Name Server Concentration: Who Controls the Domain Name System?

Posted on July 29, 2024

Name servers (NSs) play a crucial role in how the Internet works, directing traffic to the correct destinations. Specifically, NS records tell recursive resolver servers which authoritative NS is responsible for a specific domain name. The resolver would then contact the authoritative NS to obtain the domain's corresponding IP address.

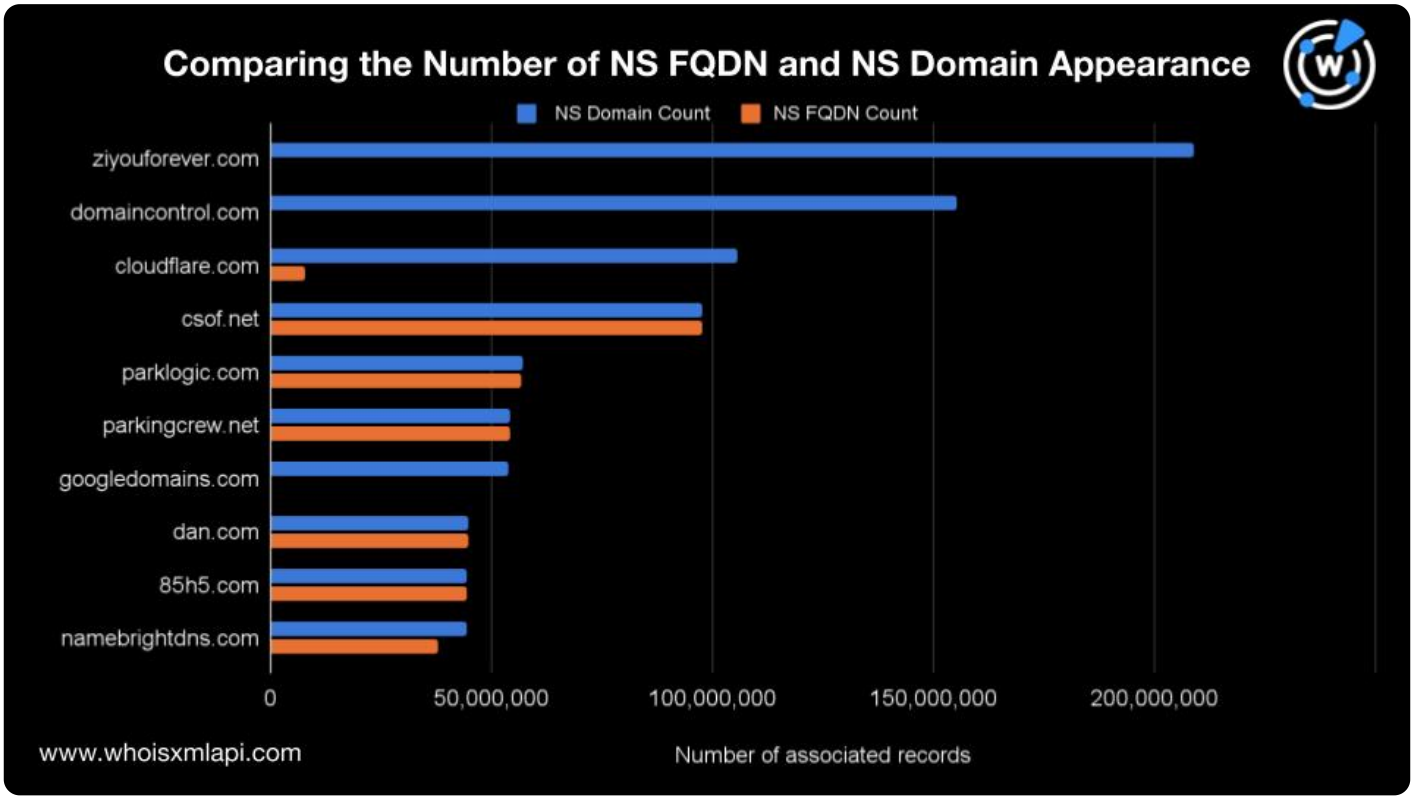
While having a small number of entities control a large portion of the DNS can increase efficiency, it could also result in choke points, where a single disruption could significantly impact a large portion of Internet traffic.

WhoisXML API researchers sought to determine NS concentration by gathering and analyzing the top 100 NS fully qualified domain names (FQDNs), such as ns1[.]parklogic[.]com and ns2[.]parklogic[.]com. These FQDNs are the exact NS values appearing on more than 1 billion NS records downloaded from a passive DNS database file generated for June 2024.We obtained their WHOIS registration details, extracting the domains' registrant organization and country data.

The research team also analyzed the top 100 NS domains or the most recurring root domain names (e.g., parklogic[.]com) from the same period.

FQDN versus Root Domain Use Prevalence

The first step in our analysis was to compare the top 100 NS FQDNs with the top 100 NS domains based on the hypothesis that the root domains of the FQDNs would also be among the top NS domains. Surprisingly, three top NS domains didn't make it to the list of the top 100 NS FQDNs. They were ziyouforever[.]com, domaincontrol[.]com, and googledomains[.]com.



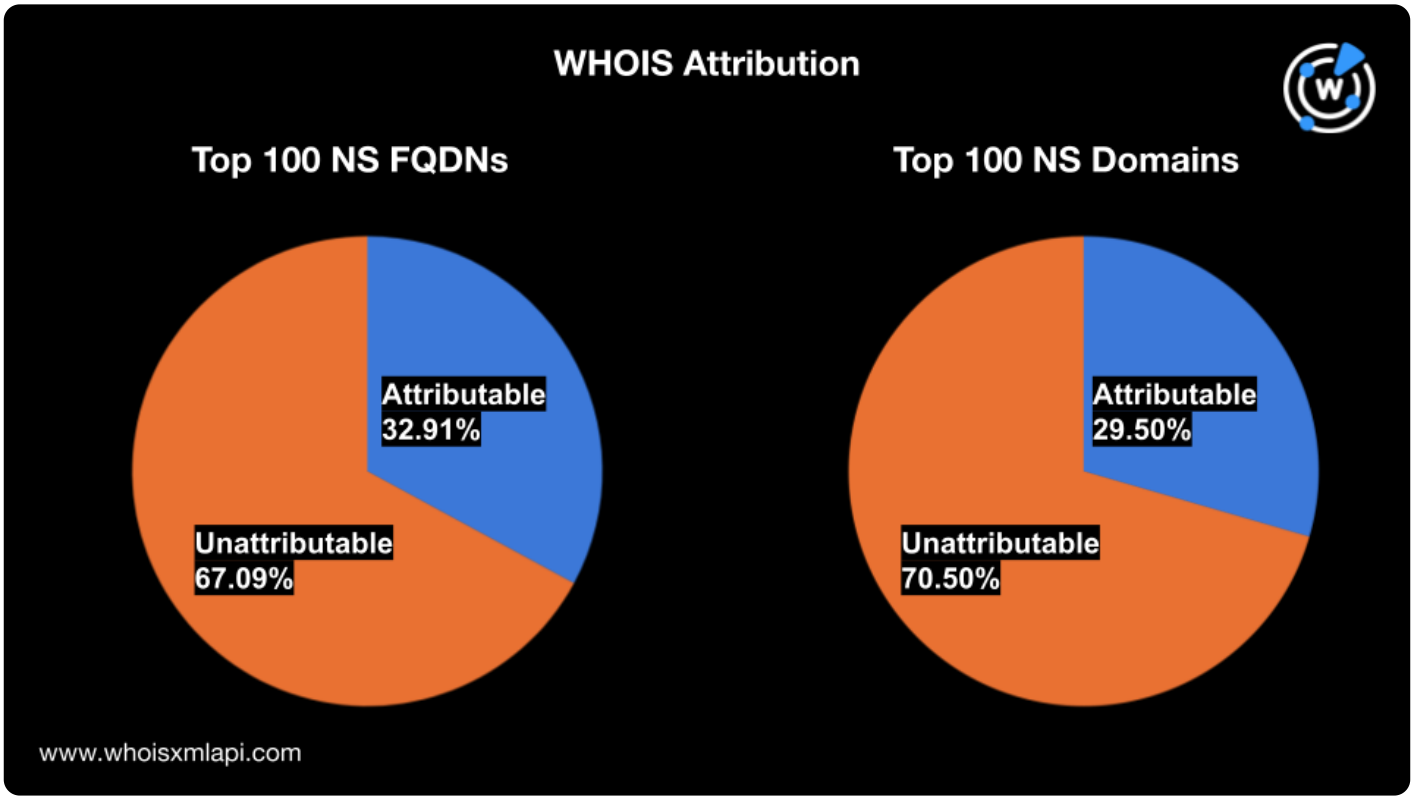
The prevalence of ziyouforever[.]com as a top NS domain coupled with its possible historical association with DNS tunneling may raise concerns, especially since more than 208 million NS records point to authoritative NSs associated with this domain.

67% of Name Servers Lead to Privacy-Protected Domains

The WHOIS details of the top 100 NS FQDNs pointed to 21 unique registrant organization values, nine of which were protected by privacy service providers. Overall, 56.53% of the NSs had privacy-protected registrant details, while 10.55% did not specify their registrant organizations. That makes more than 674 million or 67.09% of the top 100 NS FQDN records unattributable to specific NS providers.

These figures are roughly similar to the results of our NS domain analysis. About 62.04% of the

domains had privacy-protected WHOIS records, while 8.46% did not specify a current registrant organization, accounting for a total of 70.50% unattributable NS domains.



Domains by Proxy LLC was the most used privacy protection service provider by the NS FQDNs and NS domains. The company's name appeared in 23.08% and 32.25% of the NS records using the top 100 NS FQDNs and top 100 NS domains, respectively.

Amazon Controls 22% of the Attributable Name Server Records

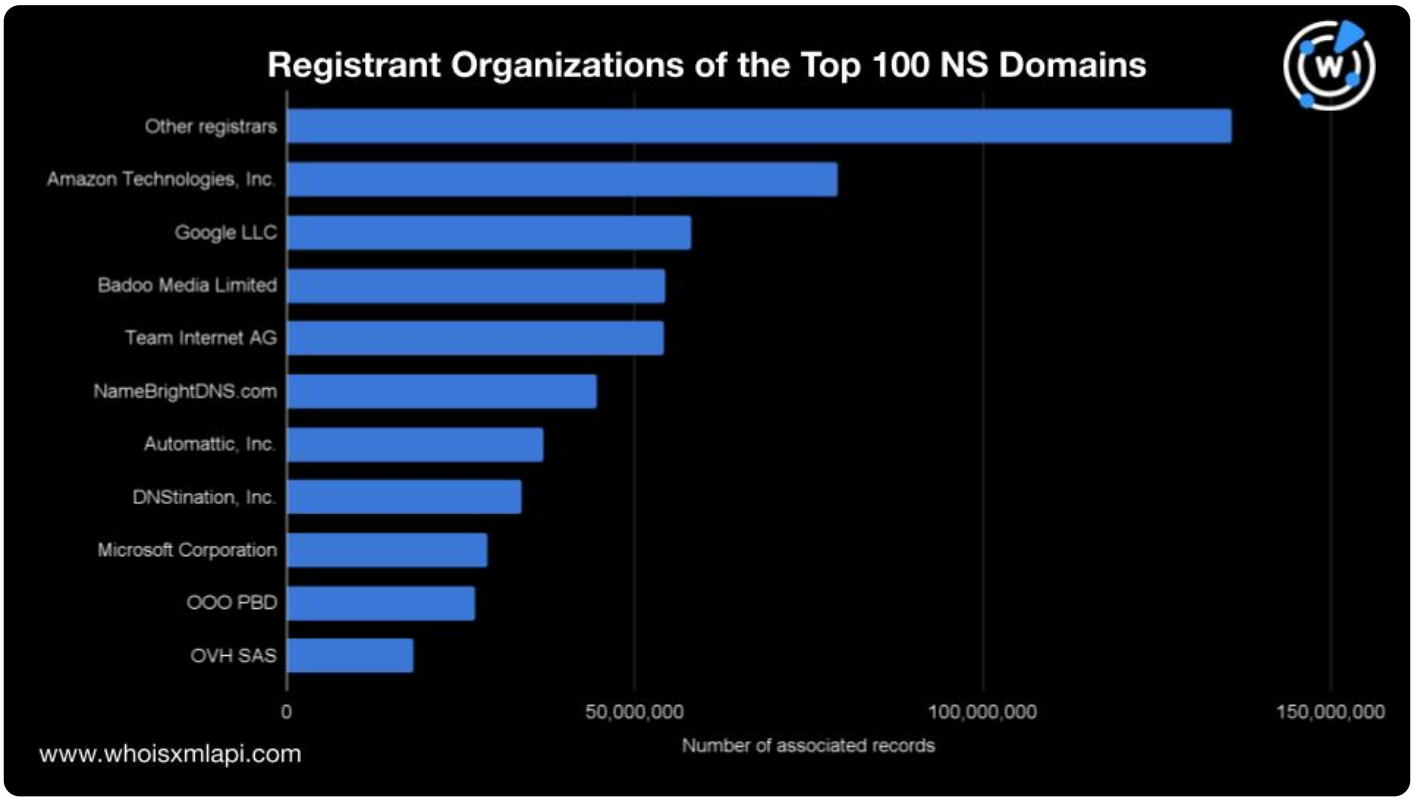
Zooming in on the attributable NS records, we found that they were distributed among 11 organizations. That means an average of 30 million NS records per NS provider.

However, Amazon Technologies, Inc. accounted for more than the average, with 74.3 million or

7.40% of the NS records using the top 100 FQDNs and 22% of the attributable records. It was followed by Team Internet AG (5.38%); NameBrightDNS.com (3.76%); DNStination, Inc. (3.36%); Badoo Media Limited (3%); Microsoft Corporation (2.8%); OOO PBD (2.68%); Automattic, Inc. (2.61%); OVH SAS (0.92%); Newfold Digital, Inc. (0.63%); and Internet CZ A.S. (0.38%).

Several of these organizations offer domain parking services, which shows domain parking' prevalence. The NSs they managed appeared in more than 171 million NS records.

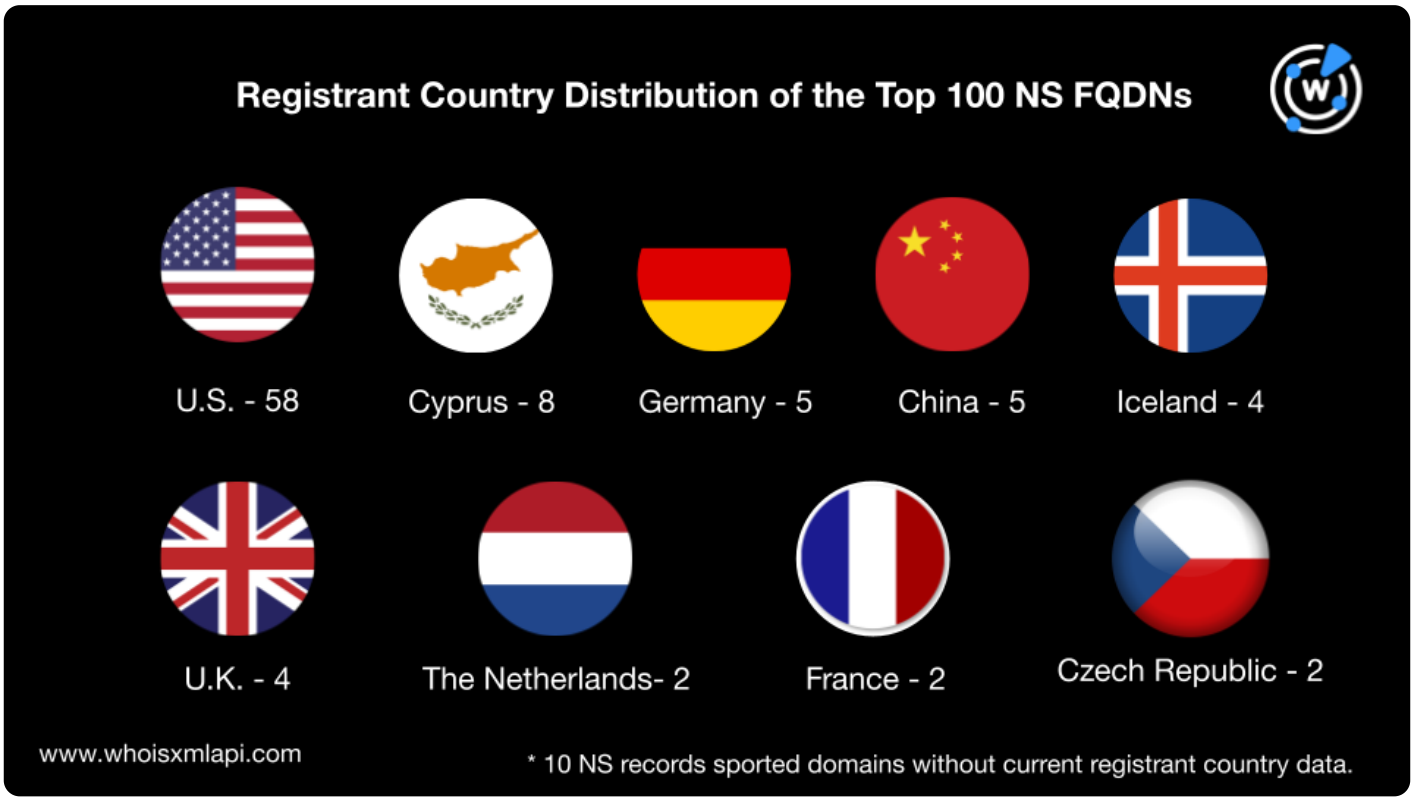
Moving the analysis to the top 100 NS domains, we found that Amazon Technologies, Inc. also emerged as the top registrant organization, along with 33 others. Unlike the NS FQDNs' registrant organizations, however, Google LLC came in second, followed by Badoo Media Limited; Team Internet AG; NameBrightDNS.com; Automattic, Inc.; DNStination, Inc.; Microsoft Corporation; OOO PBD; and OVH SAS.



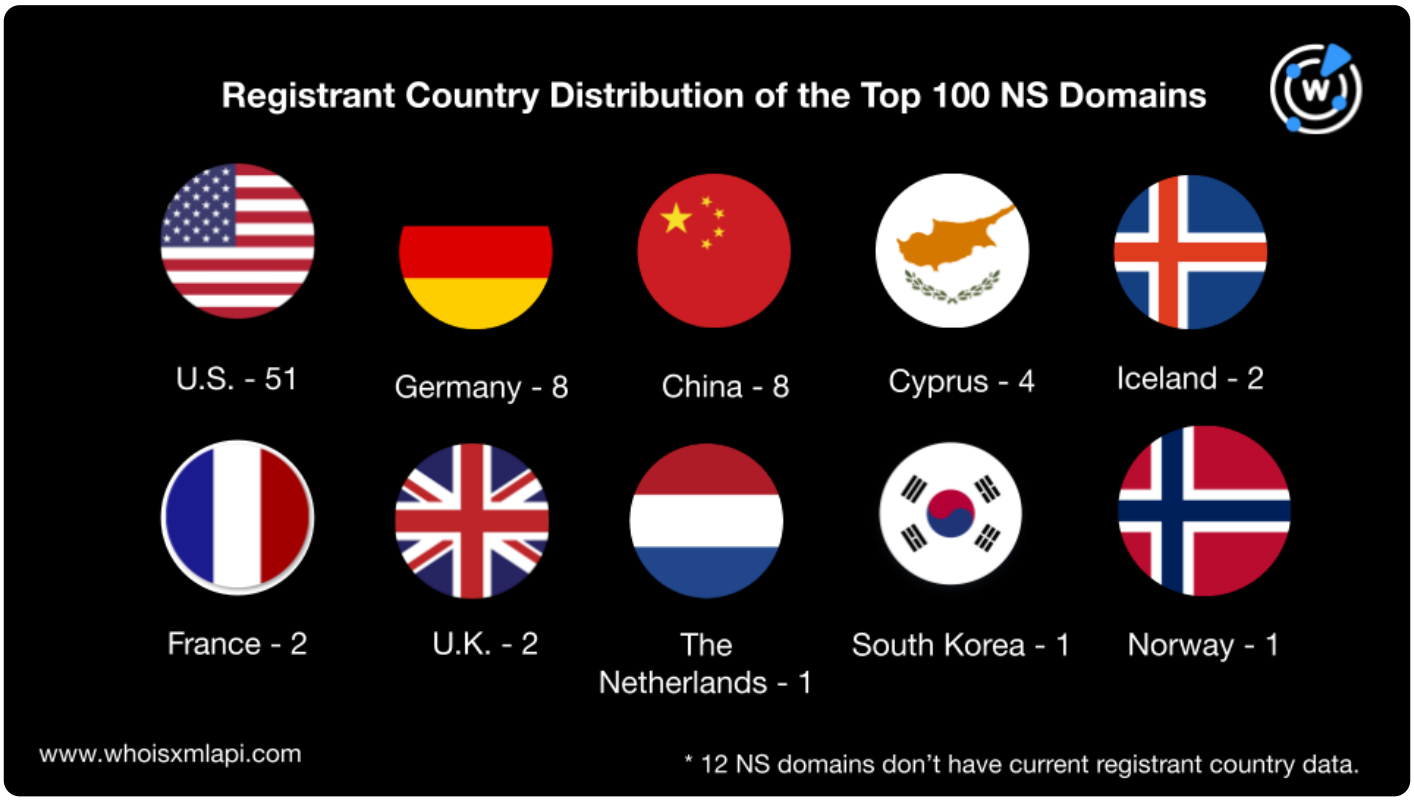
58 of the Top 100 Name Server Fully Qualified Domain Names Lead to Domains Registered in the U.S.

The registrant countries of the NS FQDNs and NS domains were then analyzed to determine their locations. We found that 58 of the most used NS FQDNs could be traced back to domains registered in the U.S., translating to 641 million NS records.

Eight NS FQDNs had root domains registered in Cyprus; five each in Germany and China; four each in Iceland and the U.K.; and two in the Netherlands, France, and the Czech Republic.



On the other hand, 51 of the top NS domains were registered in the U.S.; eight each in Germany and China; four in Cyprus; two each in Iceland, France, and the U.K.; and one each in the Netherlands, South Korea, and Norway.



Conclusion

Our analysis revealed some level of NS concentration, with 1 billion NS records pointing to 100 NSs that could be traced to only 20 unique registrants. That translates to about 50.3 million NS records per organization, most of which were unattributable due to WHOIS record privacy protection. They could serve as potential choke points that could affect Internet traffic.

In addition, we also noted that a couple of NS domains were flagged as malicious. They had redacted WHOIS details and accounted for more than 22 million NS records.

To learn more about the power of DNS intelligence to support cybersecurity use cases, request a demo with our sales team.