WhoisXMLAPI

Global Domain Activity Report

Q2 2024

Dear Reader,

Another quarter has come to an end and, as usual, I'm excited to present the latest edition of the Global Domain Activity Report.

Today's dynamic digital ecosystem demands for up-to-date intelligence and insights into emerging global DNS trends, which this report provides.

Join us as we look at global trends related to newly registered domains (NRDs), DNS activities, and verified malicious indicators of compromise (IoCs) in Q2 2024.

Feel free to use the data and share it with your team to aid in your fight against new and emerging cybersecurity threats.

Jonathan Zhang

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

Find me on LinkedIn

Executive Summary

In Q2 2024, we identified more than 21.5 million new domain registrations, representing a slight increase of 2.6% compared with Q1 2024.

Our analysis covered key domain registration trends, focusing on the prevalence of popular generic top-level domains (gTLDs) and country-code top-level domains (ccTLDs).

Additionally, we analyzed more than 3.3 million domains confirmed as malicious during the quarter and examined top mail exchange (MX) records over the past year.

Methodology

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

We began by examining the global domain activity trends related to the Q2 2024 newly registered domains (NRDs) under the lens of our NRD solution.

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

We then examined the DNS activity trends for the past 365 days using our passive DNS database file dated 2 May 2024, zooming in on the top MX fully qualified domain names (FQDNs) and the MX resolution domains.

The analysis was enriched with domain registration data gleaned from WHOIS API.

Finally, to gain insights into known threats, we gleaned data from Threat Intelligence Data Feeds (TIDF) and scrutinized confirmed malicious indicators of compromise (IoCs) that emerged between between 1 April and 30 June 2024.

Q2 2024 Findings

Newly Registered Domains by TLD Type

The domain registrations slightly rose in Q2 2024 compared with Q1, specifically a 1.4% increase in the number of NRDs sporting gTLDs and 6.6% for ccTLDs.

As in the previous quarters, the number of gTLD registrations significantly outnumbered that of ccTLD registrations in Q2. The number of gTLD registrations was, in fact, 3.43 times higher. All in all, the average daily registration volume also increased from 233,452 domains in Q1 to 239,439 in Q2.

TLD Type	April	May	June	Q2 2024 Total	Q1 2024 Total
gTLD	5,142,117	5,699,844	5,842,445	16,684,406	16,448,497
ccTLD	1,465,904	1,735,144	1,664,055	4,865,103	4,562,150
TOTAL	**6,608,021**	**7,434,988**	**7,506,500**	**21,549,509**	**21,010,647**

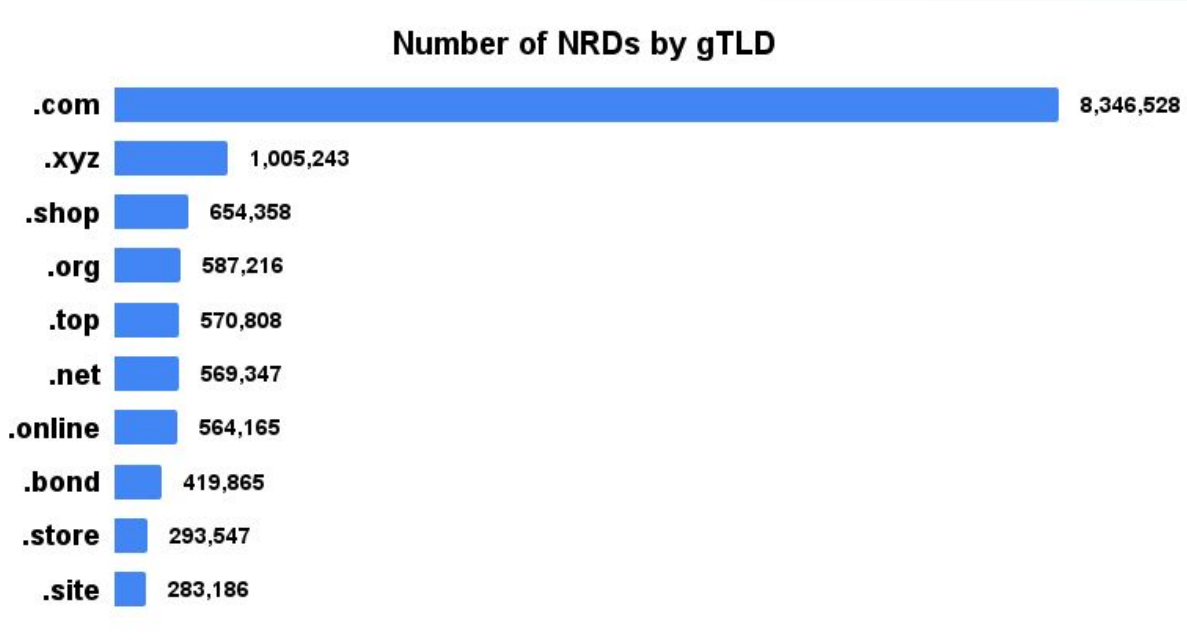
New Domain Activity: gTLD Trends

The volume of NRDs under the .com gTLD in Q2 2024 was significantly higher compared with other extensions.

This trend was the same as in the previous quarters, showing that individuals and organizations continued to prefer .com over other gTLDs.

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

Data source: Newly Registered Domains

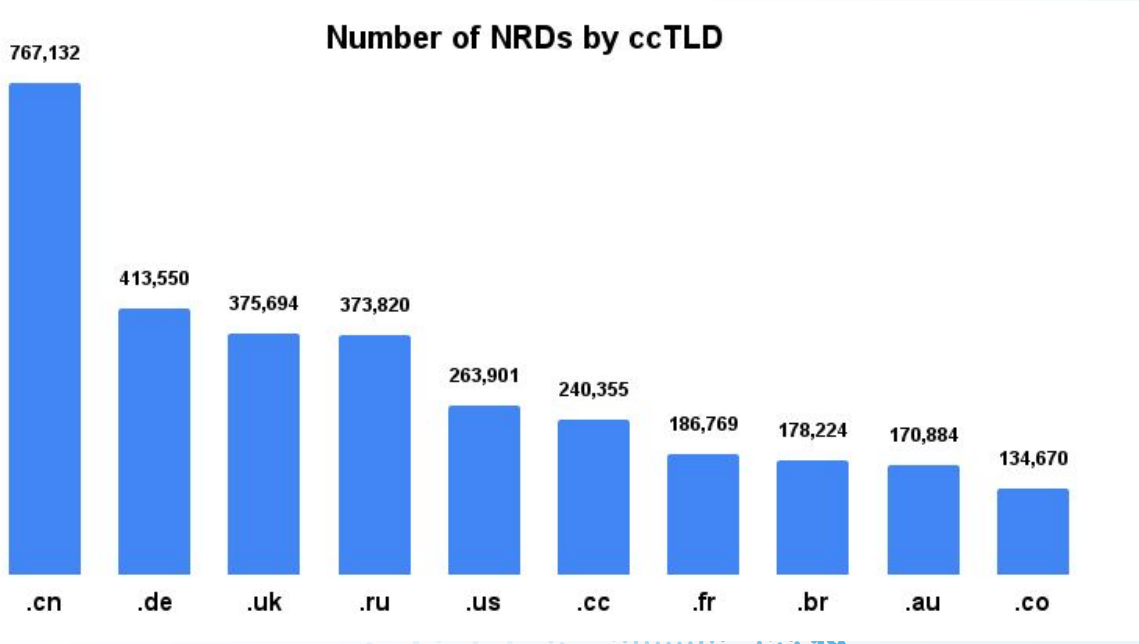


New Domain Activity: ccTLD Trends

In Q1, .uk (U.K.) was the most popular ccTLD extension, but it was replaced by .cn (China) in Q2. The .uk ccTLD only had the third highest number of new domain registrations.

The other ccTLDs with high new domain registration numbers were .de (Germany), .ru (Russia), .us (U.S.), .cc (Cocos Islands), .fr (France), .br (Brazil), .au (Australia), and .co (Colombia).

Data source: Newly Registered Domains



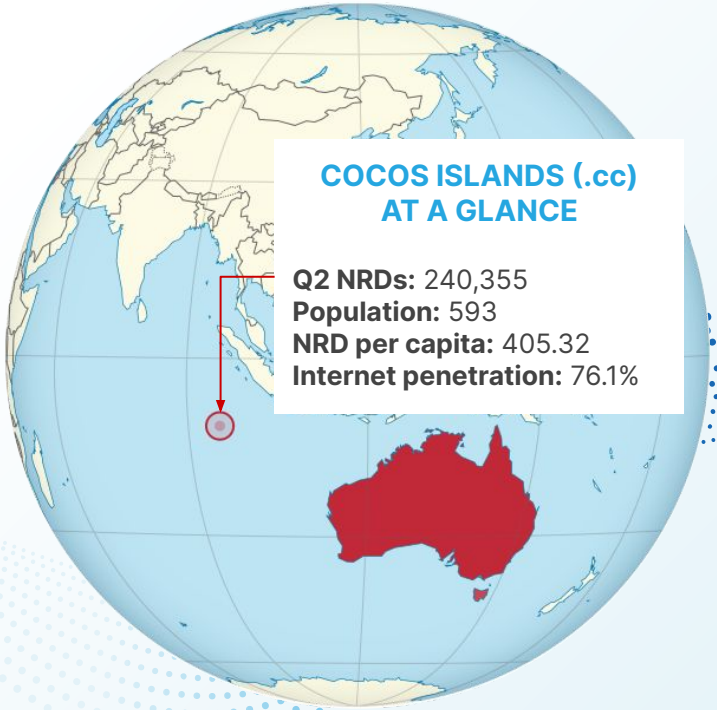
Are All ccTLD Registrations Congruent with Their Corresponding Countries' Population Sizes?

In the previous quarters, we found ccTLDs with somewhat irregular registration patterns. In Q3 and Q4 2023, for instance, Tokelau (.tk) and Samoa (.ws) had more NRDs than their corresponding countries' residents.

We had a similar finding for the Cocos Islands' .cc in Q1 2024. The extension had 151,764 new domains despite having only 593 residents.

In Q2, .cc remained in the spotlight with 240,355 or 4.94% of the total number of domain registrations sporting ccTLDs. That translated to an NRD per capita of 405.32.

Data source: Newly Registered Domains

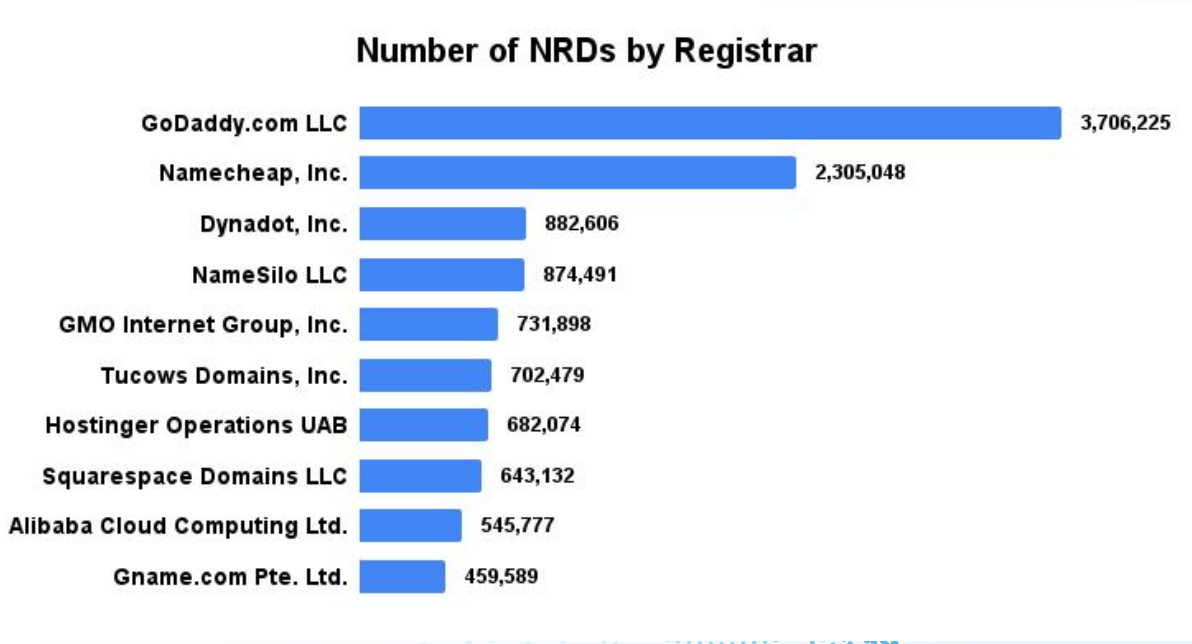


New Domain Activity: Most Popular Registrars

As in the previous quarters, GoDaddy continued to be the most popular registrar in Q2, along with Namecheap, Inc.; Dynadot, Inc.; NameSilo LLC; GMO Internet Group, Inc.; Tucows Domains, Inc.; Hostinger Operations UAB; Squarespace Domains LLC; Alibaba Cloud Computing Ltd.; and Gname.com Pte. Ltd.

These registrars accounted for 54.89% of the total Q2 domain registration volume.

Data source: Newly Registered Domains



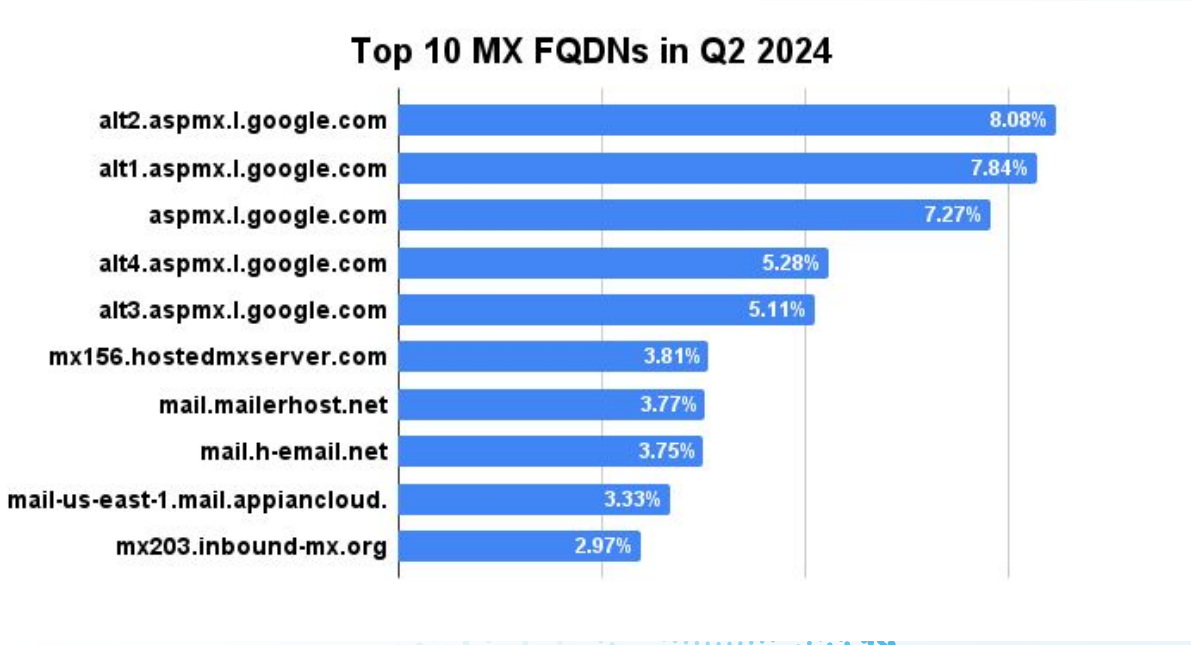
DNS Activity: Most Popular Mail Servers

We then examined the top 100 MX FQDN records, which represented the exact MX values or mail servers appearing in 630+ million MX records.

This data was collected from a passive DNS database file dated 2 May 2024 and includes MX records from the 365 days leading up to that date.

The 10 most used MX FQDNs accounted for 51.22% of the top 100.

Data source: DNS Database Download

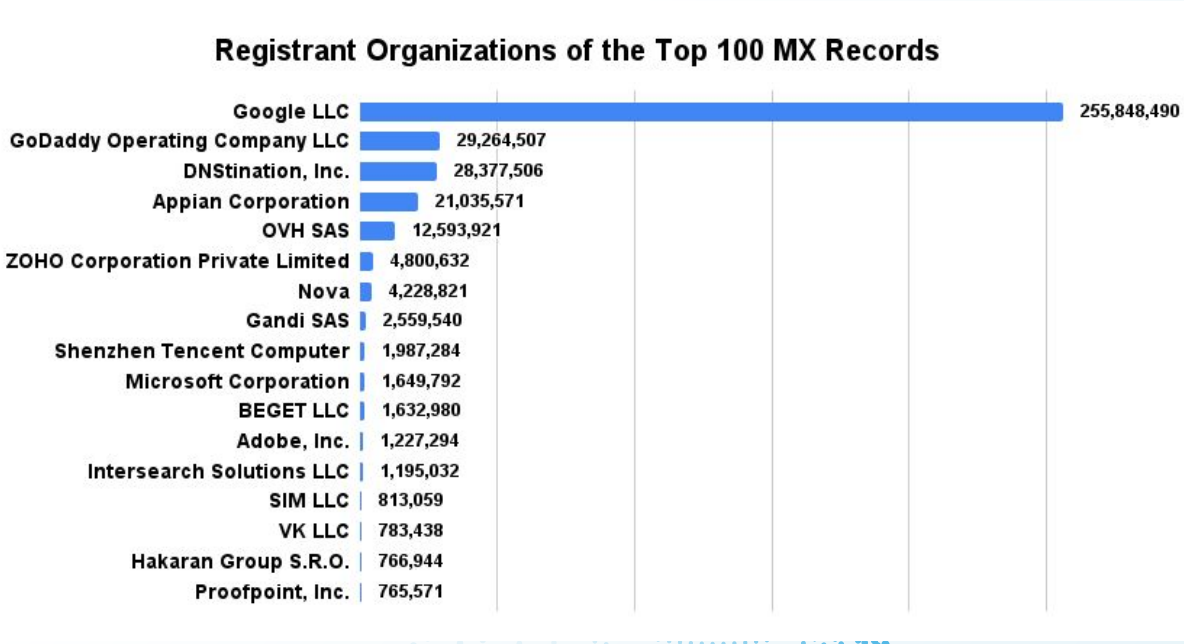


DNS Activity: Top Mail Server Providers

Running WHOIS lookups on the MX FQDNs revealed that Google LLC was the registrant organization of 15 of the most used MX FQDNs. The company accounted for 40.55% of the MX resolutions.

It's also important to note that 41.43% of the MX resolutions could not be attributed to any provider since their WHOIS records were privacy-protected.

Data sources: WHOIS API, DNS Database Download

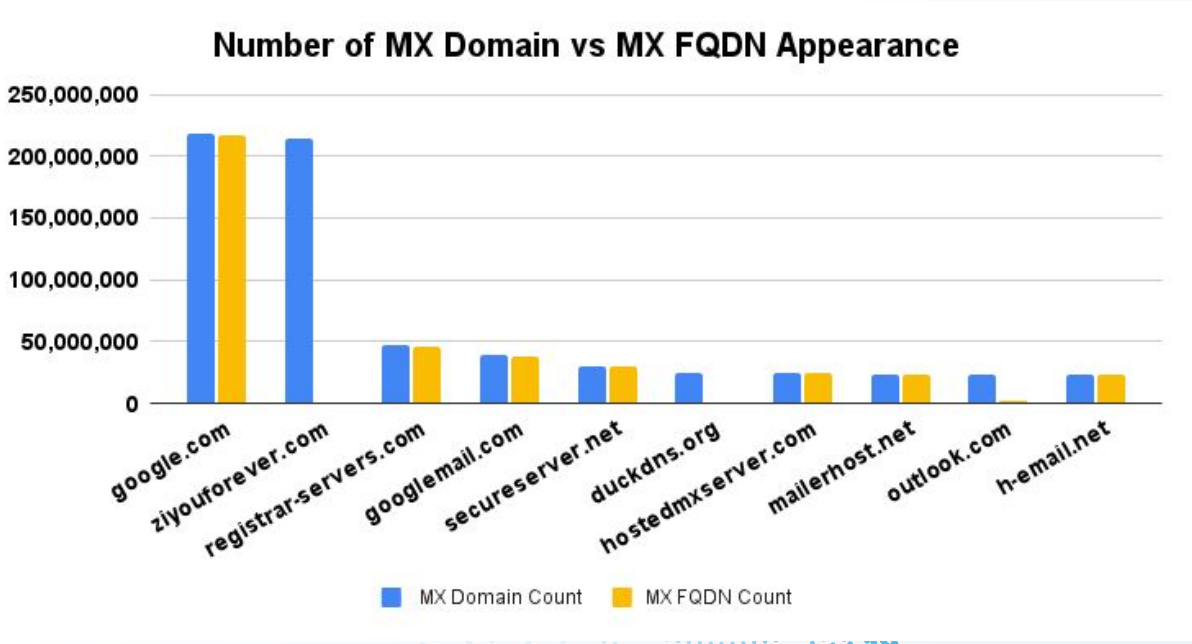


Disparity between Root Domain Use and FQDN Prevalence

Aside from obtaining the top MX FQDNs, we also gathered the top root domains from the MX records we analyzed.

An interesting finding is that although ziyouforever[.]com and duckdns[.]org were among the top 10 MX root domains, none of their FQDNs made it to the top 100.

Data sources: DNS Database Download



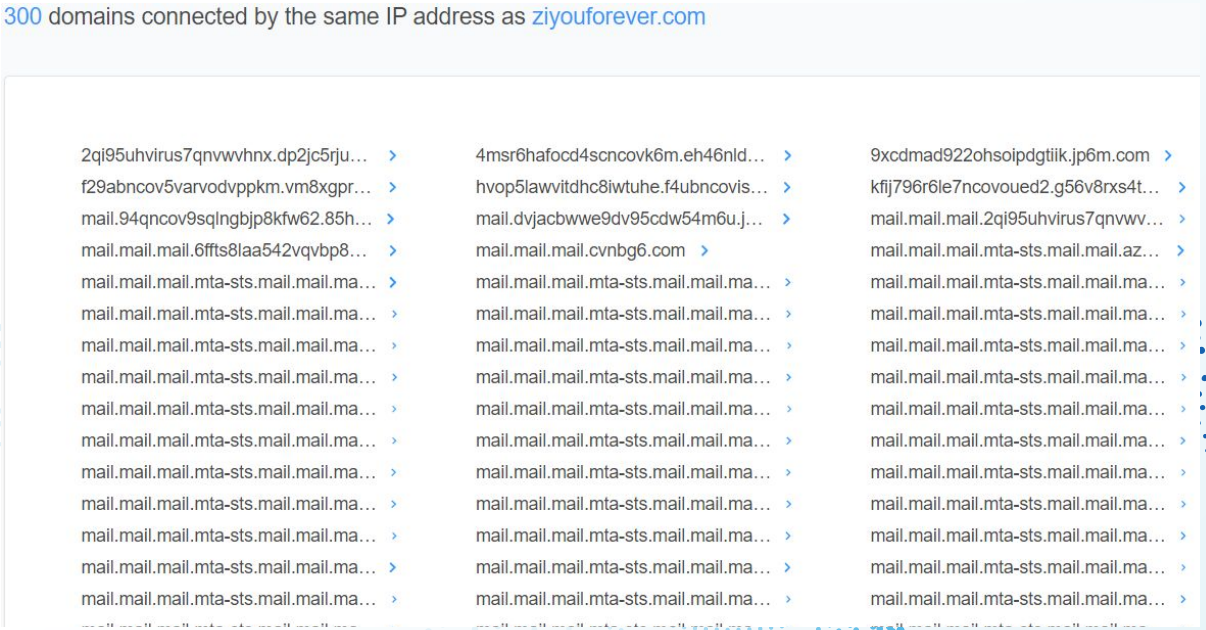
Is the Second Most Used MX Domain Tied to DNS Tunneling?

A quick research on ziyouforever[.]com uncovered [past reports] saying it could be part of a network that provides DNS tunneling services, particularly to people living in countries where Internet access is restricted.

Whether this finding remains true today, it is worth noting that the domain shares the same IP address as hundreds of subdomains containing the string **mail**.

The domain appeared in 213,545,502 or 21.53% of the Q2 2024 MX resolutions we analyzed.

Data sources: Domain Research Suite, DNS Database Download



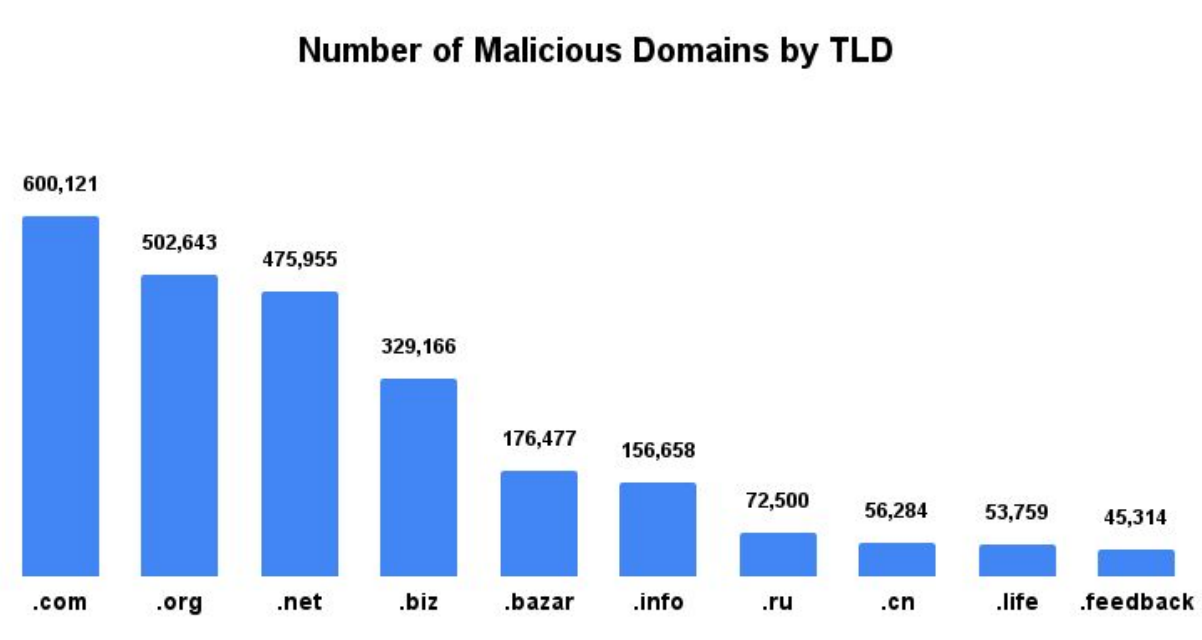
Decoding Malicious Domain TLD Usage

Next, we analyzed 3.3+ million domains tagged as IoCs for various cyber threats in Q2.

While several of the TLDs were used for the malicious domains, the most prevalent gTLD extension was .com.

On the other hand, the most popular ccTLD was .ru. These TLDs were the same as in Q1.

Data source: Threat Intelligence Data Feeds



Analyzing the Malicious gTLD Domains

Most of the domains tagged as IoCs in Q2 used .com, .org, .net, .biz, .info, and .life as gTLD extensions. Some of these extensions were also among the top 10 gTLDs of the Q2 NRDs, so their popularity could have influenced their malicious usage. For example, 8.3+ million NRDs and more than 600,000 new malicious domains used .com.

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

Data source: Threat Intelligence Data Feeds

Description	.com	.org	.net	.biz	.info	.life
New malicious domains listed in Q2	600,121	502,643	475,955	329,166	156,658	53,759
New domains added in Q2	8,346,528	587,216	569,347	57,914	261,431	83,219

Analyzing the Malicious ccTLD Domains

The most used ccTLDs of domains tagged as IoCs in Q2 were the same extensions frequently seen in Q4 2023 and Q1 2024 IoCs. They included some of the top 10 ccTLDs among the Q2 NRDs, namely, .ru, .cn, and .cc.

As in the previous quarter, extensions like .su, .so, and .to had more domains used in malicious activities compared with the number of new domains registered with these extensions in Q2 2024. This trend could be attributed to threat actors using older domains in their malicious campaigns.

Data source: Threat Intelligence Data Feeds

Description	.ru	.cn	.su	.cc	.in	.so	.to	.eu
New malicious domains listed in Q2	72,500	56,284	39,470	30,746	27,490	24,425	24,309	14,245
New domains added in Q2	373,820	767,132	3,726	240,355	134,374	564	11	103,432

Q2 2024 Wrap-Up

Wrap-Up

The Q2 2024 Global Domain Activity Report provides critical insights into domain registration patterns, DNS MX activity trends, and the TLD usage of malicious domains.

Analyzing these patterns can reveal the preferences and behaviors of both legitimate and malicious entities, enabling organizations to make data-driven decisions and security teams to stay ahead of ever-evolving threats.

Our market-leading domain, IP, DNS, and cyber threat intelligence sources enable us to provide these deep insights. We're actively seeking partnerships within the cybersecurity community to share this intelligence and collaborate on developing innovative solutions to combat cyber threats.

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 capabilities, visit our website or contact our sales team.

50 billion+
domains and subdomains

21 billion+
historical WHOIS records

116 billion+
DNS records

14+
years of data crawling


WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence