Who Runs Email Communications? A Look at the Prevalence of MX Records

Posted on July 3, 2024

Email remains a vital part of modern communication, with 347.3 billion emails sent and received daily worldwide in 2023. For each email to reach its intended recipient, mail exchange (MX) records direct it to the correct mail server.

While individual email users can create their own mail servers, most people use email services from established email service providers (ESPs) to avoid the complexity of running their own servers. These services typically provide storage, security features, and user-friendly interfaces, all without burdening users with maintenance.

However, some experts are concerned about the concentration of power within a limited number of companies controlling MX records. They warn of potential vulnerabilities if email routing relies heavily on just a handful of providers.

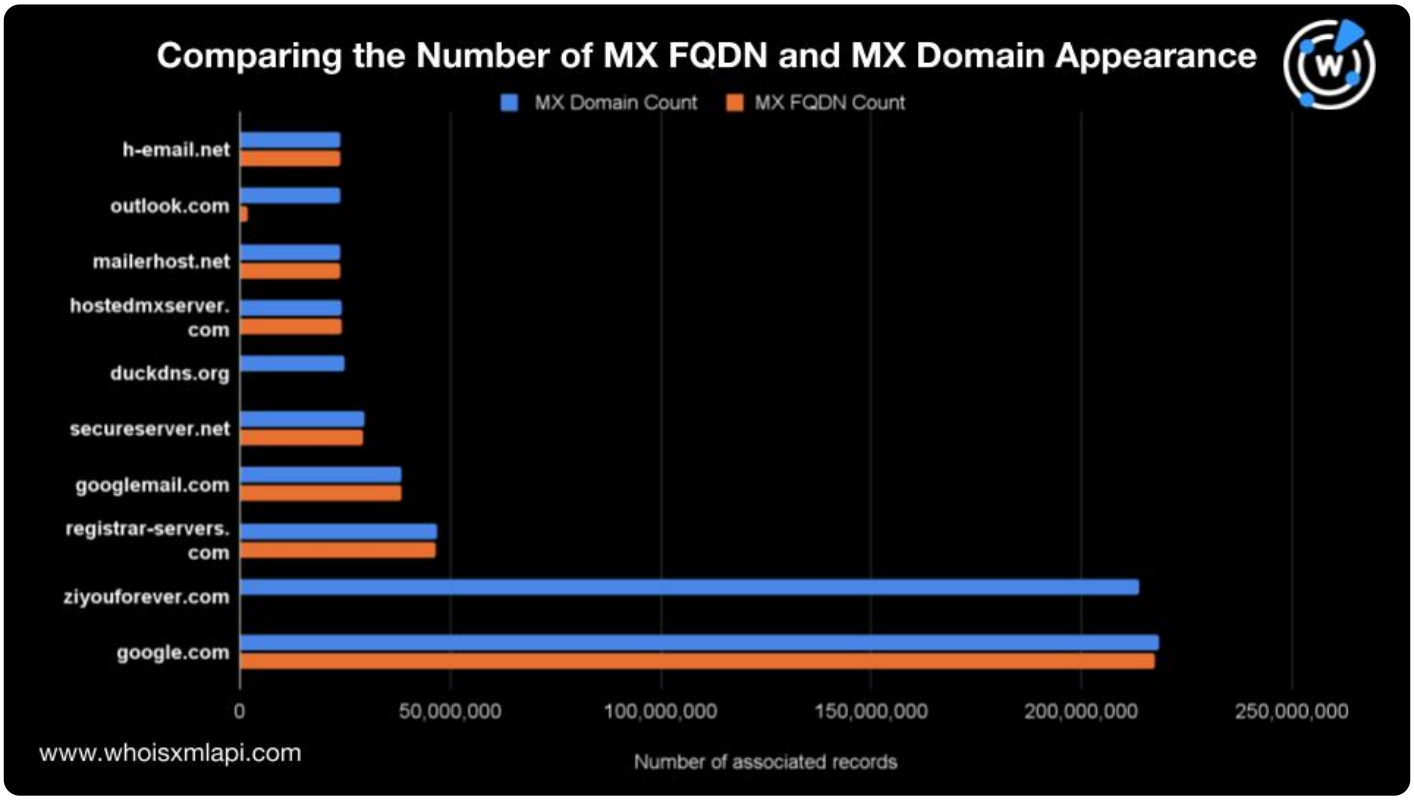
This post will explore the distribution of MX records, primarily focusing on the number of organizations controlling them and their geographical distribution.

Our research team gathered the top 100 MX fully qualified domain (FQDN) records like alt4.aspmx.l.google[.]com from a passive DNS database file dated 2 May 2024. These top FQDNs are the exact MX values appearing on more than 630.9 million MX records. We obtained their WHOIS registration details and zoomed in on the registrant organization and country fields. We also obtained the top 100 MX domains or the most recurring root domain names like google[.]com that appeared in the same downloaded file.

Disparity between Root Domain Use and FQDN Prevalence

Comparing the number of times the top 100 MX FQDNs and top 100 MX domains appeared in our

dataset brought to light interesting facts. For example, we noticed that although ziyouforever[.]com and duckdns[.]org are among the top 10 most used MX root domains, none of their FQDNs made it to the top 100.

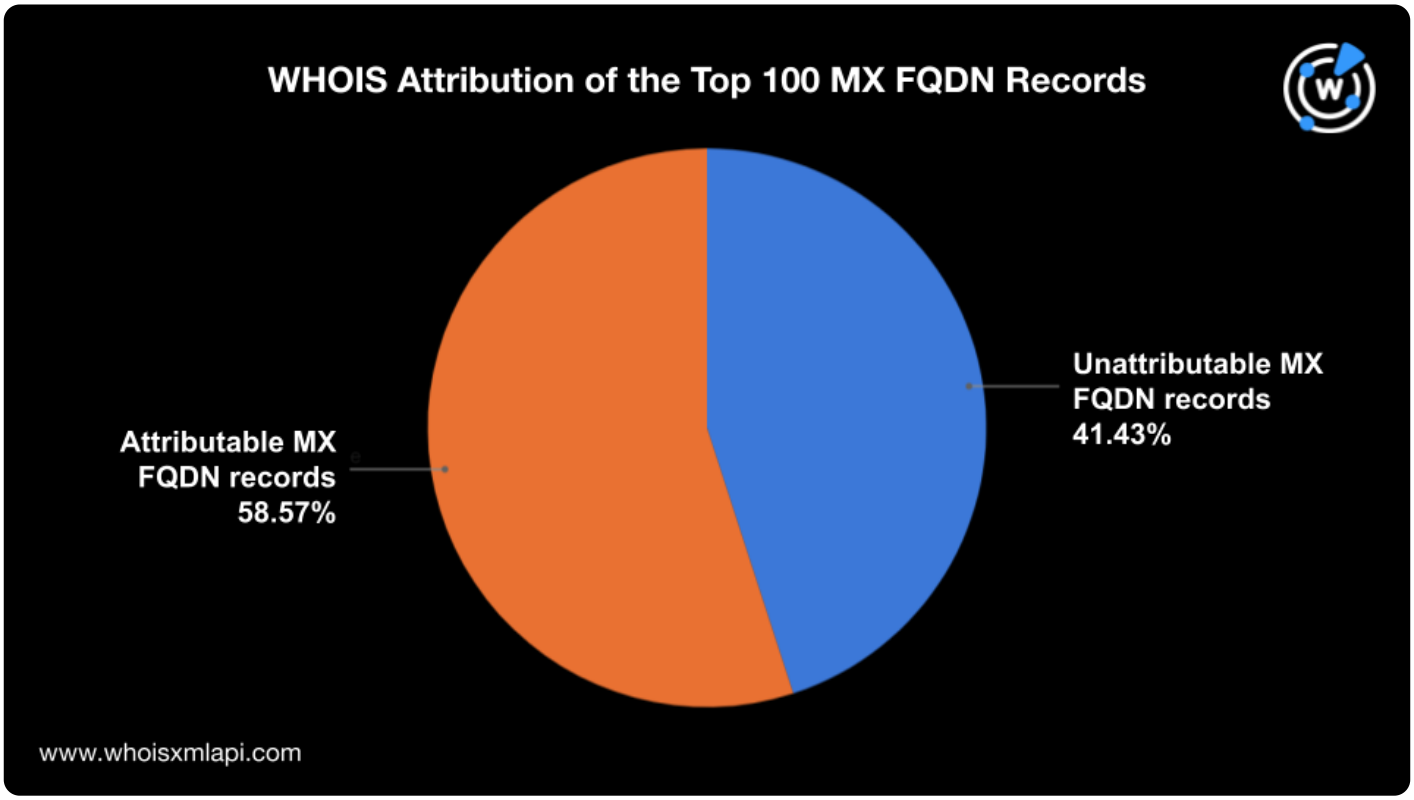


This finding could point to certain hosting providers offering custom MX server services where users can use the root domains to create subdomains that would serve as their MX FQDNs.

However, the second most used MX domain ziyouforever[.]com is another story. Past reports said the domain could be part of a network that provides DNS tunneling services to people in countries with restricted Internet access. If that is true, then the 213 million MX records using this root domain could be involved in DNS tunneling.

32% of the Top 100 MX Records Lead to Privacy-Protected Domains

The WHOIS registrant organization details of the top 100 MX FQDN records point to 25 unique organizations. However, the registrant organizations of 32.45% of the MX records are protected by various privacy service providers. In addition, 8.98% of the most used MX FQDNs did not specify their registrant organizations. That makes more than 261.3 million or 41.43% of the top 100 MX FQDN records unattributable to specific mail providers.



Looking at the top 100 MX domains, we arrived at a higher figure. About 55.6% of the domains could not be publicly attributed to specific organizations.

Google Controls Nearly 50% of the Top 100 MX Records

Focusing our attention to the attributable MX records, we found that they are under 17 different organizations. To put that into perspective, more than 369 million MX records are controlled by 17 ESPs. That means an average of about 21 million MX records per provider.

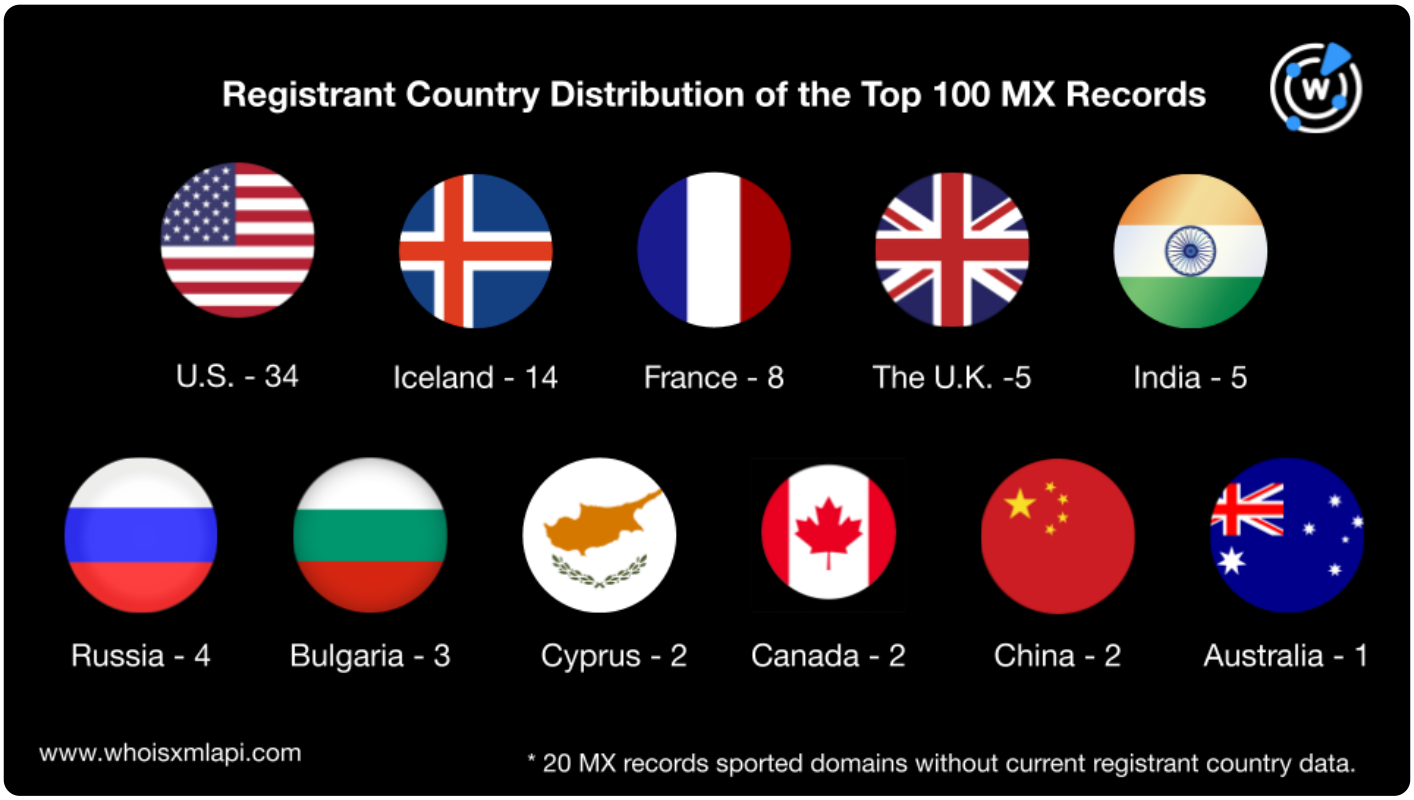
However, when it comes to the actual distribution of MX records, we found that Google LLC controls more than 255.8 million or 40.55% of the MX records. Also, we found that five of the top 10 MX records were Google mail servers.

On the other hand, GoDaddy Operating Company LLC and Appian Corporation followed with 4.64% (more than 29.2 million MX records) and 3.33% (more than 21 million) shares, respectively.

The number of organizations is higher for the top 100 MX domains. The attributable domains, which accounted for more than 440 million MX records, were spread across 39 ESPs. Google LLC and GoDaddy Operating Company LLC were still the top 2 providers with 25.91% and 2.97% shares, respectively.

34 of the Top 100 MX Records Lead to Domains Registered in the U.S.

We then analyzed the domain registrant country details of the MX records to identify theirlocations. We found that 34 of the most used MX records trace back to domains registered in theU.S., 14 in Iceland, eight in France, five each in the U.K. and India, and four in Russia. The rest ofthe countries included Cyprus, Canada, and China (two each) and Australia (one). Twenty MXrecords sported domains that didn't have current registrant country data.



The top 100 MX domains were also mostly registered in the U.S. To be exact, 33 domains could be traced to the U.S., six each to the U.K. and Germany, and five each to Iceland and Canada. A total of 23 MX domains didn't have current registrant country data, while the remaining 22 were distributed across 15 other countries.

Conclusion

Analyzing the WHOIS registration details of the most used MX servers provided evidence of concentration. The data suggests a limited number of organizations control a significant portion of the most used MX servers. It's also interesting to note the suspicious association of several MX records with certain MX domains and FQDNs, including the 24 million MX records we found containing a malicious MX FQDN.

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