WhoisXMLAPI

Global Domain Activity Report

Q3 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 provides.

Join us as we look at global trends related to newly registered domains (NRDs), DNS activities, and verified indicators of compromise (IoCs) in Q3 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 Q3 2024, we identified close to 22 million new domain registrations, representing roughly a 2% increase compared with Q2 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 more than 3 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.

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 Q3 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 dated 5 September 2024, zooming in on the top MX and NS fully qualified domain names (FQDNs), MX resolution domains, and NS domains.

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 between 1 July and 30 September 2024.

Q3 2024 Findings

Newly Registered Domains by TLD Type

The domain registrations slightly rose by 2.05% in Q3 2024 compared with Q2. The number of NRDs sporting gTLDs declined by 0.63% while those sporting ccTLDs increased by 11.24%.

As in previous quarters, the number of gTLD registrations was significantly higher than the ccTLD registrations in Q3. The number of gTLD registrations was, in fact, 3.06 times higher. Overall, the average daily registration volume also increased from 239,439 domains in Q2 to 244,341 in Q3.

TLD Type	July	August	September	Q3 2024 Total	Q2 2024 Total
gTLD	5,548,936	5,726,463	5,303,181	16,578,580	16,684,406
ccTLD	1,779,132	1,742,830	1,890,158	5,412,120	4,865,103
TOTAL	**7,328,068**	**7,469,293**	**7,193,339**	**21,990,700**	**21,549,509**

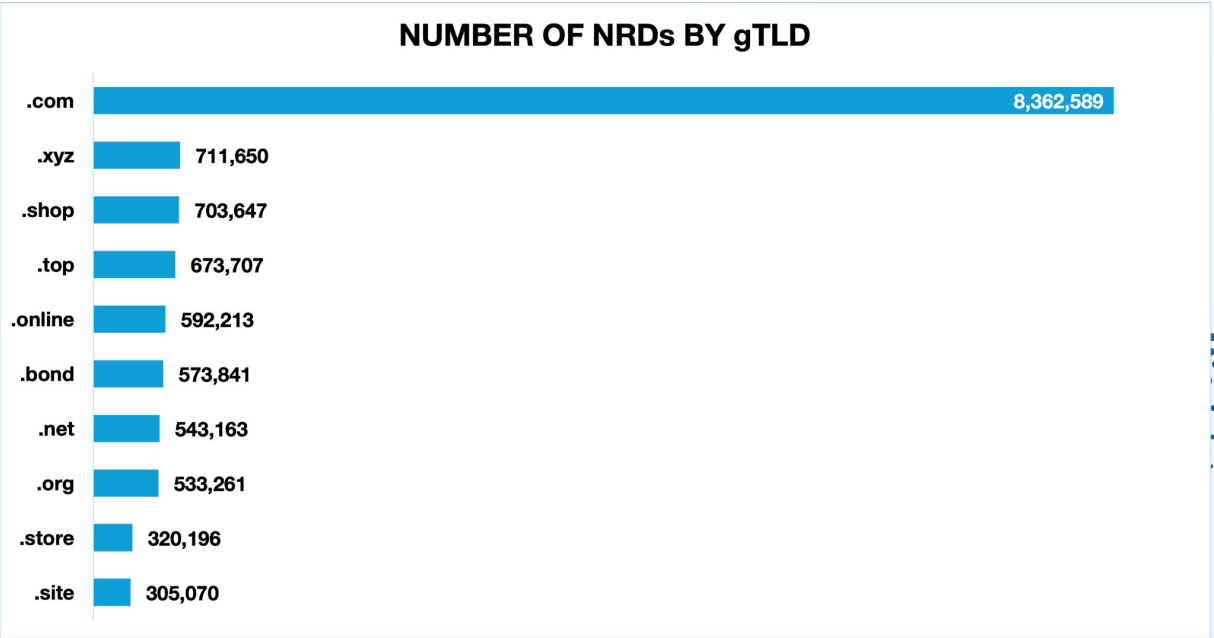
New Domain Activity: gTLD Trends

The volume of NRDs under the .com gTLD in Q3 2024 was 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 .xyz, .shop, .top, .online, .bond, .net, .org, .store, and .site.

Data source: Newly Registered Domains

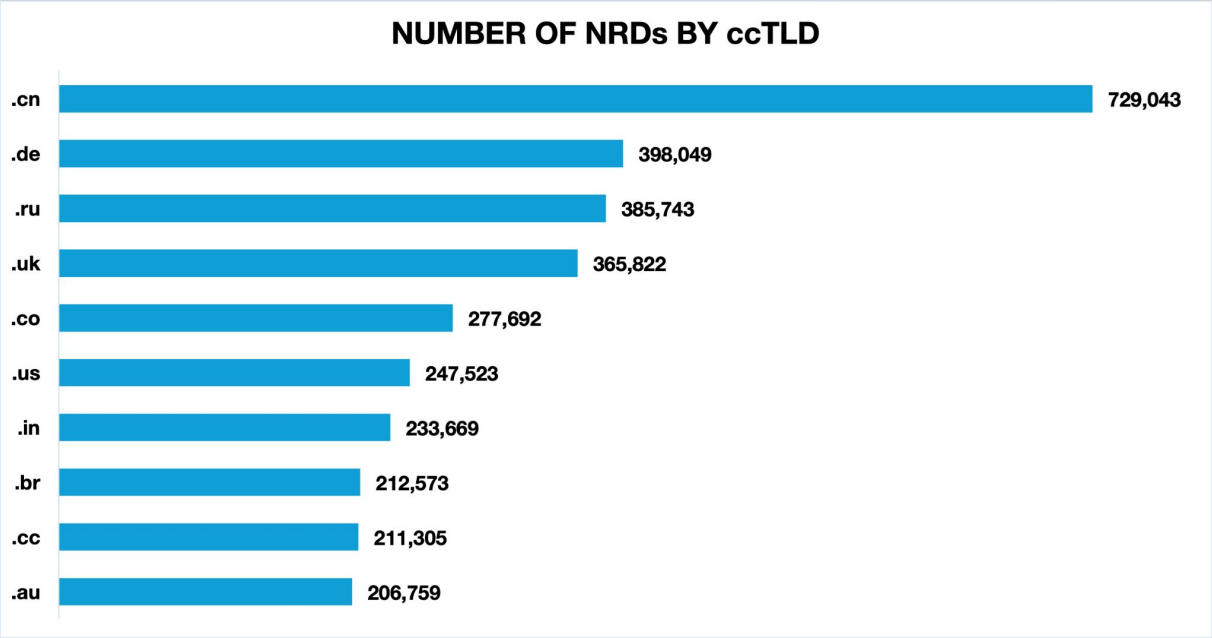


New Domain Activity: ccTLD Trends

The ccTLD extension .cn (China) remained in first place as in Q2. Two European ccTLDs .de (Germany) and .ru (Russia) rounded out the top 3.

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

Data source: Newly Registered Domains



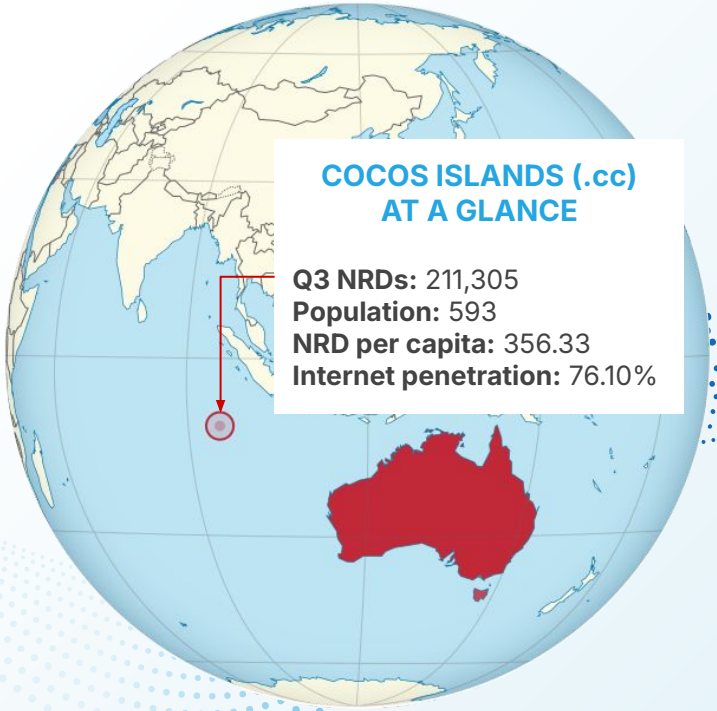
.cc ccTLD Retains Its NRD Volume-Population Size Incongruence

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) are prime examples.

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 211,305 new domains despite having only 593 residents.

In Q3, .cc stayed in the top 10, accounting for a 3.90% share of the total number of new domain registrations sporting ccTLDs. That gave the country an NRD per capita of 356.33.

Data source: Newly Registered Domains

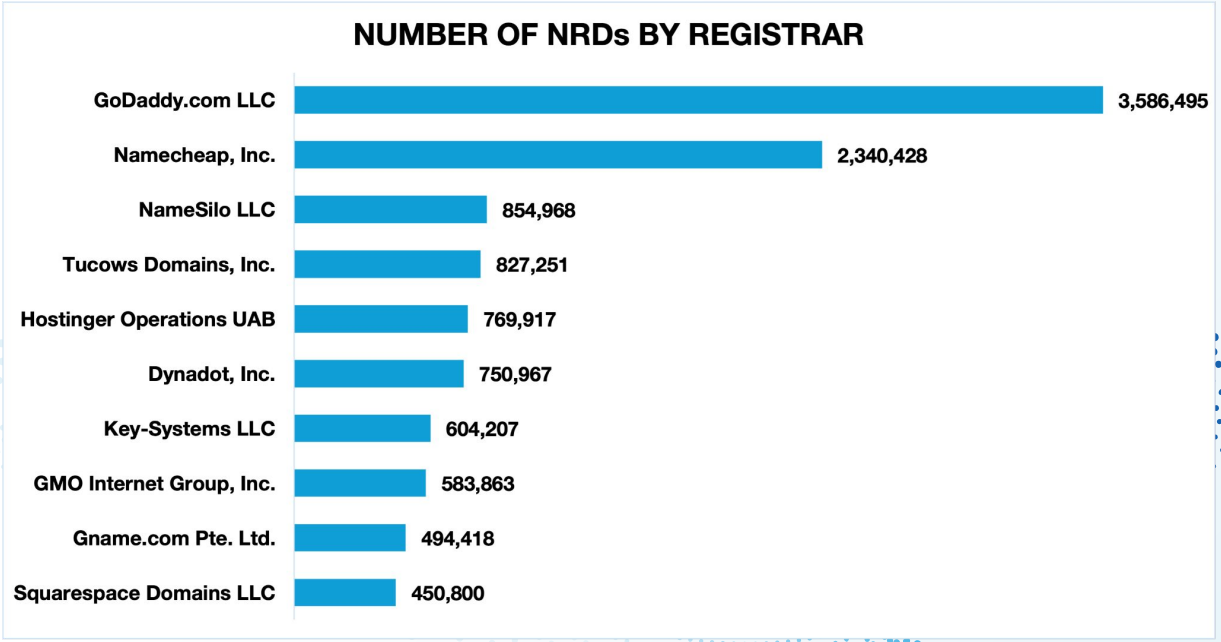


New Domain Activity: Most Popular Registrars

As in previous quarters, GoDaddy.com LLC continued to be the most popular registrar in Q3. Namecheap, Inc.; NameSilo LLC; Tucows Domains, Inc.; Hostinger Operations UAB; Dynadot, Inc.; Key-Systems LLC; GMO Internet Group, Inc.; Gname.com Pte. Ltd.; and Squarespace Domains LLC completed the top 10.

These registrars accounted for 51.22% of the total Q3 new domain registration volume.

Data source: Newly Registered Domains



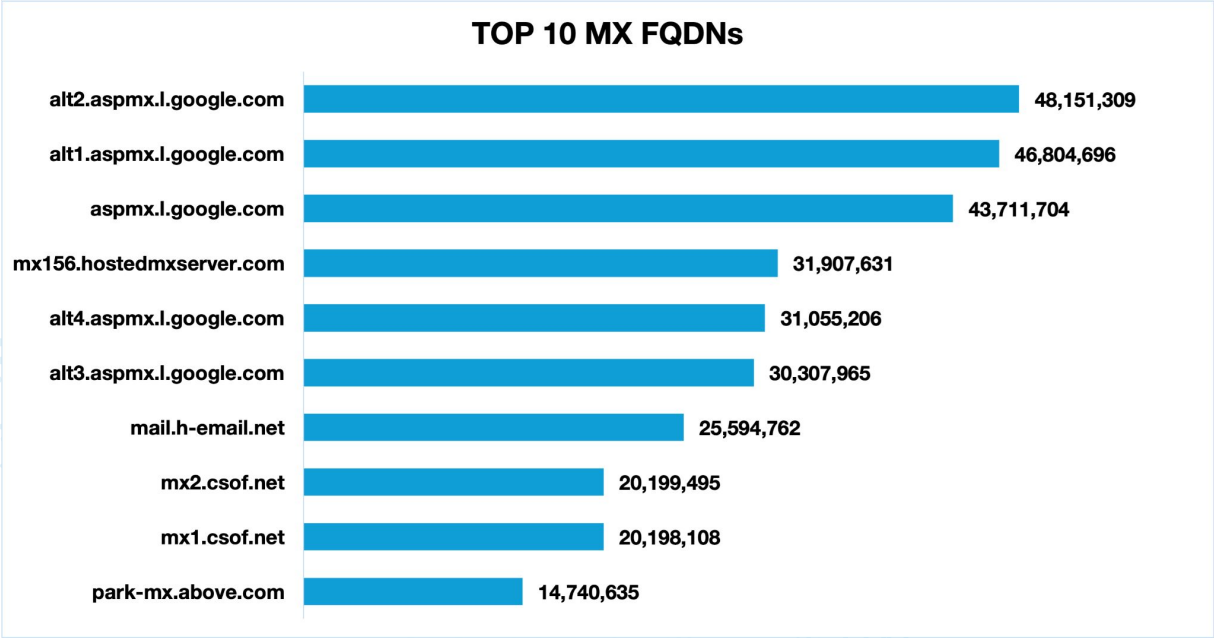
DNS Activity: Most Popular Mail Servers

We then examined the top 100 FQDNs found in MX records, which represented the exact MX values or mail servers that appeared in 618+ million MX records.

This data was collected from a passive DNS database file dated 5 September 2024 and includes MX records from the 365 days leading up to that date.

The top 10 MX FQDNs accounted for 50.55% of the top 100.

Data source: DNS Database Download

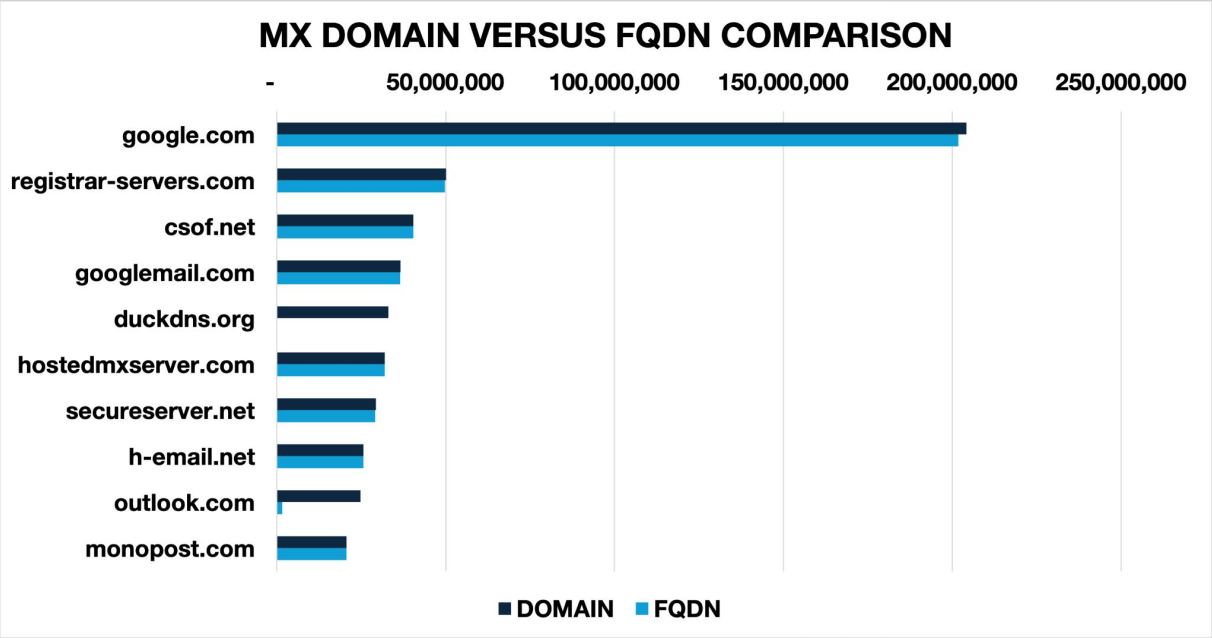


Disparity between the MX Root Domains and FQDNs

Apart from identifying the top MX FQDNs, we also determined the top 100 root domains of the MX records we analyzed.

It's interesting to note that even though duckdns[.]org was among the top 10 MX root domains, none of its FQDNs made it to the top 100 MX FQDNs.

Data sources: DNS Database Download

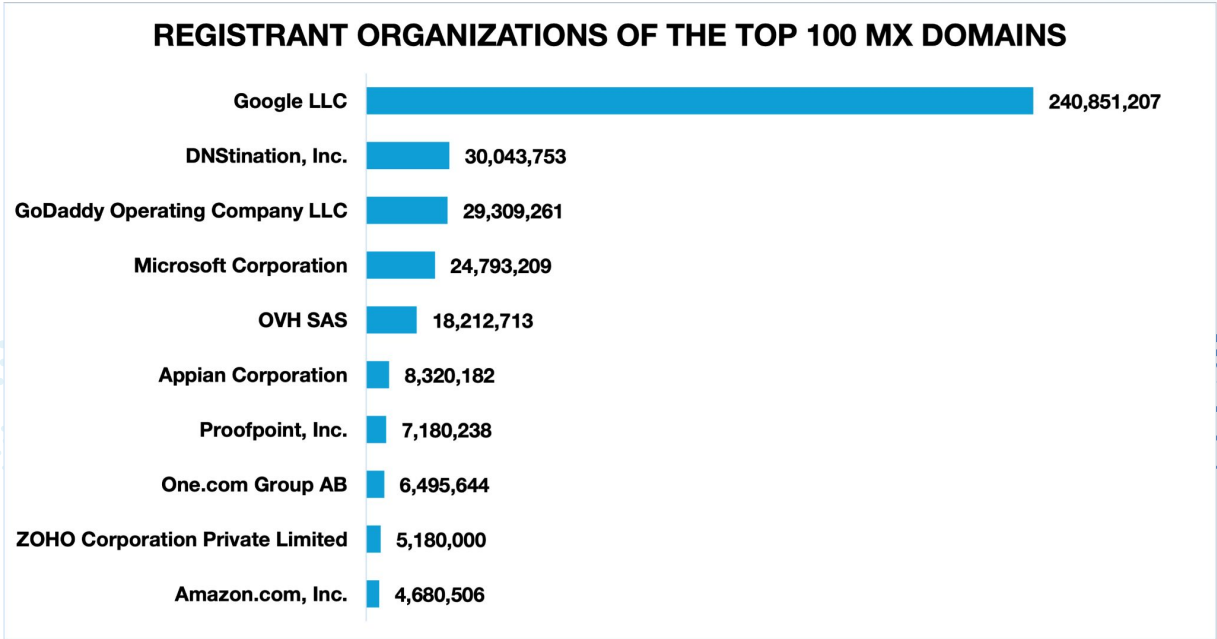


DNS Activity: Top Mail Server Providers

A bulk WHOIS lookup for the top 100 MX domains revealed that Google LLC remained the number 1 registrant organization. The company accounted for 26.04% of the total MX domain resolution volume.

It's also worth noting that 53.77% of the MX domain resolutions could not be attributed to any provider due to WHOIS record redaction.

Data sources: Bulk WHOIS Lookup, DNS Database Download



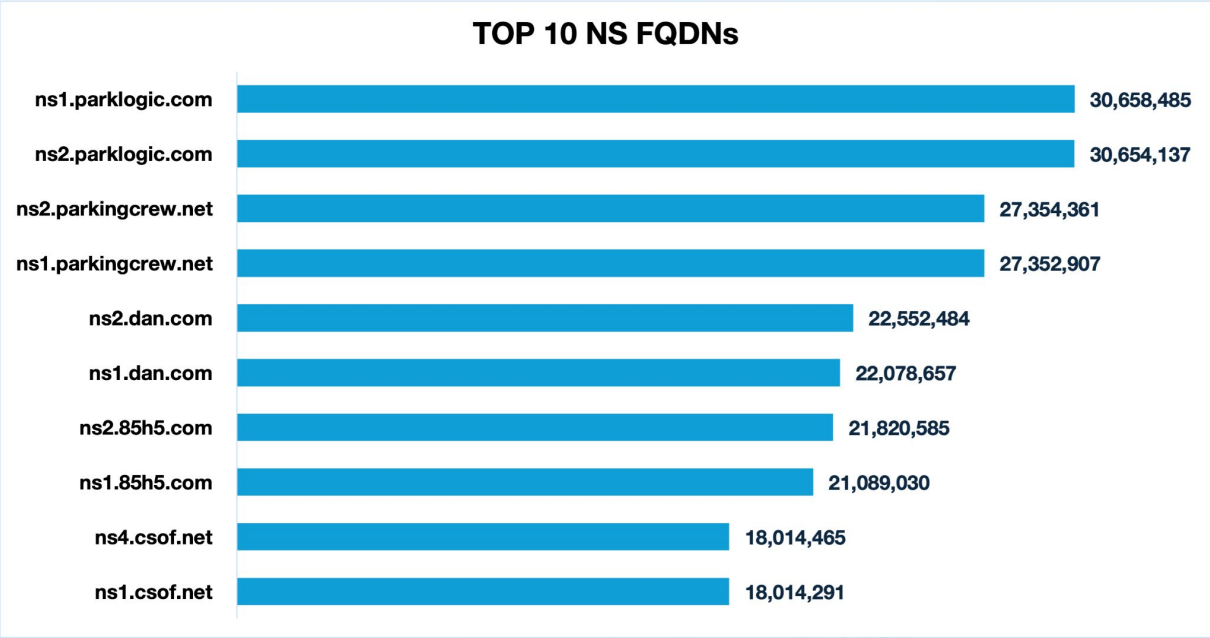
DNS Activity: Most Popular Name Servers

Next, we dove into the top 100 FQDNs found in NS records, which represented the exact NS values or name servers that appeared in more than 1 billion NS records.

This data was collected from a passive DNS database file dated 5 September 2024 and includes NS records from the 365 days leading up to that date.

The top 10 NS FQDNs accounted for 23.02% of the top 100.

Data source: DNS Database Download

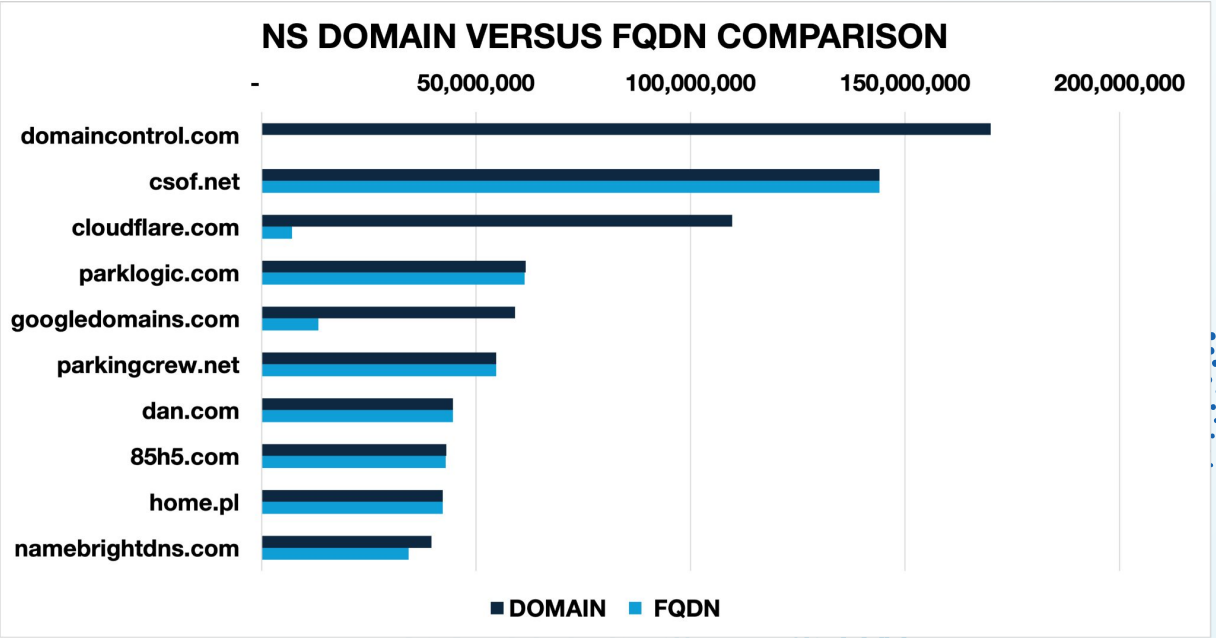


Disparity between the NS Root Domains and FQDNs

Apart from identifying the top NS FQDNs, we also determined the top 100 root domains of the NS records we analyzed.

Interestingly, even if domaincontrol[.]com was the top NS root domain, none of its FQDNs made it to the list of top 100 NS FQDNs.

Data sources: DNS Database Download

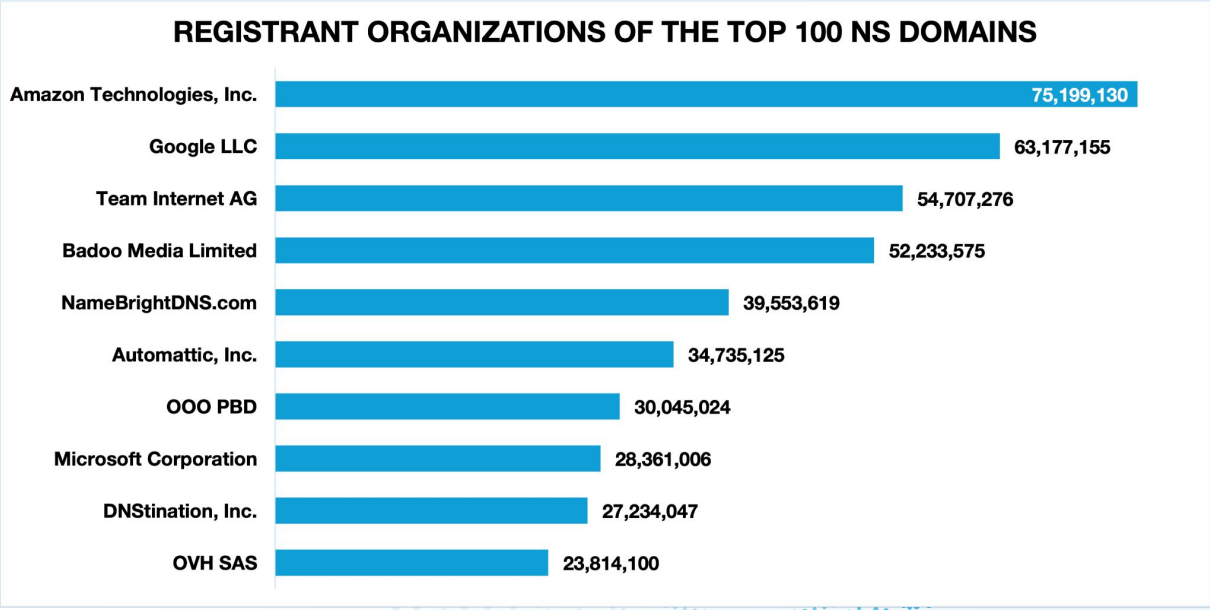


DNS Activity: Top Name Server Providers

A bulk WHOIS lookup for the top 100 NS domains showed that Amazon Technologies, Inc. was the number 1 registrant organization. The company accounted for 4.15% of the total NS domain resolution volume.

Note, however, that 73.79% of the NS domain resolutions could not be attributed to any provider since their WHOIS records have been redacted.

Data sources: Bulk WHOIS Lookup, DNS Database Download

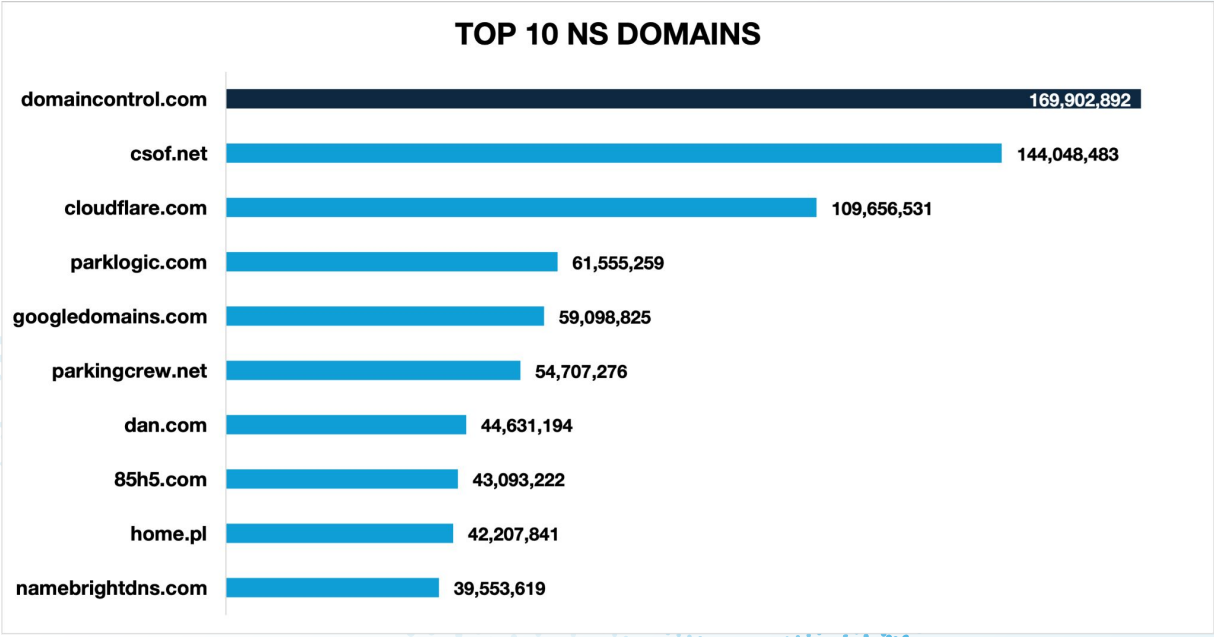


What Do We Know about the #1 NS Domain?

The top NS domain domaincontrol[.]com is owned by WildWestDomains, GoDaddy's white label reseller alias. It accounted for 169,902,892 or 9.37% of the top 100 NS domains we analyzed.

And that is not surprising, given that GoDaddy is likely the world's most popular domain registrar, reportedly owning 84 million of the registered domains as of September 2024.

Data sources: Domain Research Suite, DNS Database Download

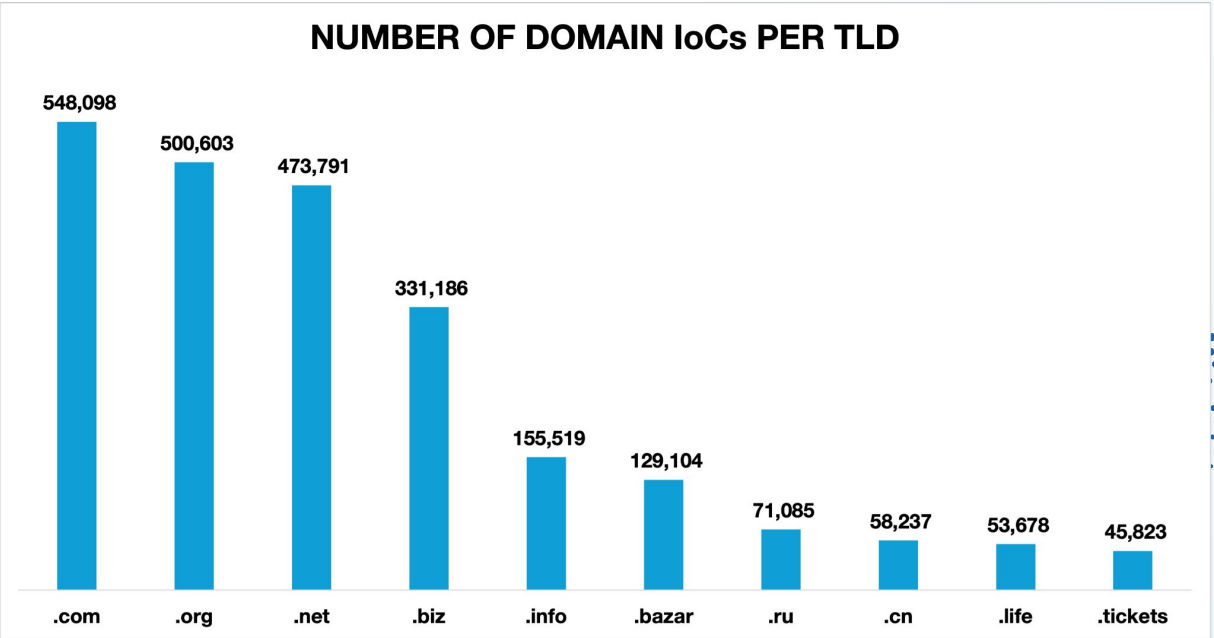


Decoding the Malicious Domain TLD Usage

Finally, we analyzed more than 3.16 million domains tagged as IoCs for various cyber threats in Q3.

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 Q3 used several gTLD extensions. The gTLDs .com, .org, .net, .biz, .info, .bazar, .life, and .tickets, 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 .org, .net, .biz, .bazar, .life, and .tickets were proportionally detected compared with new registrations.

Data source: Threat Intelligence Data Feeds

Description	.com	.org	.net	.biz	.info	.bazar	.life	.tickets
New malicious domains listed in Q3	548,098	500,603	473,791	331,186	155,519	129,104	53,678	45,823
New domains added in Q3	5,533,780	356,970	386,106	34,916	165,511	See note	38,929	13

Note: The gTLD extension .bazar did not make it to the top 100 list for Q3 2024 NRDs.

Analyzing the Malicious ccTLD Domains

The most used ccTLDs among the domains tagged as IoCs in Q3 remained the same as in previous quarters. The extensions .ru and .cn were, however, the only two that made it to the top 10 TLD list of malicious domains.

Interestingly, more .su, .to, and .so malicious domains were detected compared with their new registrations in Q3.

Data source: Threat Intelligence Data Feeds

Description	.ru	.cn	.su	.cc	.in	.to	.so
New malicious domains listed in Q3	71,085	58,237	39,372	30,240	27,164	24,860	24,695
New domains added in Q3	255,067	501,237	4,081	143,678	149,649	See note	630

Note: The ccTLD extension .to did not make it to the top 100 list for Q3 2024 NRDs.

Q3 2024 Wrap-Up

Wrap-Up

The Q3 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, 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

For more information about WhoisXML API and our DNS, IP, and WHOIS intelligence products, please contact our sales team.