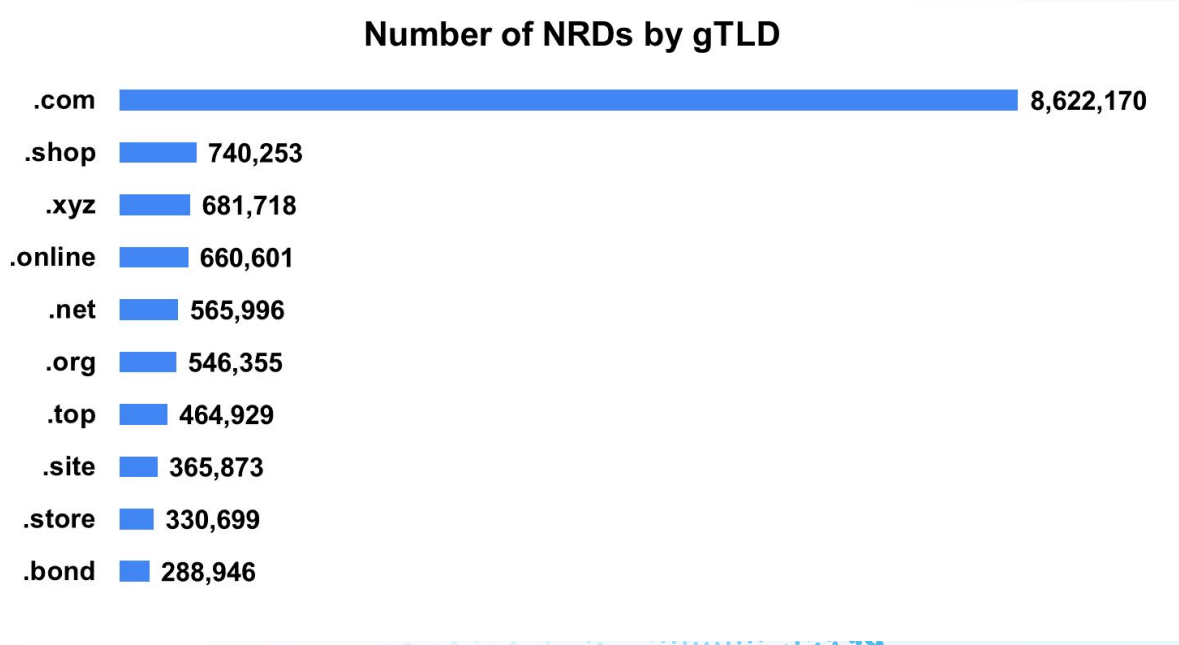
New Domain Activity: gTLD Trends

As in Q3 and Q4 2023, the number of new domain registrations under the .com gTLD in Q1 2024 was significantly higher compared to other extensions.

This ongoing trend shows individuals and organizations still preferred .com over other gTLD extensions.

The other popular gTLDs were .shop, .xyz, .online, .net, .org, .top, .site, .store, and .bond.

Data source: Newly Registered Domains

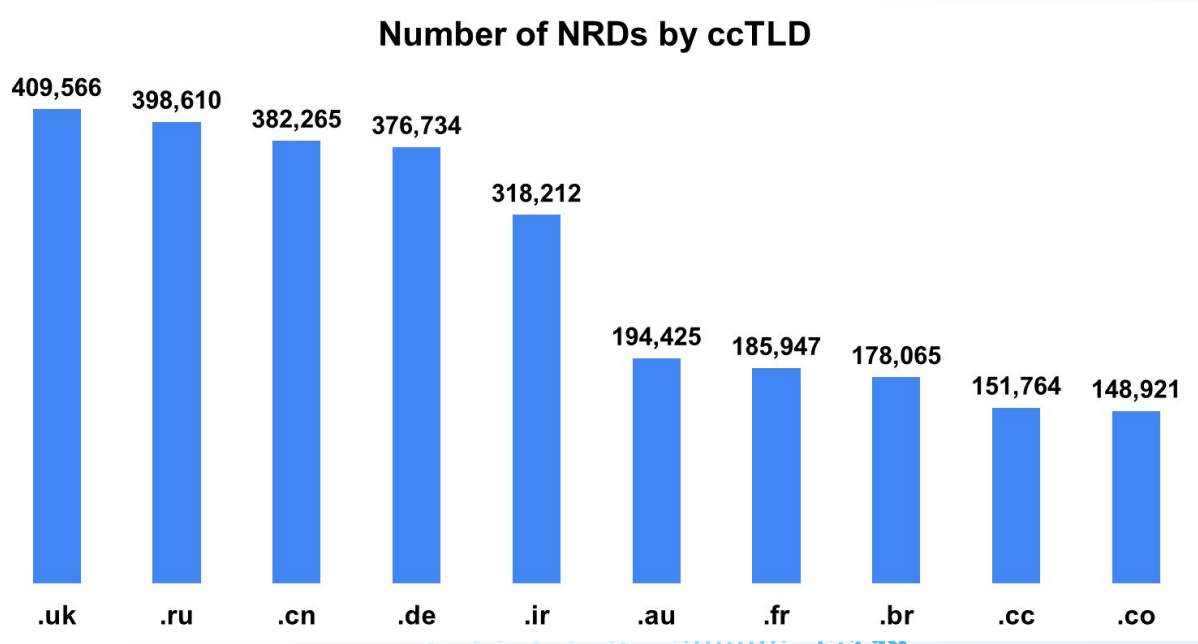


New Domain Activity: ccTLD Trends

The ccTLD extension with the highest number of new domain registrations in Q1 was .uk (U.K.) as in the previous quarter.

It was followed by .ru (Russia), .cn (China), .de (Germany), .ir (Iran), .au (Australia), .fr (France), .br (Brazil), .cc (Cocos Islands), and .co (Colombia).

Data source: Newly Registered Domains



Is the ccTLD Registration Congruent with Population Size?

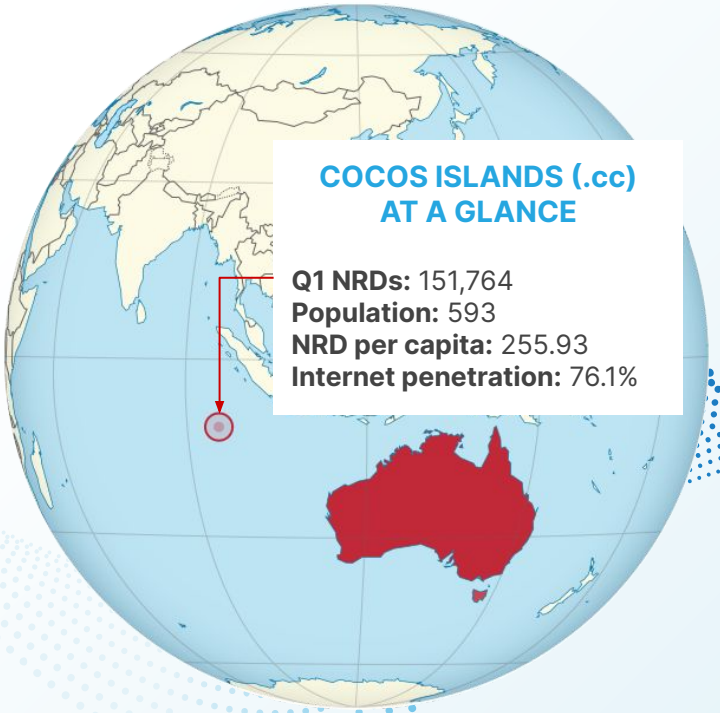
While ccTLDs are often used by local businesses, some exhibit registration patterns that raise questions. For one, do some local domains have global appeal?

Case in point for Q1? The Cocos Islands ccTLD domain activity. The extension .cc ranked ninth among 240+ ccTLDs, accounting for 151,764 or 3.27% of the total registration volume of domains sporting ccTLDs.

However, the Australian territory has less than 600 residents, translating to an enormous NRD per capita of 255.93.

We had a similar finding for Samoa (.ws) in Q4 2023 and Tokelau (.tk) in Q3 2023 that had NRD per capitas of 1.33 and 63.68, respectively.

Data source: Newly Registered Domains



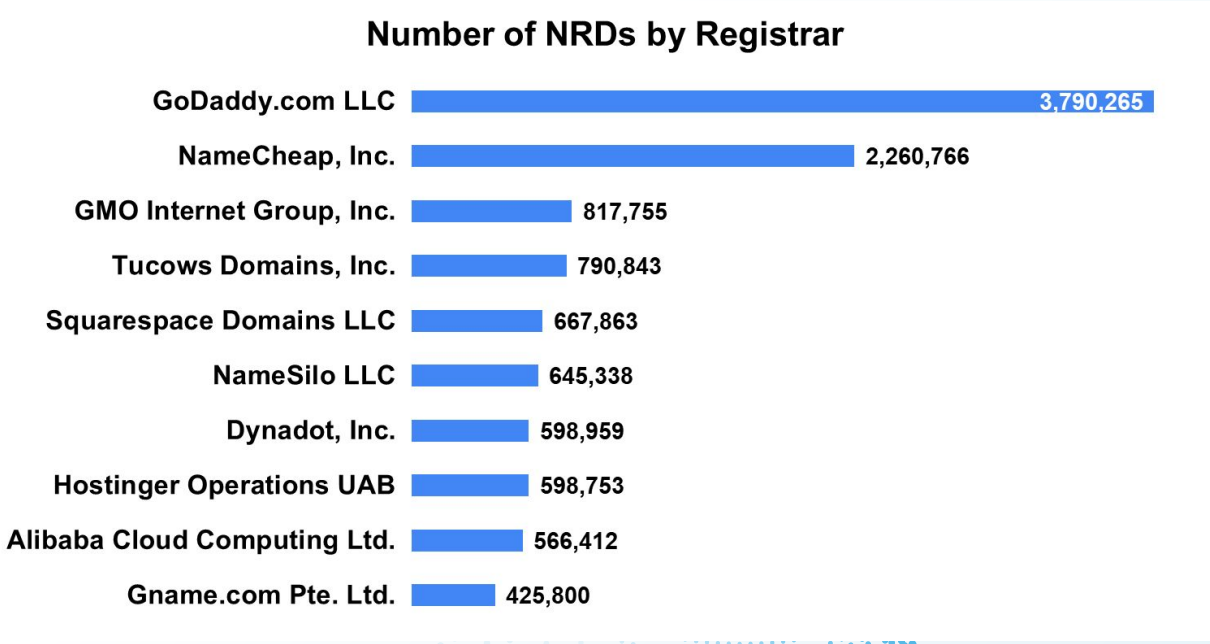
New Domain Activity: Most Popular Registrars

GoDaddy continued to be popular among the Q1 domain registrants as in the previous quarter.

Namecheap, GMO Internet Group, Tucows Domains, Squarespace Domains, NameSilo, Dynadot, Hostinger Operations, Alibaba Cloud Computing, and Gname.com completed the top 10 registrars.

Altogether, these registrars accounted for 53.13% of the total Q1 domain registration volume.

Data source: Newly Registered Domains

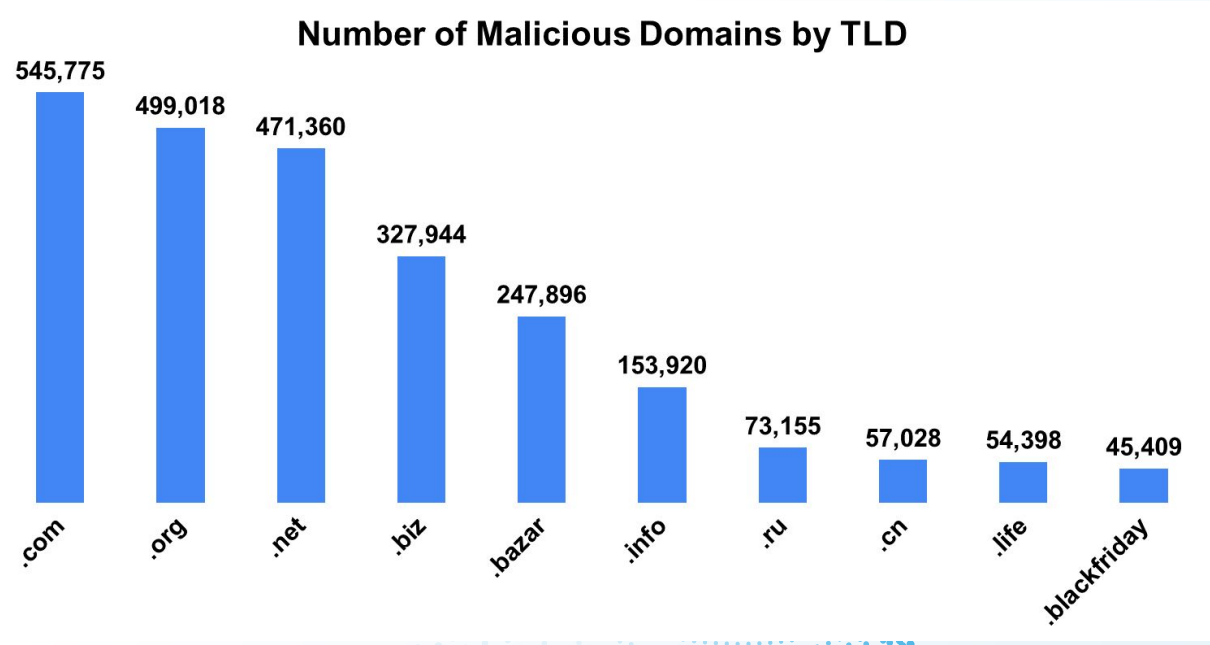


Decoding Malicious Domains TLD Usage

We then examined 3.2+ million domains tagged as IoCs for various cyber threats in Q1.

Our analysis revealed that a combination of TLDs were used for the malicious domains. The most popular gTLD extension was .com, while the most prevalent ccTLD extension was .ru.

Data source: Newly Registered Domains



Analyzing the Malicious gTLD Domains

In Q1, most of the domains tagged as IoCs sported the gTLD extensions .com, .org, .net, .biz, .info, and .life. The malicious usage of some gTLDs may be spurned by their popularity since .com, .org, and .net were among the top 10 gTLDs used for Q1 NRDs. Zooming in on .com, for instance, 500,000+ malicious domains and 8.6+ million NRDs used the extension.

However, even those that were not as popular as .com, such as .biz, .info, and .life, were also favored by malicious entities.

Data source: Threat Intelligence Data Feeds

Description	.com	.org	.net	.biz	.info	.life
New malicious domains listed in Q1	545,775	499,018	471,360	327,944	153,920	54,398
New domains added in Q1	8,622,170	546,355	565,996	53,436	256,409	70,702

Analyzing the Malicious ccTLD Domains

The domains tagged as IoCs in Q1 sported the same ccTLDs frequently seen in November and December 2023. They included some of the top 10 ccTLDs among the Q4 NRDs, namely, .ru, .cn, and .cc.

Even more interesting, a higher number of existing domains with extensions like .su, .to, .so, and .pw were used in malicious activities compared to the number of new domains registered with these extensions in Q1 2024.

Data source: Threat Intelligence Data Feeds

Description	.ru	.cn	.su	.cc	.in	.to	.so	.eu	.pw
New malicious domains listed in Q1	73,155	57,028	40,763	30,826	27,857	24,437	24,211	20,716	6,448
New domains added in Q1	398,610	382,265	6,348	151,764	147,496	714	641	124,820	6,157

Q1 2024 Wrap-Up

Wrap-Up

Our Q1 2024 Global Domain Activity Report aims to provide critical insights into domain registrations, administration, TLD usage patterns, and other evolving trends among legitimate and malicious domains.

Uncovering valuable trends that illuminate domain activities, preferences, and overall utilization can enable organizations across sectors to make informed and data-driven decisions amid the fast-changing DNS and threat landscape.

Join us in building a more secure online environment. As a leader in providing comprehensive domain, IP, DNS, and cyber threat intelligence, we are always actively seeking partnerships within the cybersecurity community.

Get in touch with us to access the data behind this report and discuss collaboration opportunities.

About WhoisXML API

WhoisXML API empowers all types of cybersecurity enterprises, including MSSPs, SOCs, Fortune 1000 organizations, government agencies, and SMBs with digital footprints. We relentlessly collect, process, and deliver the most comprehensive and readily available domain, IP, and DNS intelligence there is on the market.

To explore how our data can fortify your digital presence, visit our website or contact our sales team.

32 billion+
domains and subdomains

20 billion+
historical WHOIS records

116 billion+
DNS records

14+
years of data crawling


WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence