



Global Domain Activity Report

Q4 2024



Dear Reader,

Another quarter has come to pass 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 aims to provide.

Join us as we look at global trends related to newly registered domains (NRDs), DNS activities, and verified indicators of compromise (IoCs) in Q4 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 Q4 2024, we identified 24.4+ million new domain registrations, increasing from 21.9+ million recorded in Q3 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 3.5+ million domains tagged as loCs 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. [New Domain Activity: Most Popular Registrars](#)
5. [DNS Activity: Most Popular Mail Servers](#)
6. [DNS Activity: Top Mail Server Providers](#)
7. [DNS Activity: Most Popular Name Servers](#)
8. [DNS Activity: Top Name Server Providers](#)
9. [Decoding Malicious Domain TLD Usage](#)
10. [Analyzing the Malicious gTLD Domains](#)
11. [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 Q4 2024 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 December 2024, 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](#).

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 October and 31 December 2024.

Q4 2024 Findings

The background features a solid blue color with decorative wavy lines composed of small dots in varying shades of blue and white, creating a sense of movement and depth.



Newly Registered Domains by TLD Type

The domain registrations increased from 21.9+ million in Q3 2024 to 24.4+ million in Q4. The number of NRDs sporting gTLDs rose by 9.8% while those sporting ccTLDs increased by 14.5%.

As in previous quarters, the number of gTLD registrations was significantly higher than the ccTLD registrations in Q4. The number of gTLD registrations was, in fact, 2.9 times higher. Overall, the average daily registration volume also rose from 239,029 in Q3 to 265,231 in Q4.

TLD Type	October	November	December	Q4 2024 Total	Q3 2024 Total
gTLD	6,232,212	5,915,802	6,058,660	18,206,674	16,578,580
ccTLD	1,991,327	2,270,992	1,932,243	6,194,562	5,412,120
TOTAL	8,223,539	8,186,794	7,990,903	24,401,236	21,990,700



New Domain Activity: gTLD Trends

The volume of NRDs under the .com gTLD in Q4 2024 remained significantly higher compared with other extensions.

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

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

Data source: [Newly Registered Domains](#)

NUMBER OF NRDs BY gTLD



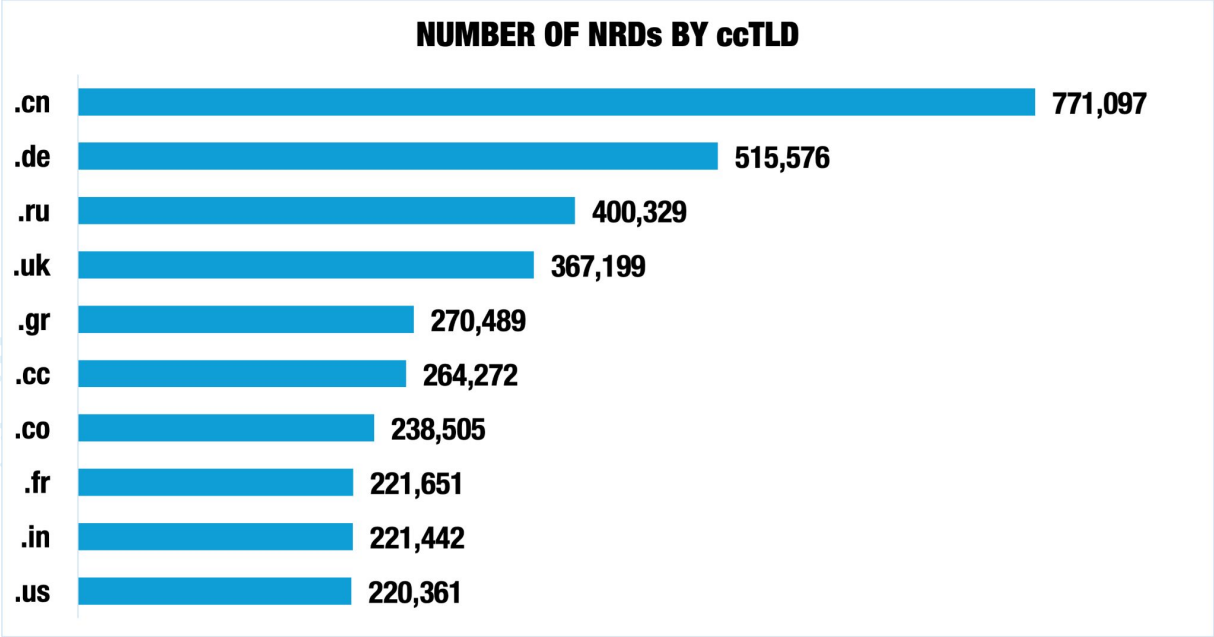


New Domain Activity: ccTLD Trends

The ccTLD extension .cn (China) remained in first place as in Q3. The extensions .de (Germany) and .ru (Russia) rounded out the top 3.

The other ccTLDs with high new domain registration numbers were .uk (U.K.), .gr (Greece), .cc (Cocos [Keeling] Islands), .co (Colombia), .fr (France), .in (India), and .us (U.S.).

Data source: [Newly Registered Domains](#)





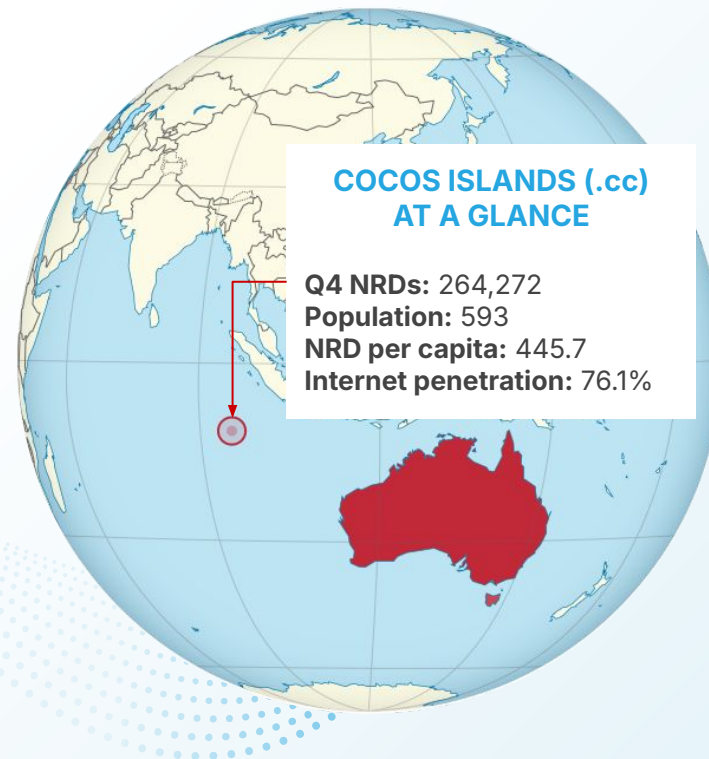
.cc ccTLD Retains Its NRD Volume-Population Size Incongruence

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 this year, however, we have had a similar finding for the Cocos (Keeling) Islands' .cc. The extension has consistently been in the quarterly top 10, this time around with 264,272 new domains despite having only [593 residents](#).

In Q4 2024, .cc stayed in the top 10, accounting for a 4.3% share of the total number of new domain registrations sporting ccTLDs. That gave the country an NRD per capita of 445.7.

Data source: [Newly Registered Domains](#)



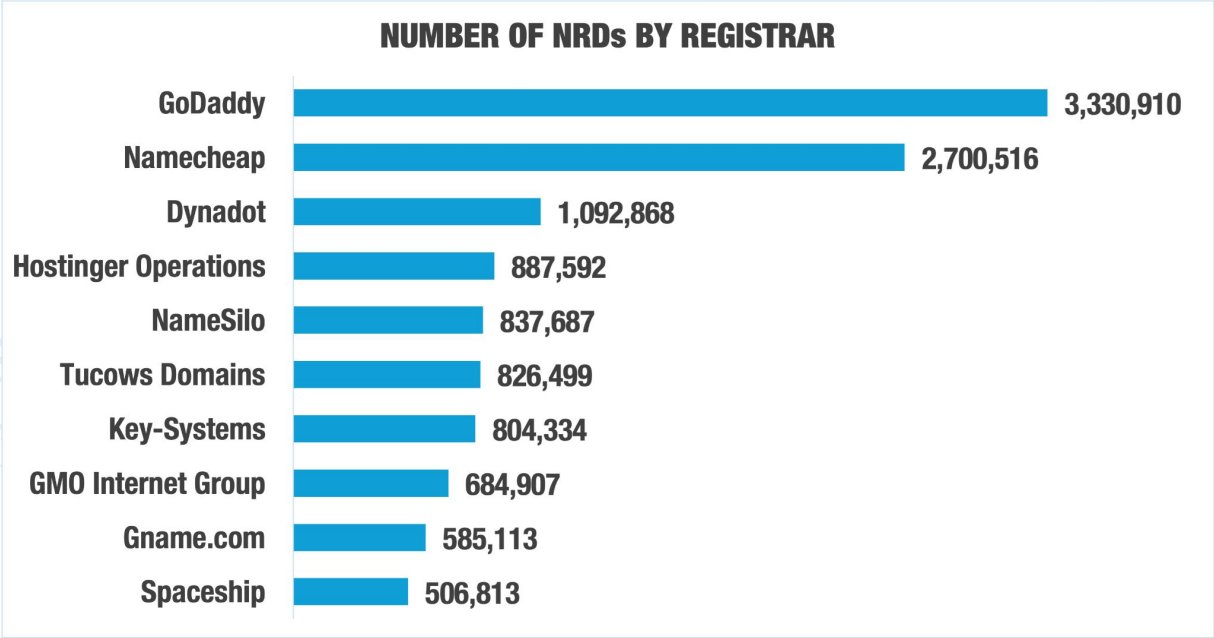


New Domain Activity: Most Popular Registrars

As in previous quarters, GoDaddy continued to be the most popular registrar in Q4. Namecheap, Dynadot, Hostinger Operations, NameSilo, Tucows Domains, Key-Systems, GMO Internet Group, Gname.com, and Spaceship rounded out the top 10.

In sum, these 10 registrars accounted for 50.2% of the total Q4 new domain registration volume.

Data source: [Newly Registered Domains](#)





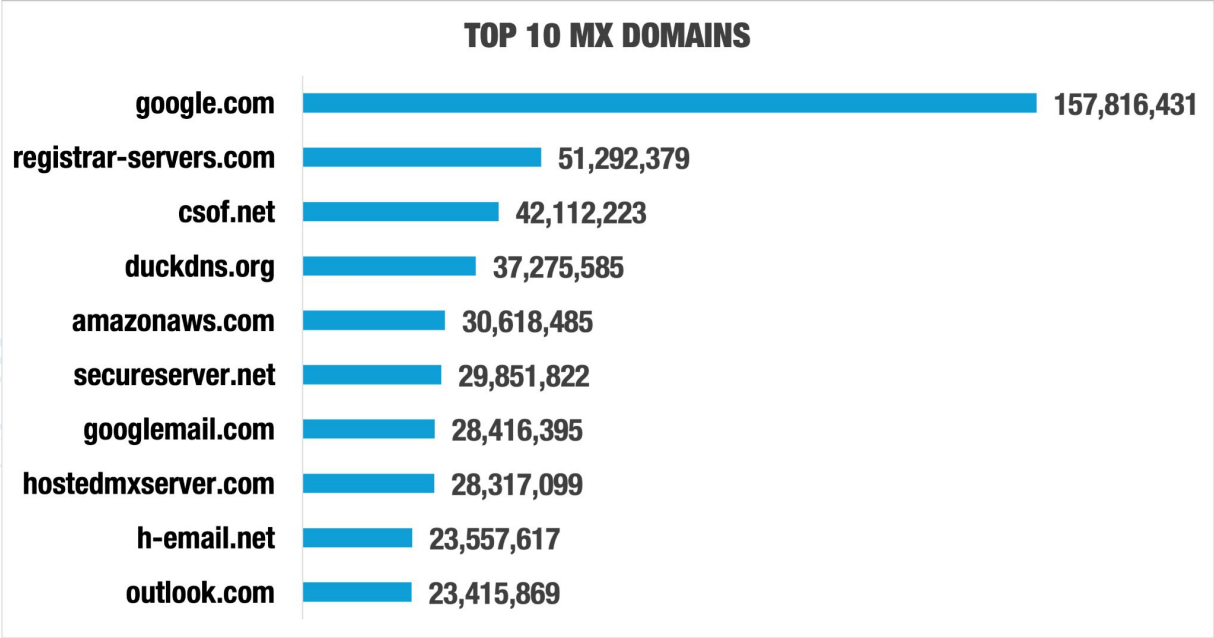
DNS Activity: Most Popular Mail Servers

We then examined the top 100 MX domains, which represented the mail server values that appeared in 697.4+ million MX records.

This data was collected from a passive DNS database file for December 2024 and includes MX records from the past 365 days.

The top 10 MX domains accounted for 64.9% of the top 100.

Data source: [DNS Database Download](#)



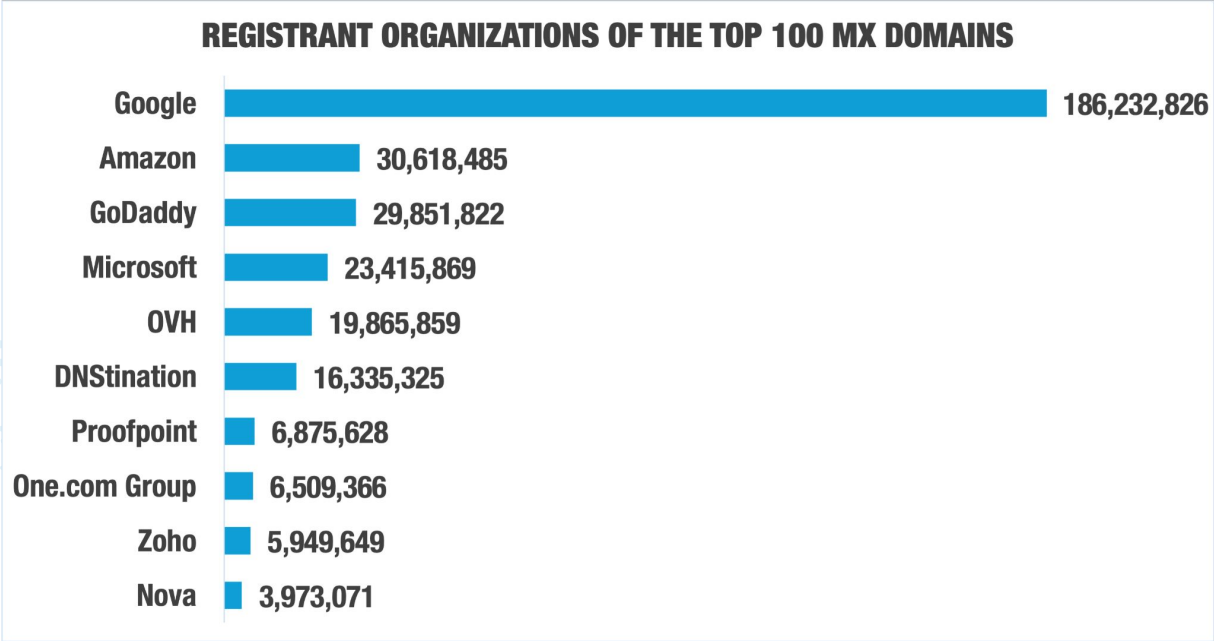


DNS Activity: Top Mail Server Providers

A bulk WHOIS lookup for the top 100 MX domains revealed that Google remained the number 1 registrant organization. The company accounted for 26.7% of the total MX domain volume.

It's also worth noting that 47.9% of the MX domain resolutions could not be attributed to any provider due to WHOIS record redaction or non-identification.

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





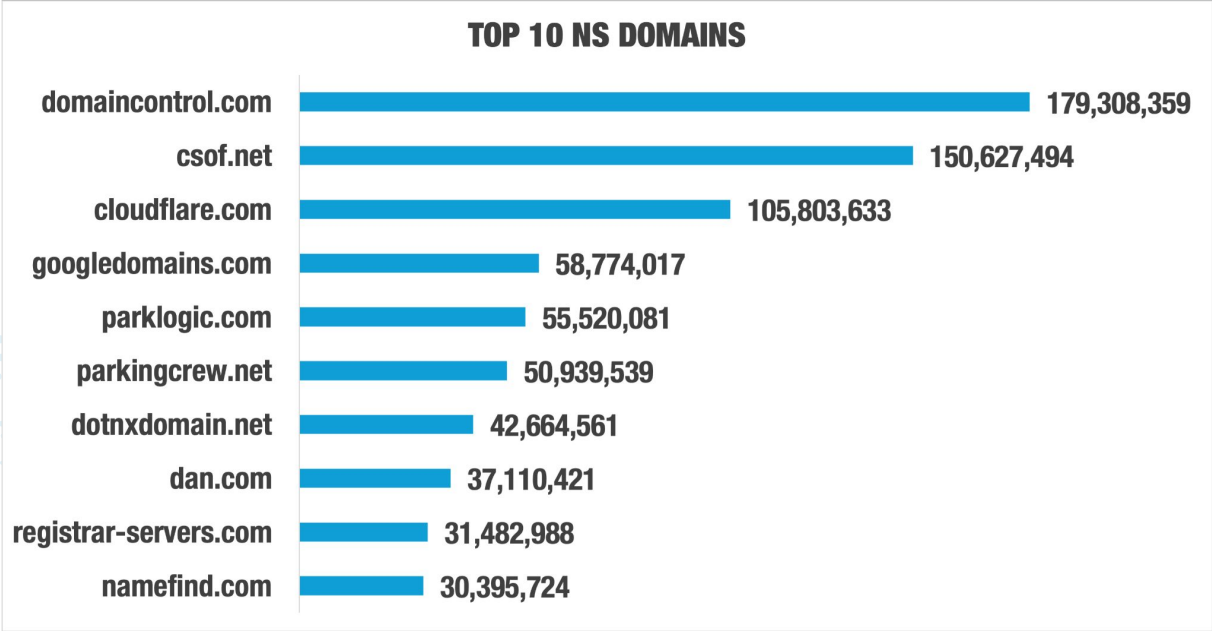
DNS Activity: Most Popular Name Servers

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

This data was collected from a passive DNS database file for December 2024 and includes NS records from the past 365 days.

The top 10 NS domains accounted for 46.5% of the top 100.

Data source: [DNS Database Download](#)



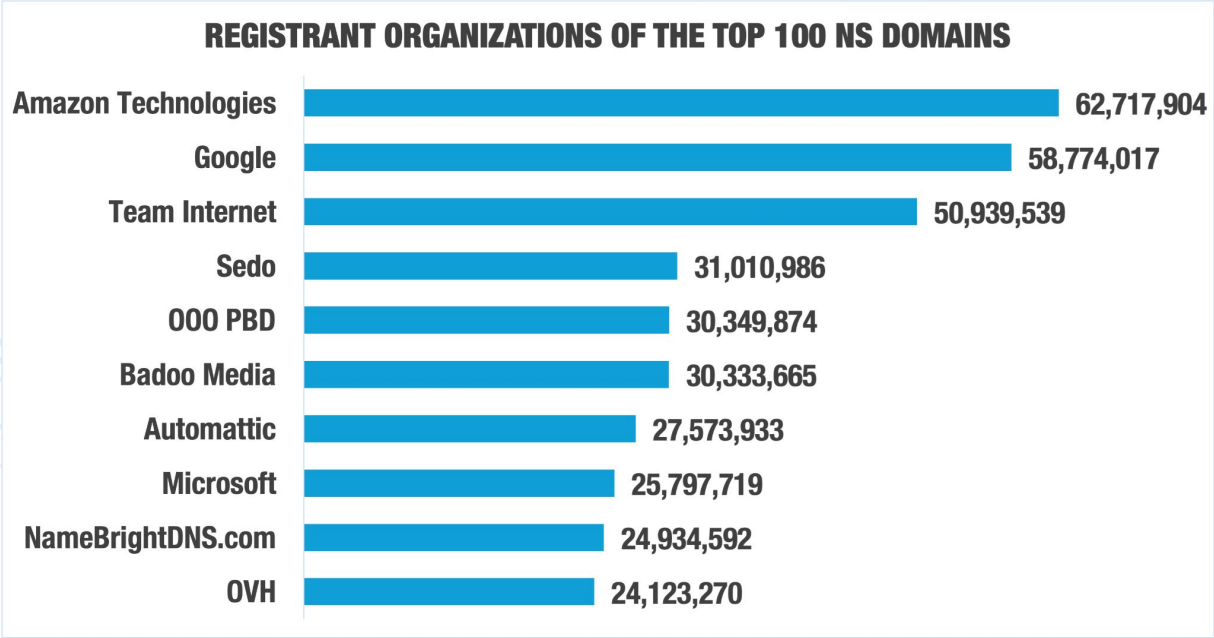


DNS Activity: Top Name Server Providers

A bulk WHOIS lookup for the top 100 NS domains showed that Amazon Technologies was the number 1 registrant organization. The company accounted for 3.9% of the total NS domain volume.

Note, however, that 68.5% 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 Lookup](#), [DNS Database Download](#)



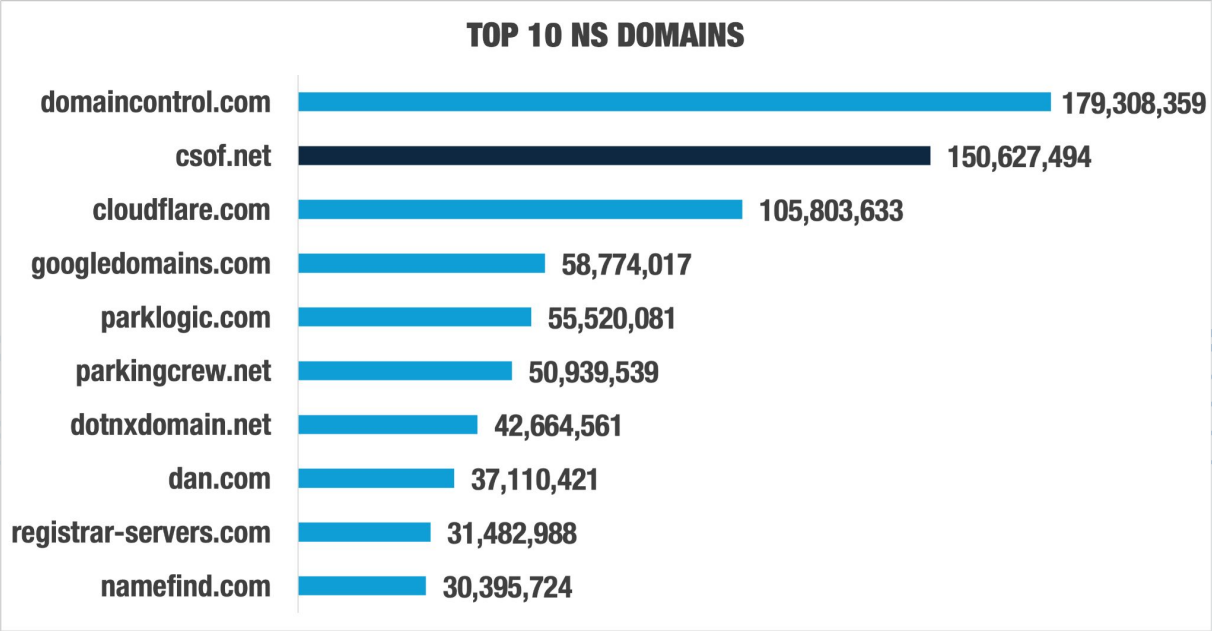


What Do We Know about csf[.]net?

Top 2 NS domain csf[.]net is owned by Csoft Hosting, a Manhattan-based open-source hosting service provider for the past 25 years. It accounted for 150.6+ million or 9.4% of the top 100 NS domains we analyzed.

It taking second place in the chart may be related to the open-source nature of its service.

Data sources: [Domain Research Suite](#), [DNS Database Download](#)



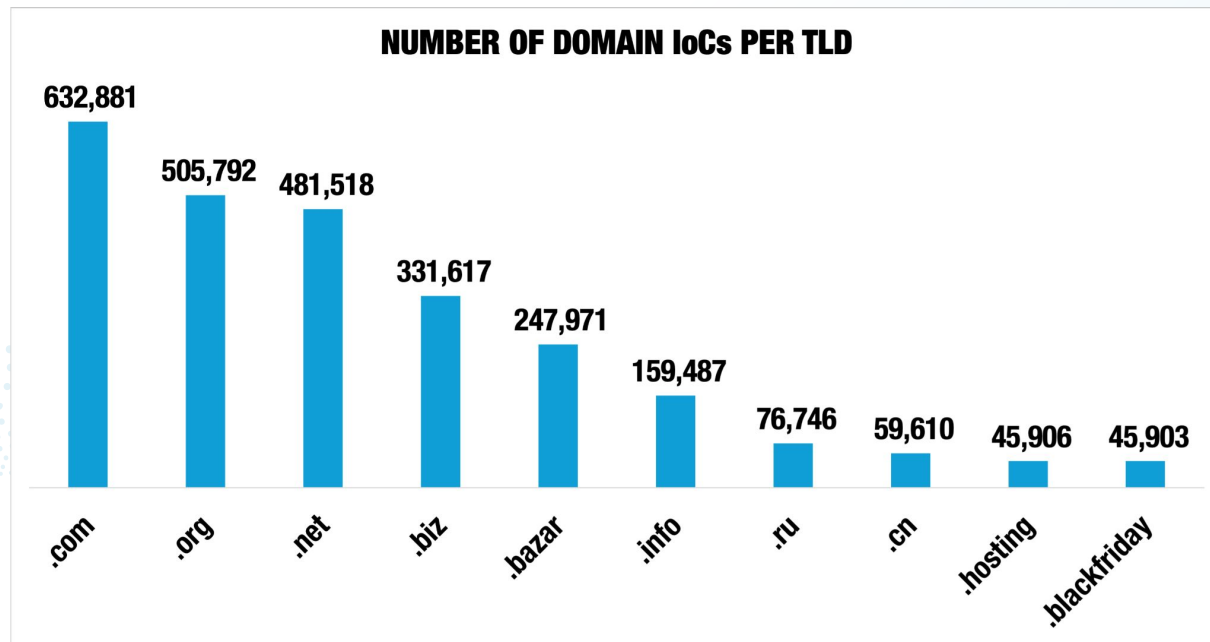


Decoding the Malicious Domain TLD Usage

Finally, we analyzed 3.5+ million domains tagged as IoCs for various cyber threats in Q4.

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

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





Analyzing the Malicious gTLD Domains

The domains tagged as IoCs in Q4 used several gTLD extensions. The gTLDs .com, .org, .net, .biz, .bazar, .info, .hosting, and .blackfriday, in fact, made it to the top 10 TLD list of malicious domain volumes. 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, .hosting, and .blackfriday were proportionally detected compared with new registrations.

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

Description	.com	.org	.net	.biz	.bazar	.info	.hosting	.blackfriday
New malicious domains listed in Q4	632,881	505,792	481,518	331,617	247,971	159,487	45,906	45,903
New domains added in Q4	8,654,747	567,696	589,151	75,722	-	400,434	21	53



Analyzing the Malicious ccTLD Domains

The most used ccTLDs among the domains tagged as IoCs in Q4 remained the same as in the previous quarter. The extensions .ru and .cn were, however, the only ones that made it to the top 10 TLDs for malicious domains.

A comparison of the ccTLDs' shares of the total new additions in Q4 showed that they comprised 3.9% of the total number of IoCs and 4.8% of the total NRD volume.

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

Description	.ru	.cn
New malicious domains listed in Q4	76,746	59,610
New domains added in Q4	400,329	771,097

Q4 2024 Wrap-Up

The background of the slide is a solid blue color. Overlaid on this background are several wavy, horizontal lines composed of small, dark blue dots. These lines create a sense of motion and flow, starting from the left side and extending towards the right. The dots are arranged in a way that forms a series of connected, undulating curves, giving the impression of a stylized wave or a data visualization element.

Wrap-Up

The Q4 2024 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](#).