メールのやりとりは誰が管理？
MXレコードの現状を調査

現代のコミュニケーションにおいて、電子メールは非常に重要な役割を果たしています。2023年には世界中で毎日3,473億通のメールが送受信されました。それぞれのメールを意図した宛先に届けるため、DNSではMail Exchanger（MX）レコードによってメール転送先のメールサーバーを指定しています。

メールサーバーはユーザーが独自に作成することもできますが、ほとんどの人は、複雑なサーバー運用を避けてメールサービスプロバイダー（ESP）のサービスを利用しています。ESPのサービスでは通常、ストレージ、セキュリティ機能、使いやすいインターフェースを全て提供しており、ユーザーにメンテナンスの負担をかけません。

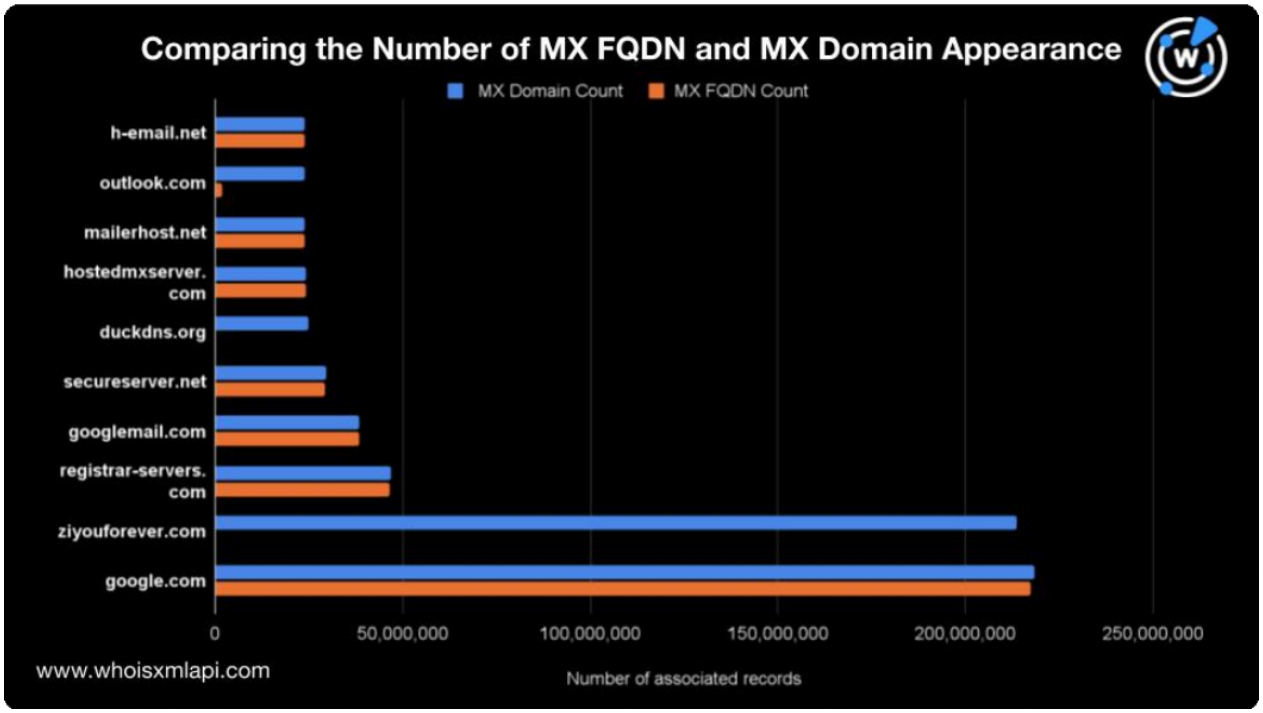
ただ、メールサーバーを管理するESPの数が限られていることから、集中化を懸念する専門家もいます。メールの経路が少数のプロバイダーに大きく依存した状態は潜在的な脆弱性になる、と彼らは警告しています。

この記事では、MXレコードの現状について、主にメールサーバーを管理している組織の数と地理的分布に焦点を当てて分析します。

当社の研究チームは、2024年5月2日時点のパッシブDNSデータベースファイルに収録されていたMXレコードから、転送先メールサーバーのホスト名として最も多く指定されていた完全修飾ドメイン名（FQDN。例：alt4.aspmx.l.google[.]com）の上位100件を集めました。これらの上位FQDNは、6億3,090万件を超えるMXレコードにMX値として書かれていたものです。当社はそれらFQDNのWHOIS情報を入手し、ドメイン名登録者の組織と国に注目しました。また、同じパッシブDNSデータベースファイルのMXレコードで最も多く見られた上位100のドメイン名（サブドメインを含まないルートドメイン。例：google[.]com）も調べました。

ルートドメインとFQDNの利用状況の違い

上位100のFQDNと上位100のルートドメインが当社のパッシブDNSデータベースファイルに見られた数を比較したところ、興味深い事実が明らかになりました。例えば、ziyouforever[.]comとduckdns[.]orgはMXで最も多く見られたルートドメインのトップ10に入っています。しかし、それらのMXレコードで指定されていたメールサーバーのFQDNは、いずれもトップ100以内にも入っていませんでした。

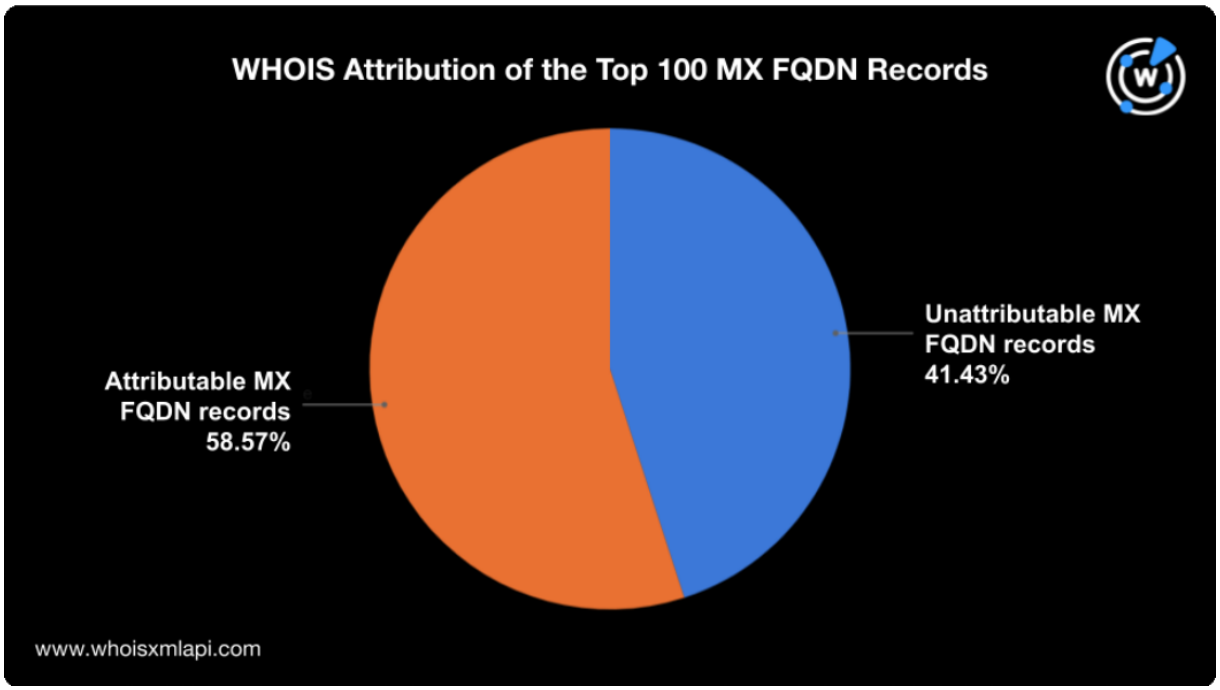


これは、カスタムMXサーバーサービスを提供するホスティングプロバイダーの存在を示唆しているのかもしれません。そうしたサービスでは、ユーザーがルートドメインを使ってサブドメインを作成し、MXのFQDNとして機能させることができるのです。

しかし、MXに2番目に多く見られたziyouforever[.]comというドメイン名では事情が異なります。このドメイン名については、インターネットアクセスが制限されている国の人々向けにDNSトンネリングをサービスとして提供しているネットワークの一部かもしれない、と過去に報道されたことがあります。

トップ100 MXレコードの32%はプライバシー保護ドメイン

WHOISで調べたところ、MXで上位100に入るFQDNの登録者組織の情報から、25のユニークなドメイン名が特定されました。ただし、32.45%のFQDNについては、プライバシーサービスプロバイダーによってWHOISデータが保護されており、登録者の組織名がわかりませんでした。加えて、8.98%のFQDNは、登録者の組織名を指定していませんでした。つまり、トップ100のFQDNが指定されていたMXレコードのうち2億6,130件超（調査対象全体の41.43%）については、メールサービスプロバイダーを特定できなかったのです。



また、MXレコードのルートドメインのトップ100を調べたところ、その約55.6%は特定の組織への帰属を確認できませんでした。

Googleが上位100のMXレコードの約50%を管理

帰属先が特定できた3億6,900万件超のFQDNは、17のESPによって管理されていました。つまり、1プロバイダーあたり平均約2,100万のFQDNを管理していることになります。

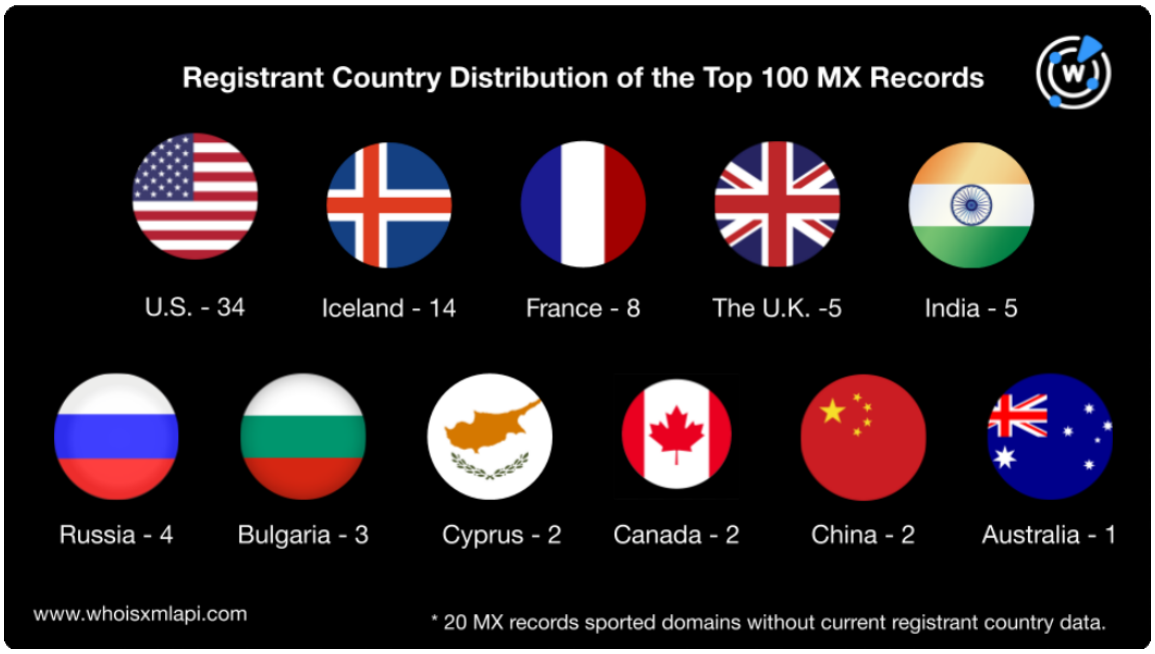
ただ、実際はGoogle LLCが2億5,580万件超（40.55%）を1社で管理していました。また、トップ10に入るFQDNのうち5件がGoogleのメールサーバーであることも判明しました。

Googleの次にシェアが大きかったGoDaddy Operating Company LLCとAppian Corporationの割合は、それぞれ4.64%（2,920万件超）と3.33%（2,100万超）でした。

MXで最も多く見られた上位100のルートドメインについても調べてみました。その結果、4億4,000万件超のドメインについては帰属先を特定でき、ESPは39社が判明しました。ESPの中ではGoogle LLCとGoDaddy Operating Company LLCがそれぞれ25.91%と2.97%のシェアを占め、FQDNの場合と同様にこの2社がトップ2となっていました。

トップ100のFQDNのうち34件は米国で登録されたドメイン

次に、MXレコード（FQDN）のドメイン名登録者の国に関するデータを分析し、所在地を特定しました。34件は米国、14件はアイスランド、8件はフランス、5件はそれぞれ英国とインド、4件はロシアで登録されたものでした。その他の国としては、キプロス、カナダおよび中国（各2件）、オーストラリア（1件）が判明しました。また、20件のMXレコードには、登録者の国のデータがないドメイン名のFQDNが指定されていました。



また、MXレコードのルートドメインのうち33件は米国で登録されたものでした。その他、英国とドイツで各6件、アイスランドとカナダで各5件が登録されていました。他方、23件のルートドメインについては、登録者の国のデータがありませんでした。そして、残りの22件は15カ国に分散していました。

まとめ

今回、MXレコードで最も多く指定されているメールサーバーのWHOISデータを分析することで、メールサーバーの管理が少数のESPに集中していることを確認できました。また、悪意あるFQDNを含むMXレコードを2,400万件検出したことなどから、一部のMXレコードと特定のルートドメインおよびFQDNの間に不審な関連性があることもわかりました。

組織のサイバーセキュリティ対策を支援する当社のDNSインテリジェンスにご興味をお持ちいただけましたら、こちらのページから当社のセールスチームにお気軽にご連絡ください。