ドメイン名動向ハイライト：2023年9月

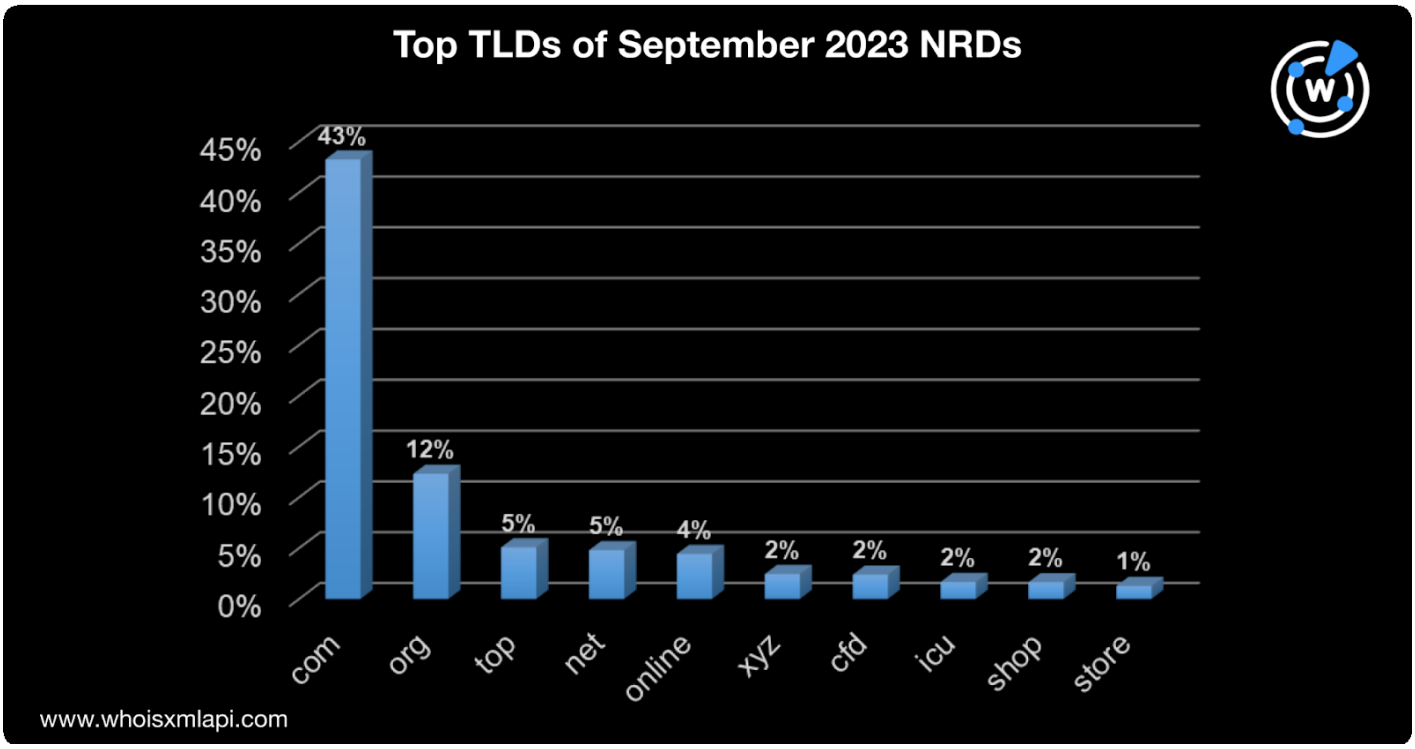
WhoisXML APIの研究者がこのほど、2023年9月1日から30日の間に新規登録された数百万のドメイン名から無作為に30,000個を抽出し、WHOISデータ、登録者の国、レジストラ、TLDの共通点を調べました。

また、ドメイン名の文字列の使用状況から潜在的な新傾向を明らかにするとともに、予測インテリジェンスソースを活用して9月に最も模倣されたブランドや文字列を特定しました。本調査の結果と、DNS、IPアドレスおよびドメイン名のインテリジェンスを用いてWhoisXML APIが作成した脅威レポートへのリンクを以下に示します。

9月の新規登録ドメイン名（NRD）をクローズアップ

TLDの分布

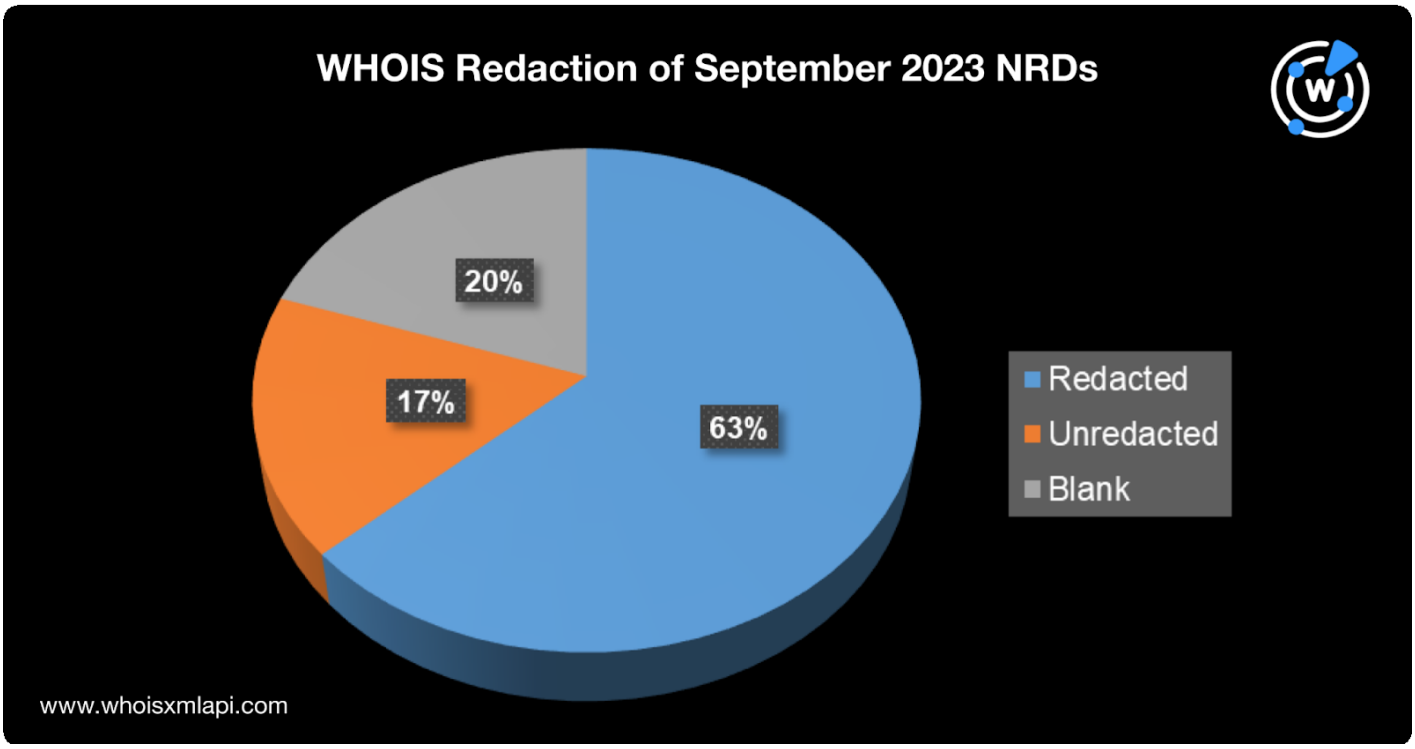
2023年9月のTLDトップ10は前月とほぼ同じでした。最も人気があったのは.comで、NRD登録数全体の43%を占めました。.comに続き、.org（12%）、.top（5%）、.net（5%）、.online（4%）、.xyz（2%）、.cfd（2%）、.icu（2%）、.shop（2%）、.store（1%）の順となりました。



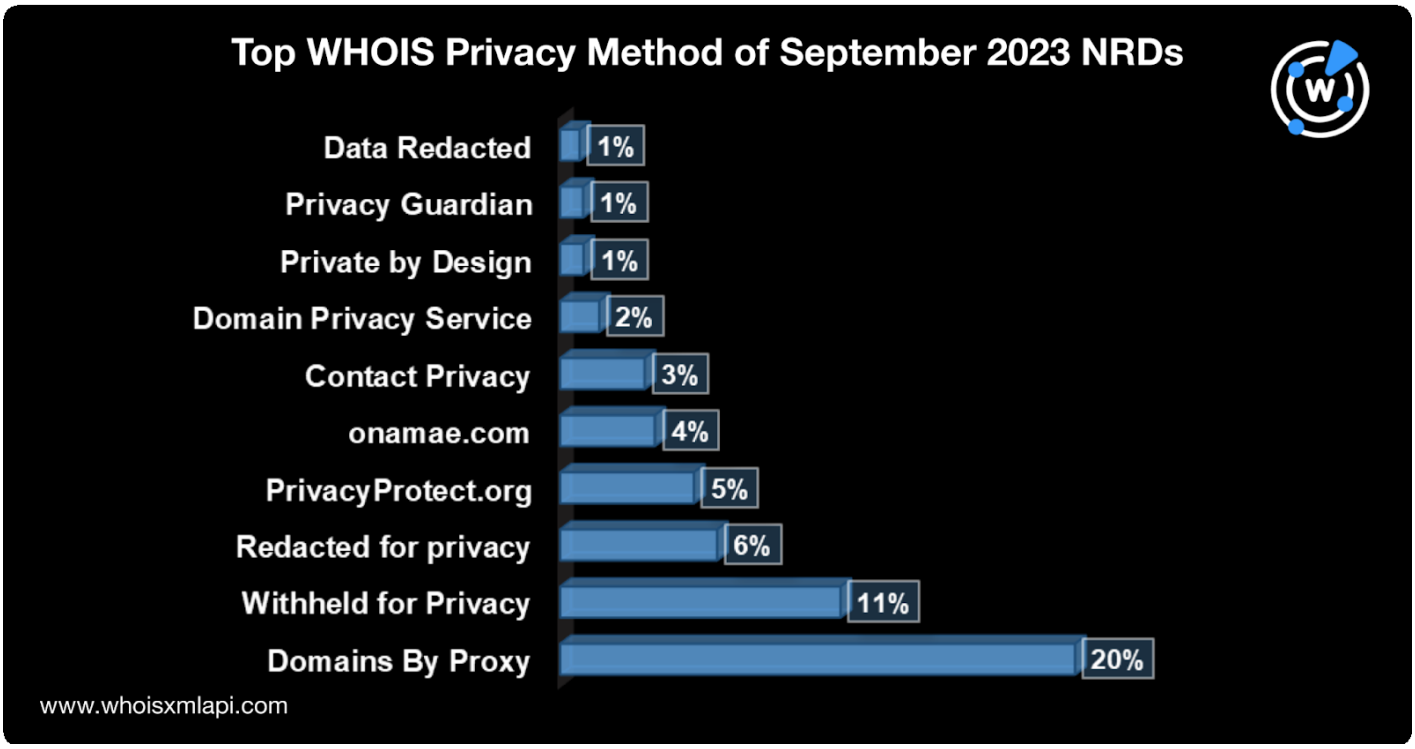
NRDの79%は上位10 TLDのドメイン名でした。残りは630を超える他のTLDに分散しています。

WHOISデータの非公開化

新規登録ドメイン名のうち約63%では、WHOISレコードが非公開化されていました。登録者の組織名が公開されていたのはわずか17%で、約20%はそのフィールドが空白でした。



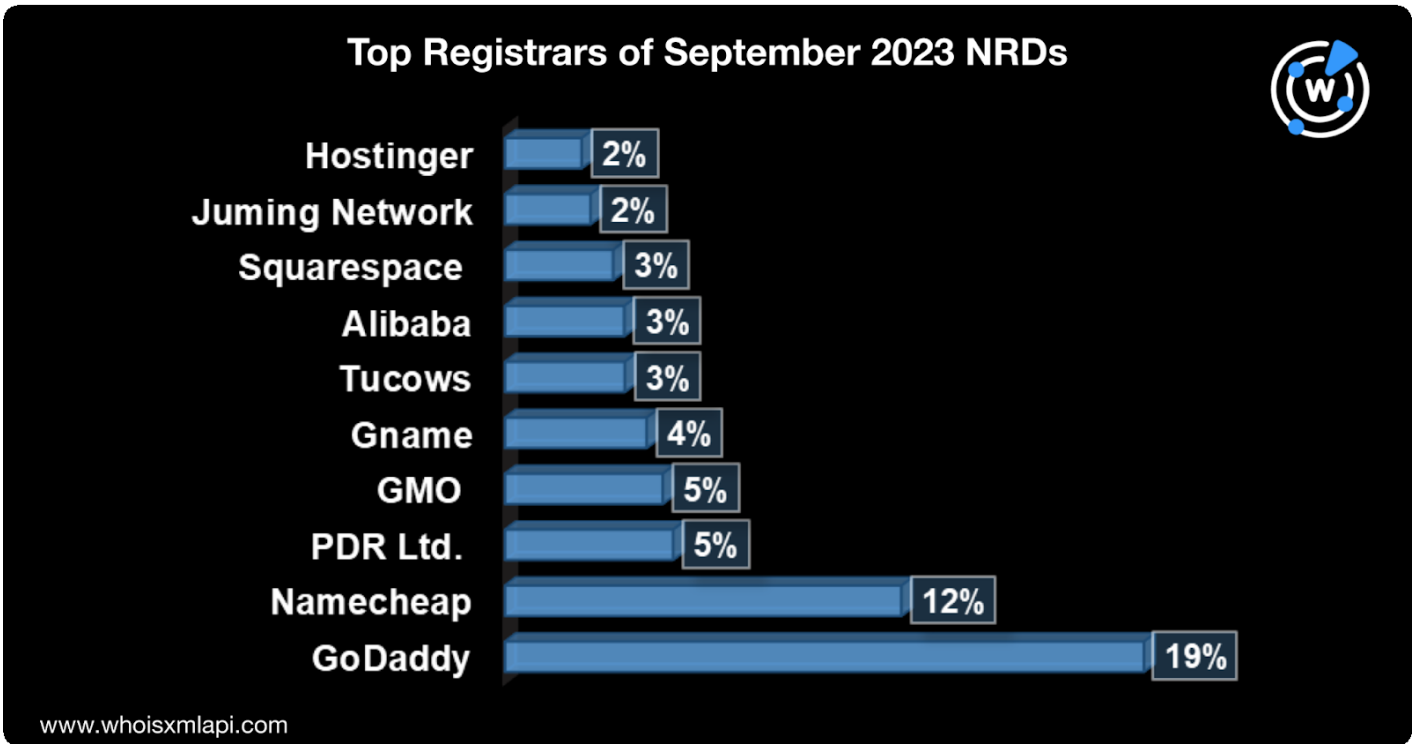
最も人気のあったプライバシーサービスプロバイダーはDomains By Proxyで、NRDの20％で使われていました。次いで多かったのはWithheld for Privacy（11%）、Privacy Protect（5%）、 お名前（4%）、Contact Privacy（3%）、Domain Privacy Service（2%）、Private by Design（1%）、PrivacyGuardian.org（1%）でした。



複数のNRDでは、その登録者組織名欄に**Redacted for privacy**、**Data Redacted**などのラベルが含まれていました。

レジストラの分布

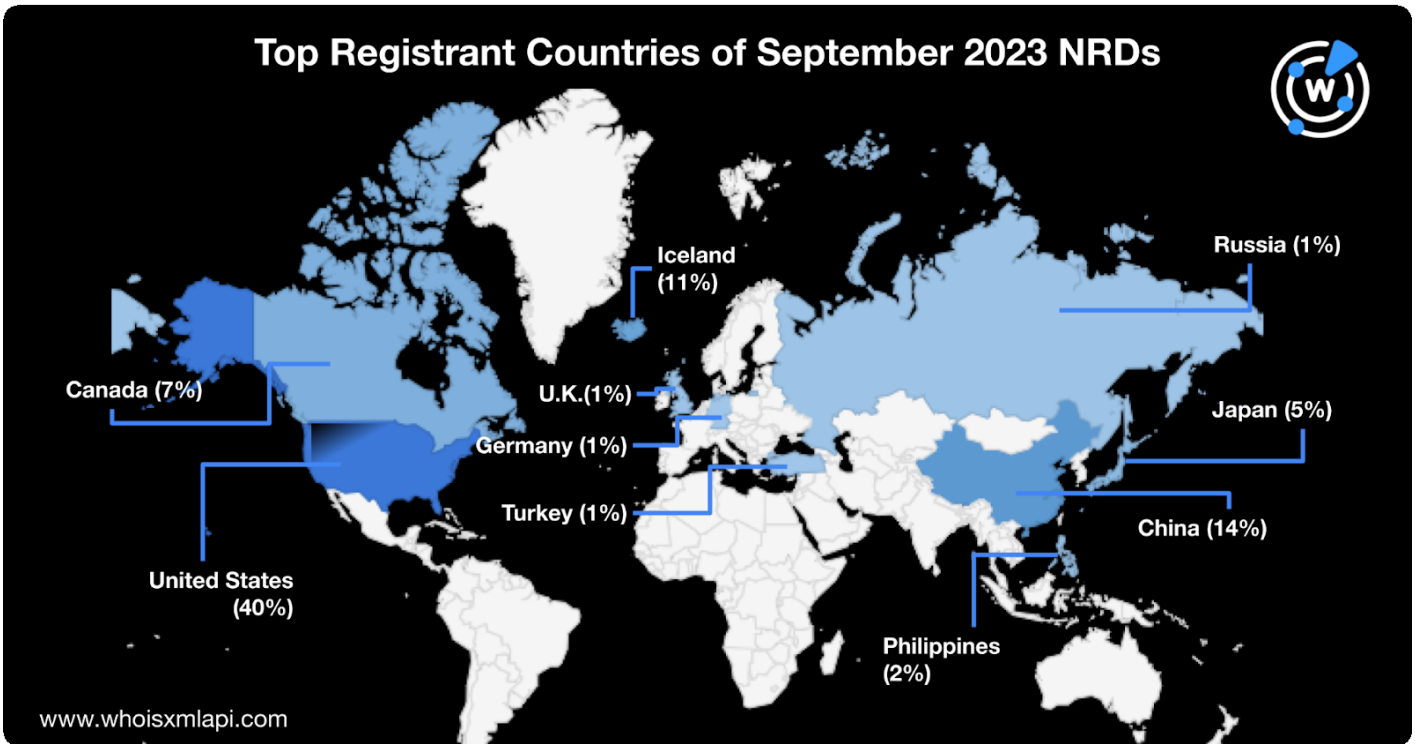
データによると、GoDaddyはNRD登録数の19%を占め、トップレジストラの座を維持しました。次いで多かったのは、Namecheap（12%）、PDR Ltd.（5%）、GMOインターネット（5%）、Gname（4%）、Tucows（3%）、Alibaba（3%）、Squarespace（3%）、Juming Network（2%）、Hostinger（2%）でした。



トップ10のレジストラが登録総数の58%を占めました。残りのドメイン名は、他の580を超えるレジストラに分散しています。

登録数上位の国

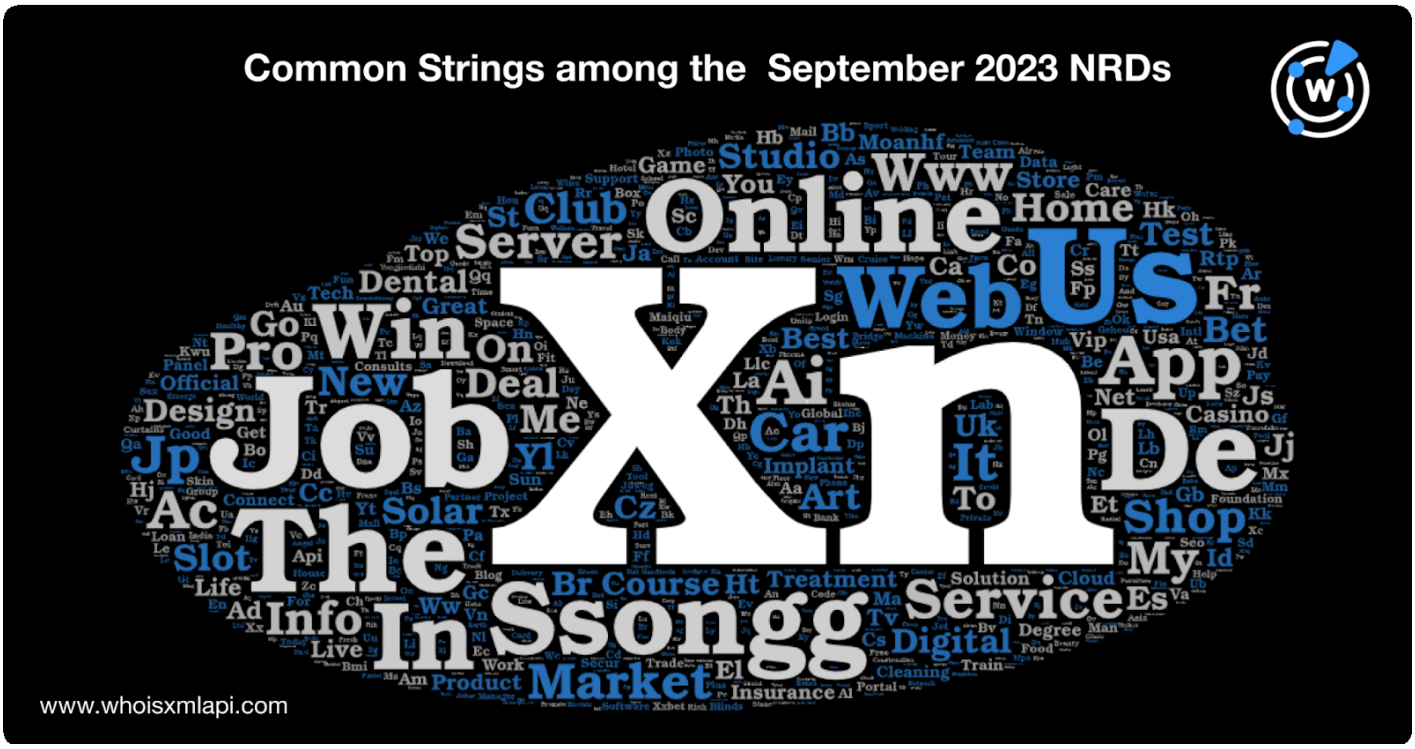
ドメイン名の新規登録が最も多く行われた国は先月に引き続き米国で、全体の40%を占めました。そして、中国（14%）とアイスランド（11%）、カナダ（7%）、日本（5%）、フィリピン（2%）が米国に続きました。さらに、ロシア、英国、ドイツ、トルコがそれぞれ1%以下でトップ10入りしています。



登録者数上位10カ国が総登録数の83 %を占めました。残りのドメイン名は115を超える他の国に分散しています。

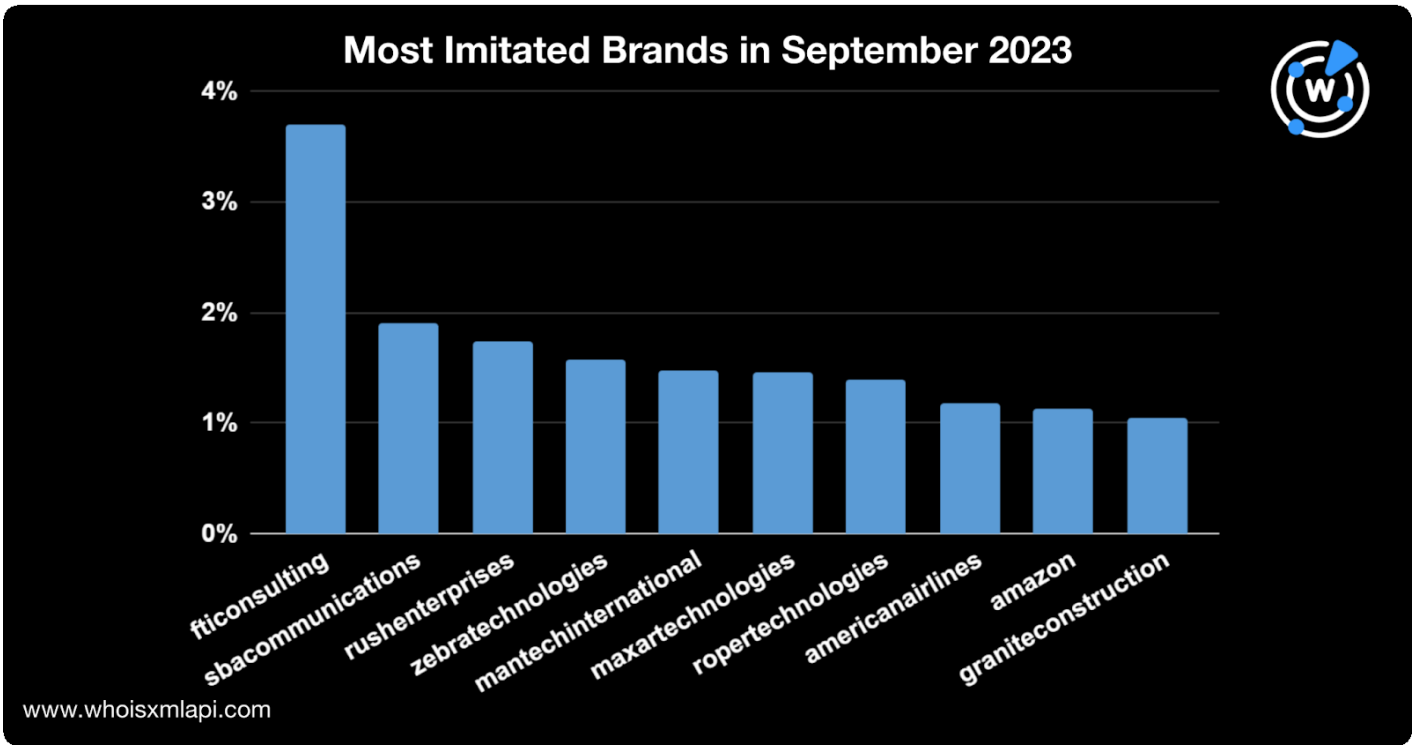
第2レベルドメイン（SLD）に共通して見られる文字列

9月にNRDの文字列として最も多く見られた単語は、インターネットやテクノロジーに関連するものでした。例えば、**web**、**online**、**www**、**app**、**service**などです。**market**、 **job**、**home**もよく使われていました。また、**xn**の人気は、国際化ドメイン名（IDN）が依然としてポピュラーであることを示唆しています。



Early Warning Phishing Feedによるフィッシングの早期検出

Early Warning Phishing Feedのサンプルとして数千のドメイン名を抽出し分析したところ、最も頻繁に出現した文字列は**fticonsulting**で、不審なドメイン名のほぼ**4%**に含まれていました。他によく見られた文字列としては、**sbacommunications**、**rushenterprises**、**zebratechnologies**、**nantechinternational**、**maxartechnologies**、**ropertechnologies**、**americanairlines**、**amazon**および**graniteconstruction**がありました。



DNSのレンズで見るサイバーセキュリティ

当社が9月に公開した脅威リサーチ報告の一部を以下にご紹介します。

- **Decoy DogはDNSに痕跡を残さないほど狡猾か？**：WhoisXML APIの研究者がDecoy Dogに関連するセキュリティ侵害インジケーター（IoC）を詳細に調査し、共通のIPアドレスを使用しているドメイン名90個、共通の文字列を含むドメイン名2,000個あまりからなる数千のアーティファクトを新たに検出しました。

- **DNSでWoofLockerの実態を解明**：当社の研究者が、WoofLockerの8年間の活動期間中に報告された数百のIoCをDNSの観点から分析しました。その結果、IoCの専用IPホストの一部を共用する1,000個あまりの未公開ドメイン名を含むアーティファクトがさらに見つかりました。

- **DNS分析でIcedIDの実態をあぶり出す**：WhoisXML APIの調査により、IcedIDマルウェアとの関連が疑われるメールアドレスとドメイン名を含む70個あまりのアーティファクトが特定されました。

- **Smishing TriadがDNSに残した痕跡をたどる**：Smishing Triadの最新のキャンペーンに関与した可能性のある2,500個超のドメイン名を特定しました。これらのうち600個以上が、すでに悪意あるドメイン名として確認されています。

当社の過去の脅威レポートはこちらでご覧になれます。

今回のドメイン登録の分析や他のユースケースのサポートで使用した当社の商品につきましては、こちらまでお気軽にお問い合わせください。