



Global Domain Activity Report

Q1 2025

“

Dear Reader,

Another quarter has passed and, as always, I'm excited to present the latest edition of the Global Domain Activity Report.

The ever-evolving security landscape demands 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 indicators of compromise (IoCs) in Q1 2025.

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 Q1 2025, we identified 23.4+ million new domain registrations, down from 24.4+ million in Q4 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).

We also analyzed 2.1+ million domains tagged as IoCs during the quarter and examined the top TLDs of the domains found in the associated mail exchange (MX) and name server (NS) records over the past year.

1. [Newly Registered Domains by TLD Type](#)
2. [New Domain Activity: gTLD Trends](#)
3. [New Domain Activity: ccTLD Trends](#)
4. [.cc ccTLD Still Sports NRD Volume-Population Size Incongruence](#)
5. [New Domain Activity: Most Popular Registrars](#)
6. [DNS Activity: Most Popular Mail Servers](#)
7. [DNS Activity: Top Mail Server Providers](#)
8. [DNS Activity: Most Popular MX FQDNs](#)
9. [DNS Activity: Most Popular Name Servers](#)
10. [DNS Activity: Top Name Server Providers](#)
11. [DNS Activity: Most Popular NS FQDNs](#)
12. [Decoding Malicious Domain TLD Usage Trends](#)
13. [Analyzing the Malicious gTLD Domains](#)
14. [Analyzing the Malicious ccTLD Domains](#)



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 Q1 2025 NRDs under the lens of our [Newly Registered Domains \(NRD2\)](#) 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 [DNS Database Download](#) files for March 2025, zooming in on the top MX and NS domains and their respective registrant organizations. The analysis was enriched with domain registration data gleaned from [WHOIS API](#). We also looked at the top MX and NS fully qualified domain names (FQDNs).

Finally, to gain insights into known threats, we obtained data from [Threat Intelligence Data Feeds \(TIDF\)](#) and scrutinized those that have been confirmed as IoCs between 1 January and 31 March 2025.

Q1 2025 Findings

The background features a solid blue color. Overlaid on this are several wavy, horizontal lines composed of small, dark blue dots. These lines create a sense of motion and depth, with some lines appearing more prominent than others, creating a layered effect.



Newly Registered Domains by TLD Type

The new domain registrations decreased from 24.4+ million in Q4 2024 to 23.4+ million in Q1 2025. The number of NRDs sporting gTLDs fell by 1.1% while those sporting ccTLDs decreased by 11.8%.

As in previous quarters, the number of gTLD registrations was significantly higher than the ccTLD registrations in Q1. The number of gTLD registrations was, in fact, 3.3 times higher. Overall, the average daily registration volume also fell from 265,231 in Q4 2024 to 260,686 in Q1 2025.

TLD Type	January	February	March	Q1 2025 Total	Q4 2024 Total
gTLD	5,907,702	5,678,830	6,414,671	18,001,203	18,206,674
ccTLD	1,751,809	1,907,971	1,800,731	5,460,511	6,194,562
TOTAL	7,659,511	7,586,801	8,215,402	23,461,714	24,401,236



New Domain Activity: gTLD Trends

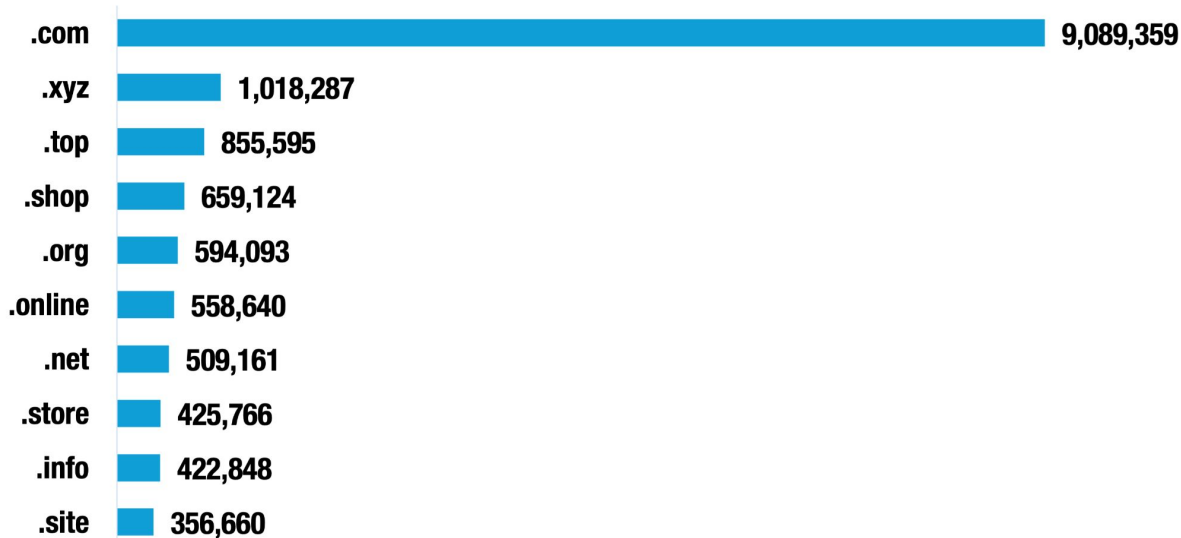
The volume of NRDs under the .com gTLD in Q1 2025 remained significantly higher compared with other extensions at 9.0+ million.

This trend continued from previous quarters, showing that individuals and organizations continued to prefer .com over other gTLDs.

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

Data source: [Newly Registered Domains](#)

NUMBER OF NRDs BY gTLD





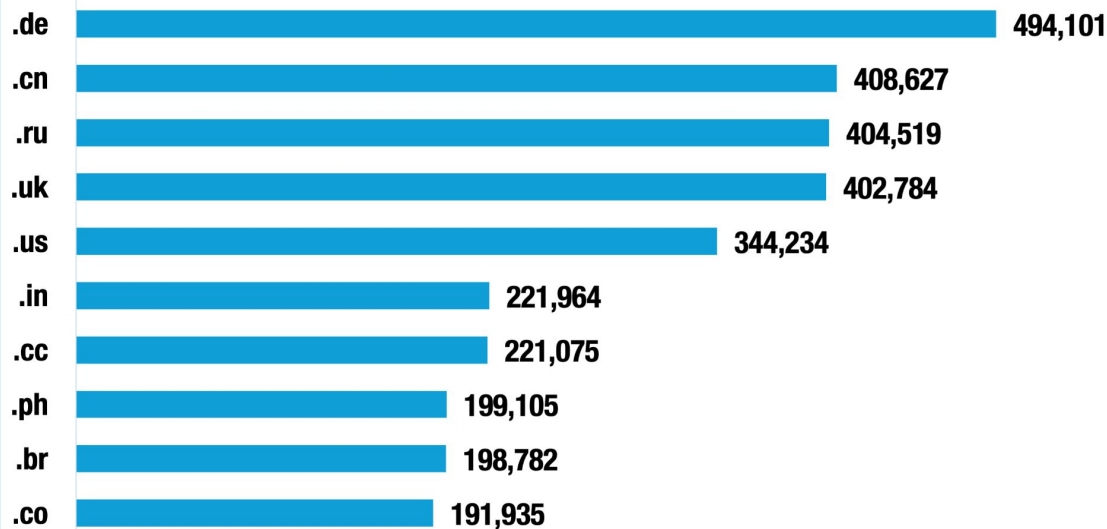
New Domain Activity: ccTLD Trends

The ccTLD extension .de (Germany) topped last quarter's topnotcher .cn (China). The .cn extension dropped to second place, followed by .ru (Russia).

The other ccTLDs with high new domain registration numbers were .uk (U.K.), .us (U.S.), .in (India), .cc (Cocos [Keeling] Islands), .ph (Philippines), .br (Brazil), and .co (Colombia).

Data source: [Newly Registered Domains](#)

NUMBER OF NRDs BY ccTLD





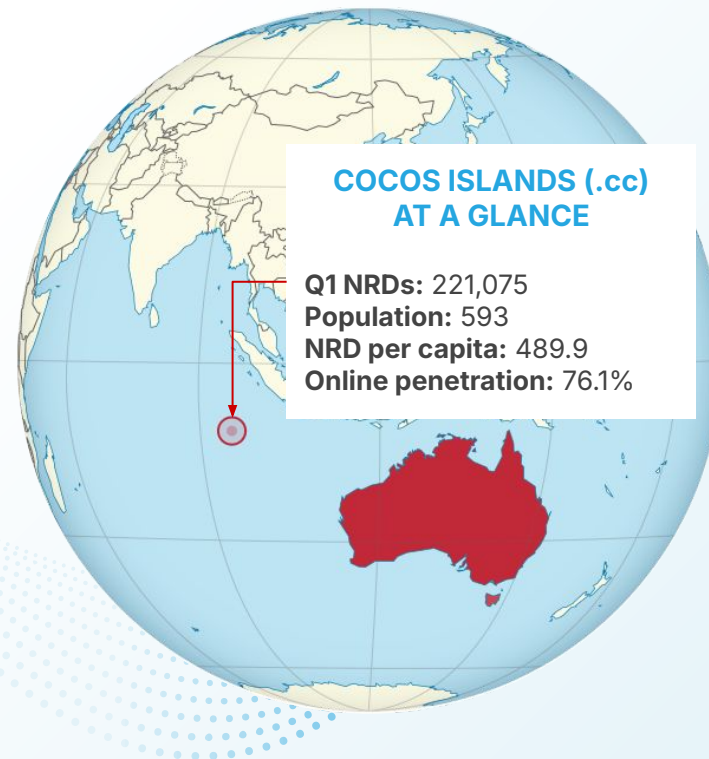
.cc ccTLD Still Sports NRD Volume-Population Size Incongruence

Over time, we found ccTLDs with somewhat irregular registration patterns—their total NRD registrations were significantly higher than their population sizes. Tokelau (.tk) and Samoa (.ws) were prime examples in our [Q3 2023](#) and [Q4 2023](#) reports, respectively.

Throughout last year up to this one, however, we have had a similar finding for the Cocos (Keeling) Islands' .cc. The extension has consistently been in the quarterly top 10. In Q1 2025, it had 221,075 new domains despite having only [593 residents](#).

In fact, this quarter, .cc was number 7, accounting for a 4.0% share of the total number of new domain registrations sporting ccTLDs. That gave the country an NRD per capita of 489.9 considering an online penetration of [76.1%](#).

Data source: [Newly Registered Domains](#)



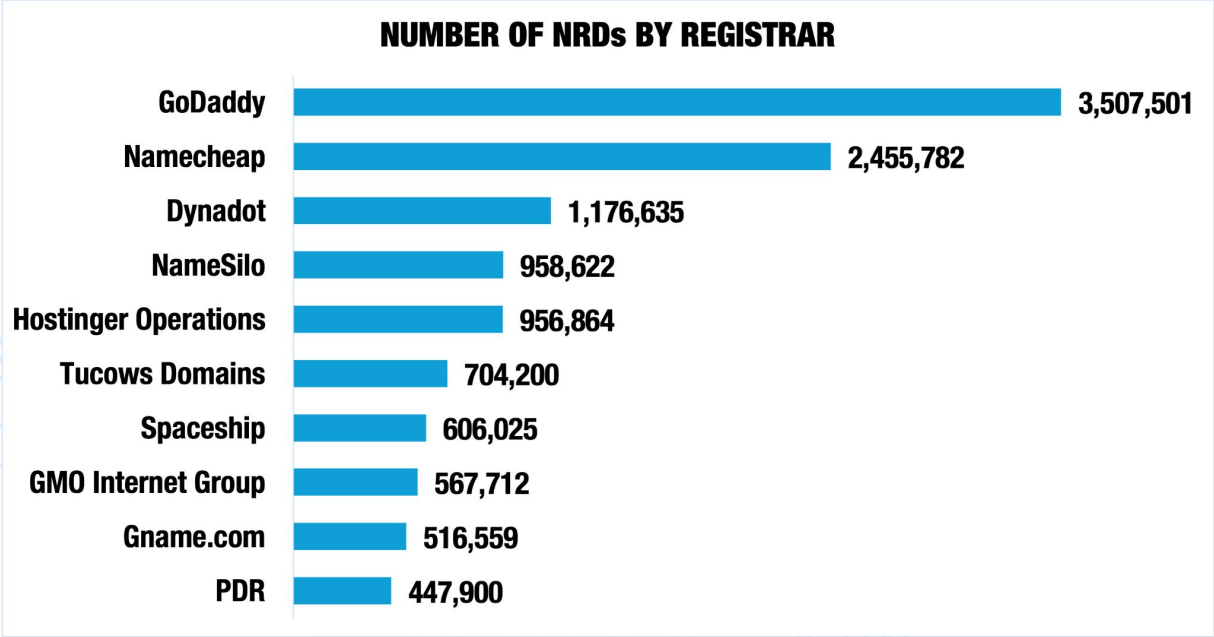


New Domain Activity: Most Popular Registrars

As in previous quarters, GoDaddy continued to be the most popular registrar in Q1. Namecheap, Dynadot, NameSilo, Hostinger Operations, Tucows Domains, Spaceship, GMO Internet Group, Gname.com, and PDR rounded out the top 10.

In sum, these 10 registrars accounted for 50.6% of the total Q1 2025 new domain registration volume.

Data source: [Newly Registered Domains](#)





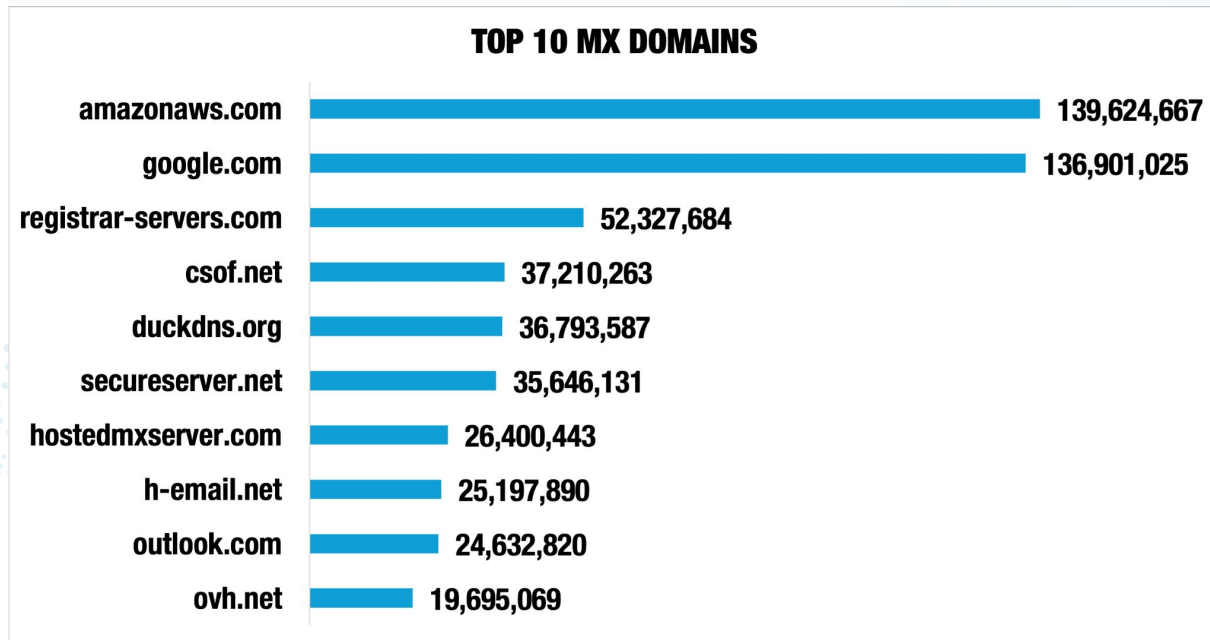
DNS Activity: Most Popular Mail Servers

We then examined the top 100 MX domains, which represented the mail server values that appeared in 790.0+ million MX records.

This data was collected from a passive DNS database file for March 2025 and includes MX records from the past 365 days.

The top 10 MX domains accounted for 67.6% of the top 100.

Data source: [DNS Database Download](#)





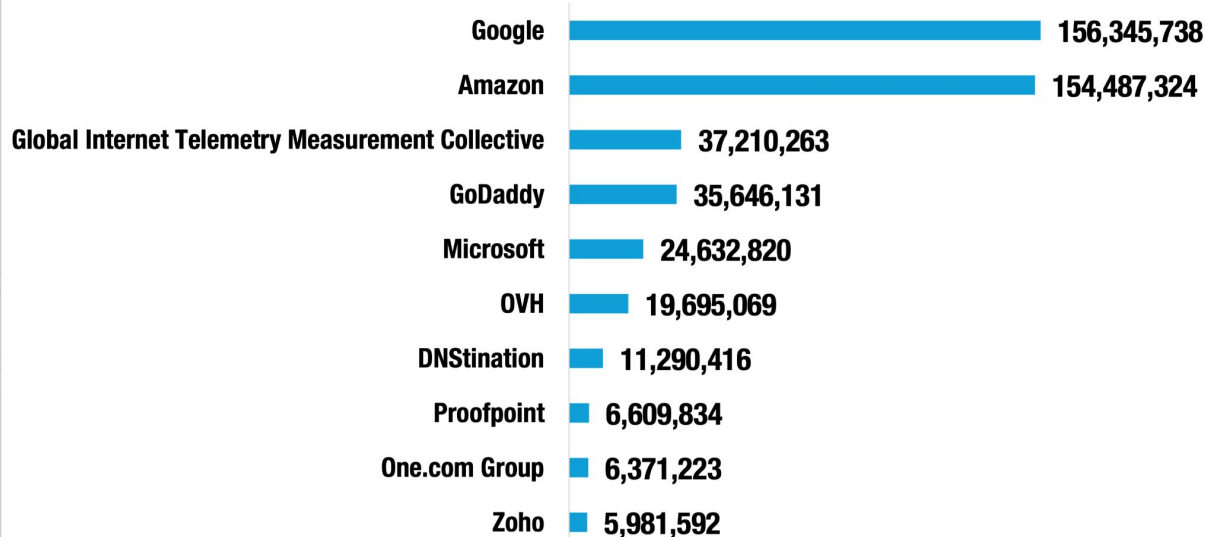
DNS Activity: Top Mail Server Providers

A Bulk WHOIS API query for the top 100 MX domains revealed that Google remained the number 1 registrant organization. The company accounted for 19.8% of the total MX domain resolution volume.

It's also worth noting that 37.6% of the MX domain resolutions could not be attributed to any provider due to WHOIS record redaction or nonidentification.

Data sources: [Bulk WHOIS API](#), [DNS Database Download](#)

TOP 10 MX DOMAIN REGISTRANT ORGANIZATIONS





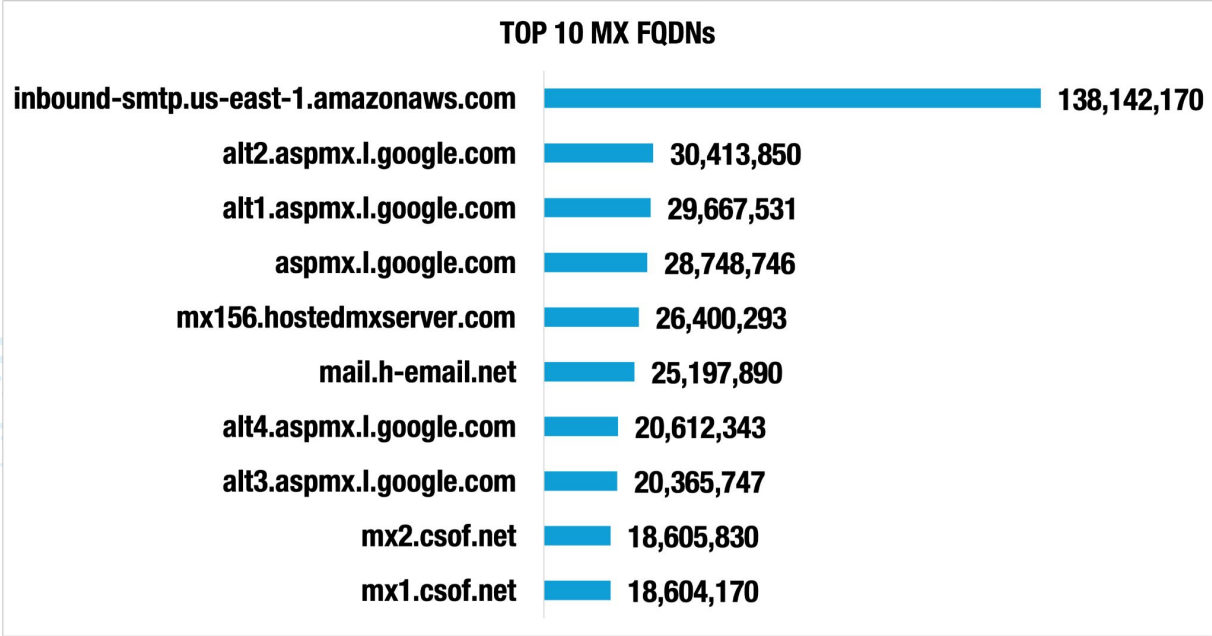
DNS Activity: Most Popular MX FQDNs

We also took a closer look at 642.0+ million MX domain records to determine the top 100 MX FQDNs.

This data was collected from a passive DNS database file for March 2025 and includes MX records from the past 365 days.

The top 10 MX FQDNs accounted for 55.6% of the top 100.

Data source: [DNS Database Download](#)





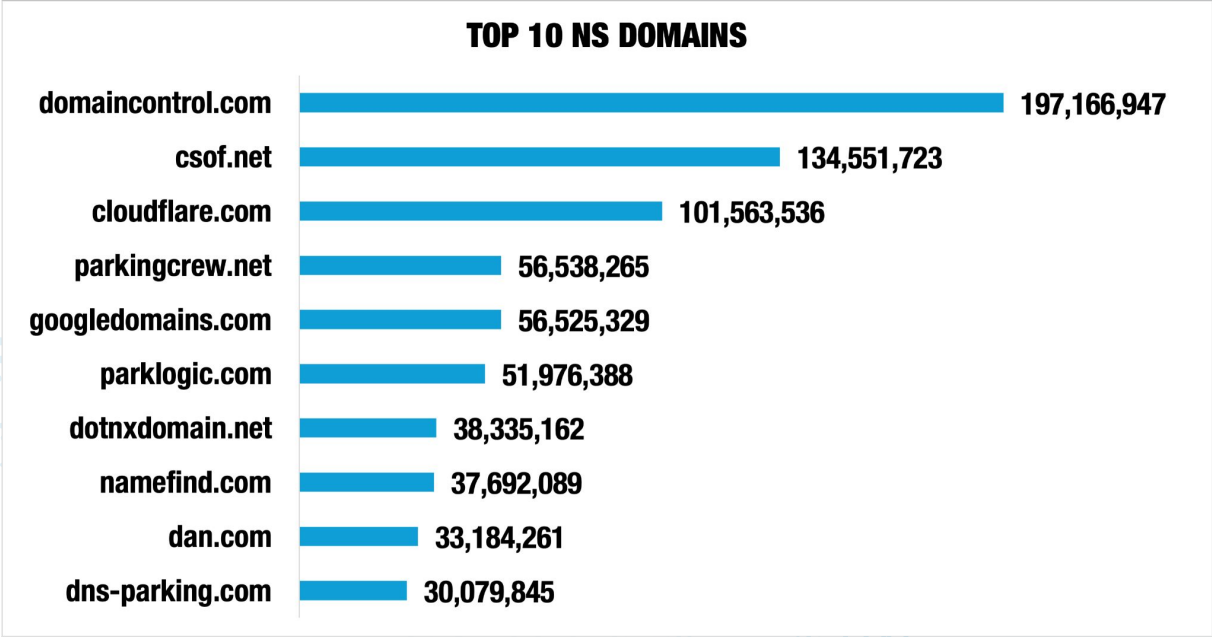
DNS Activity: Most Popular Name Servers

Next, we dove into the top 100 NS domains, which represented the NS values that appeared in 1.5+ billion NS records.

This data was collected from a passive DNS database file for March 2025 and includes NS records from the past 365 days.

The top 10 NS domains accounted for 48.0% of the top 100.

Data source: [DNS Database Download](#)



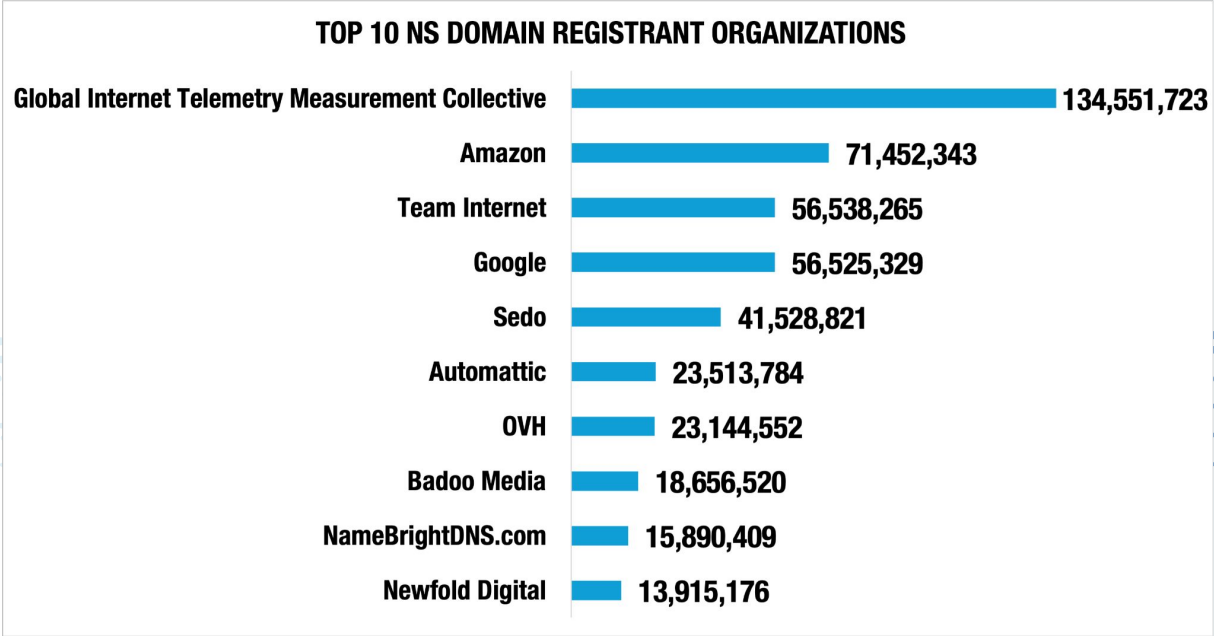


DNS Activity: Top Name Server Providers

A Bulk WHOIS API query for the top 100 NS domains showed that Global Internet Telemetry Measurement Collective was the number 1 registrant organization. The company accounted for 8.8% of the total NS domain resolution volume.

Note, however, that 64.0% of the NS domain resolutions could not be attributed to any provider since their WHOIS records have either been redacted or left blank.

Data sources: [Bulk WHOIS API](#), [DNS Database Download](#)





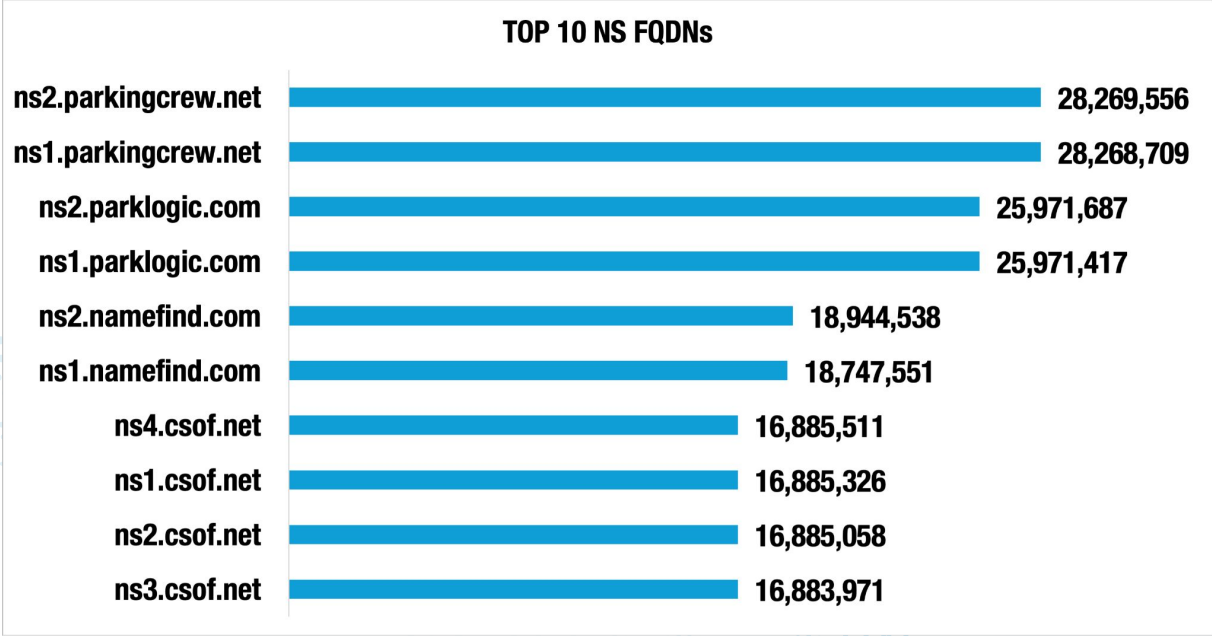
DNS Activity: Most Popular NS FQDNs

We also scrutinized the 825.4+ million NS domain records to determine the top 100 NS FQDNs.

This data was collected from a passive DNS database file for March 2025 and includes NS records from the past 365 days.

The top 10 NS FQDNs accounted for 25.9% of the top 100.

Data source: [DNS Database Download](#)



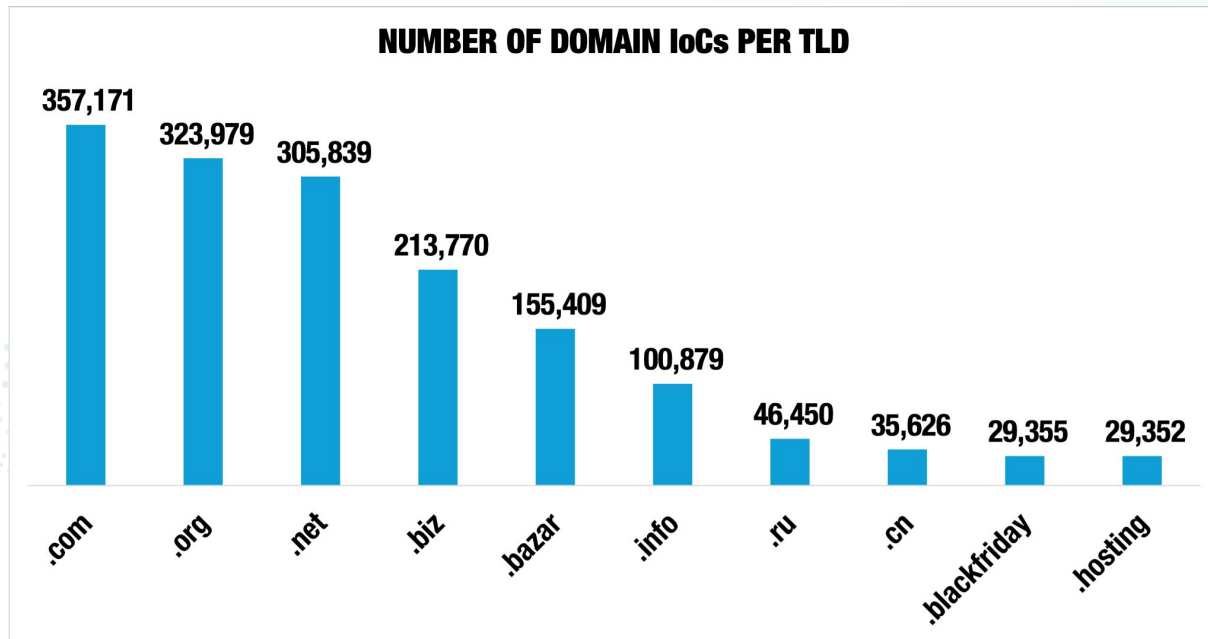


Decoding the Malicious Domain TLD Usage Trends

Finally, we analyzed 2.1+ million domains tagged as IoCs for various cyber threats in Q1 2025.

A bigger proportion of the top domain IoC TLDs was made up of gTLDs. In particular, .com was the most prevalent gTLD extension as usual. The most popular ccTLD extension, meanwhile, was .ru, the same as in Q4 2024.

Data source: [Threat Intelligence Data Feeds](#)





Analyzing the Malicious gTLD Domains

The domains tagged as IoCs in Q1 2025 used several gTLD extensions. The gTLDs .com, .org, .net, .biz, .bazar, .info, .blackfriday, and .hosting, in fact, made it to the top 10 TLD list of malicious domains. As usual, their popularity in terms of general usage patterns likely influenced their employment in malicious campaigns.

Take .com, for instance. It consistently topped the list of most used gTLD extensions for NRDs and domain IoCs alike. Interestingly, though, more malicious domains using .biz, .bazar, .hosting, and .blackfriday were proportionally detected compared with new registrations. In fact, .bazar did not even make it to the top 100 list of NRD TLDs.

Data source: [Threat Intelligence Data Feeds](#)

Description	.com	.org	.net	.biz	.bazar	.info	.blackfriday	.hosting
New malicious domains listed in Q1	357,171	323,979	305,839	213,770	155,409	100,879	29,355	29,352
New domains added in Q1	9,089,359	594,093	509,161	56,540	Not in the top list	422,848	8	27



Analyzing the Malicious ccTLD Domains

The most used ccTLDs among the domains tagged as IoCs in Q1 2025 remained the same as in previous quarters. The extension .ru took the top spot as seen in Q4 2024.

A comparison of the ccTLDs' shares of the total new additions in Q1 showed they comprised 3.9% of the total number of IoCs and 0.3% of the total NRD volume.

Data source: [Threat Intelligence Data Feeds](#)

Description	.ru	.cn
New malicious domains listed in Q1	46,450	35,626
New domains added in Q1	404,519	408,627

Q1 2025 Wrap-Up

The background features a solid blue color. Overlaid on this are several wavy, horizontal lines composed of small, dark blue dots. These lines create a sense of motion and depth, flowing from the left side towards the right, with some lines appearing more prominent than others.

Wrap-Up

The Q1 2025 Global Domain Activity Report provides critical insights into domain registration patterns, DNS MX and NS activity trends, and the TLD usage of malicious domains.

Analyzing these patterns can reveal the preferences and behaviors of legitimate and malicious entities alike, 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, SOC's, 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

For more information about WhoisXML API and our DNS, IP, and WHOIS intelligence products, please [contact our sales team](#).