ドメイン名動向ハイライト：2023年8月

投稿日 2023年9月28日

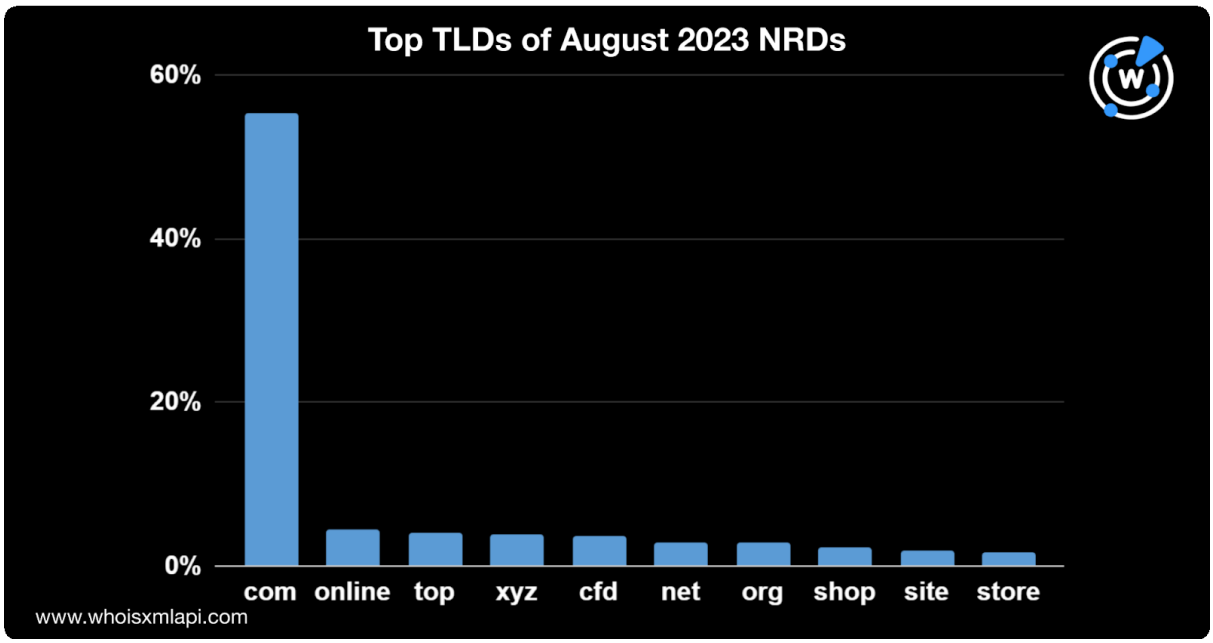
WhoisXML APIの研究者がこのたび、2023年8月1日から31日の間に新規登録された数百万のドメイン名から無作為に31,000個を抽出し、WHOISデータ、登録者の国、レジストラ、TLDの共通点を調べました。

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8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。

8月の新規登録ドメイン名（NRD）をクローズアップ

TLDの分布

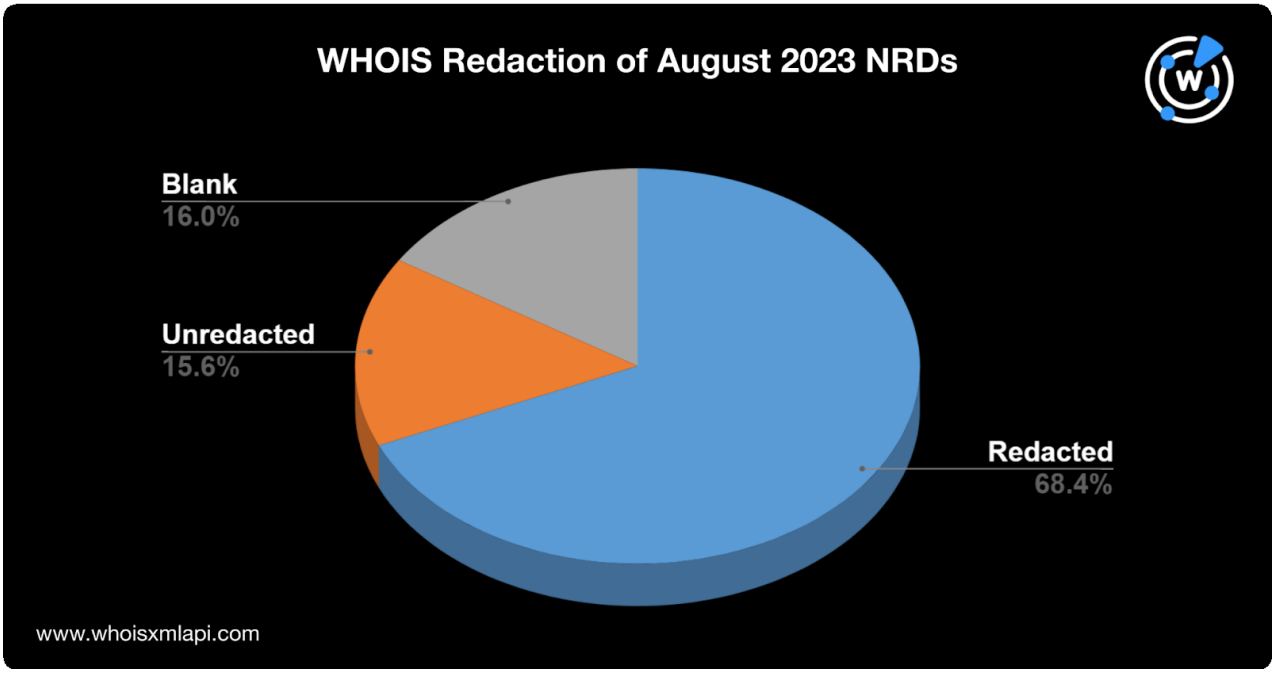
7月のトップ10 TLDのほとんどが8月も引き続き上位にランクインしました。.comは依然として最も多く利用されており、調査対象のドメイン名登録数全体の55%を占めました。下図の通り、.comに次いで.online（5%）、.top（4%）、.xyz（4%）、.cfd（4%）、.net（3%）、.org（3%）、.shop（2%）、.site（2%）、.store（2%）がトップ10に入りました。



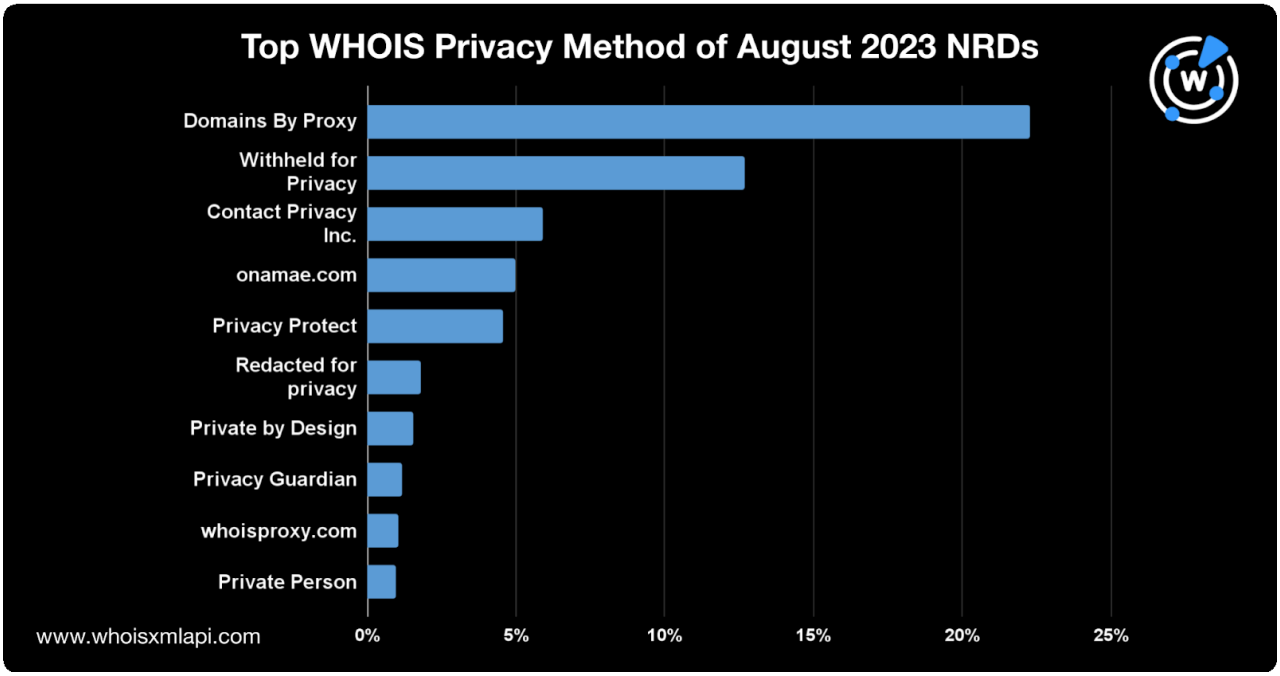
NRDの83%は上位10 TLDのドメイン名でした。残りは620を超える他のTLDに分散しています。

WHOISデータの非公開化

NRDの大半については、その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15.6%で、16%はそのフィールドが空白でした。



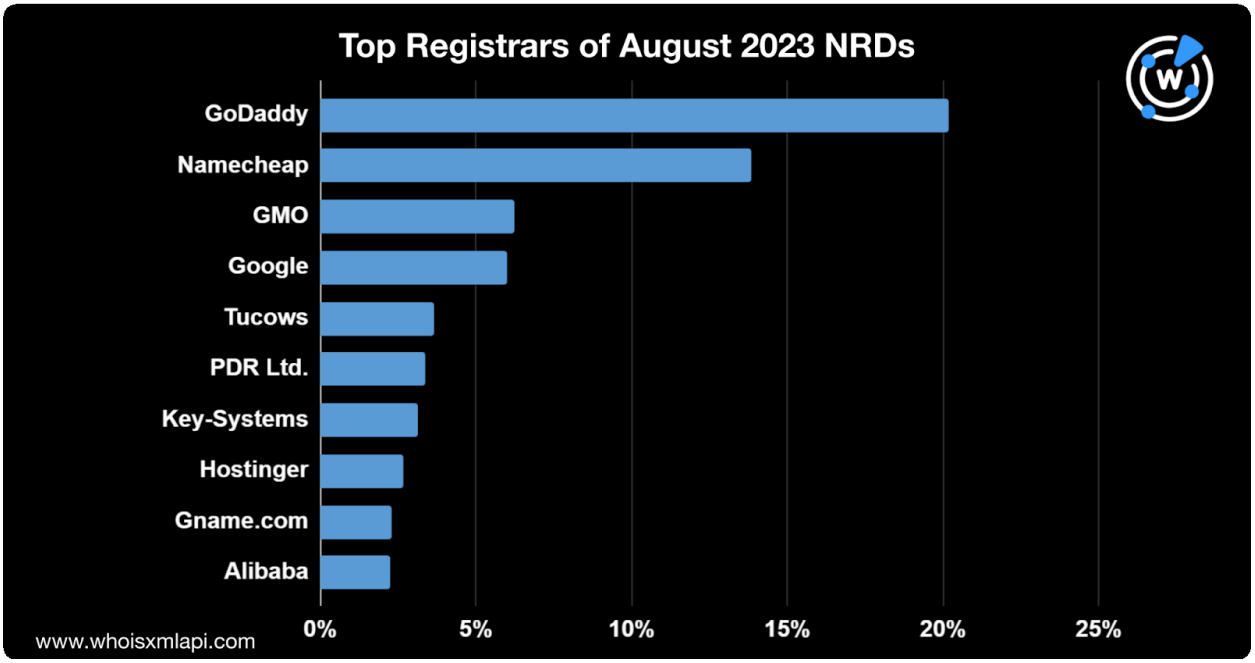
最も人気のあったプライバシーサービスプロバイダーは引き続きDomains By Proxyで、新規登録ドメイン名の22%が使っていました。次いで多かったのはWithheld for Privacy（13%）、Contact Privacy（6%）、お名前（5%）、Privacy Protect, LLC（5%）、Private by Design（2%）、PrivacyGuardian.org（1%）、WhoisSproxy（1%）でした。



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

レジストラの分布

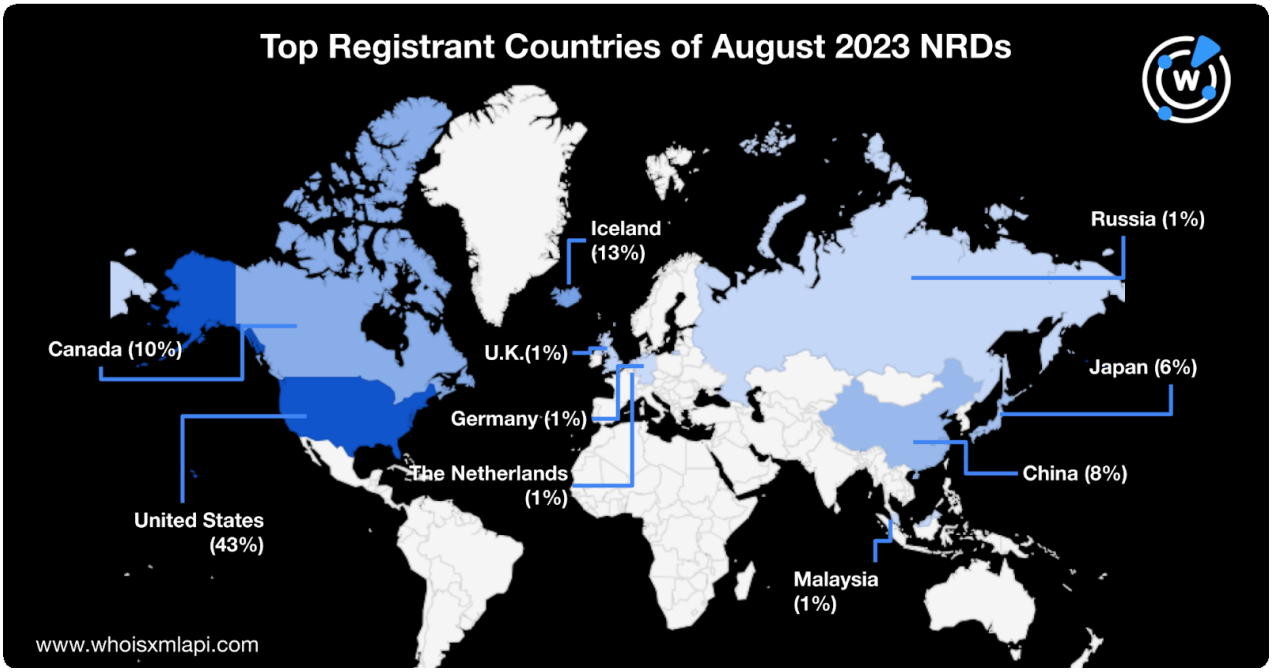
8月のNRD上位レジストラは7月と変わらず、GoDaddyが登録数の20%を占めて最多となりました。次いで多かったのは、Namecheap（14%）、Google（6%）、GMOインターネット（6%）、Tucows（4%）、PDR Ltd.（3%）、Key-Systems（3%）、Hostinger（3%）、Gname（2%）、Alibaba（2%）でした。



トップ10のレジストラがドメイン名登録総数の64%を占めました。残りのドメイン名は、他の400を超えるレジストラに分散していました。

登録数上位の国

8月はNRDの43%が米国で登録されました。そして、アイスランド（13%）とカナダ（10%）が米国に続きました。登録者が多く所在する国トップ10の残りは、中国（8%）、日本（6%）、英国（2%）、ロシア（1%）、マレーシア（1%）、オランダ（1%）、ドイツ（1%）となりました。



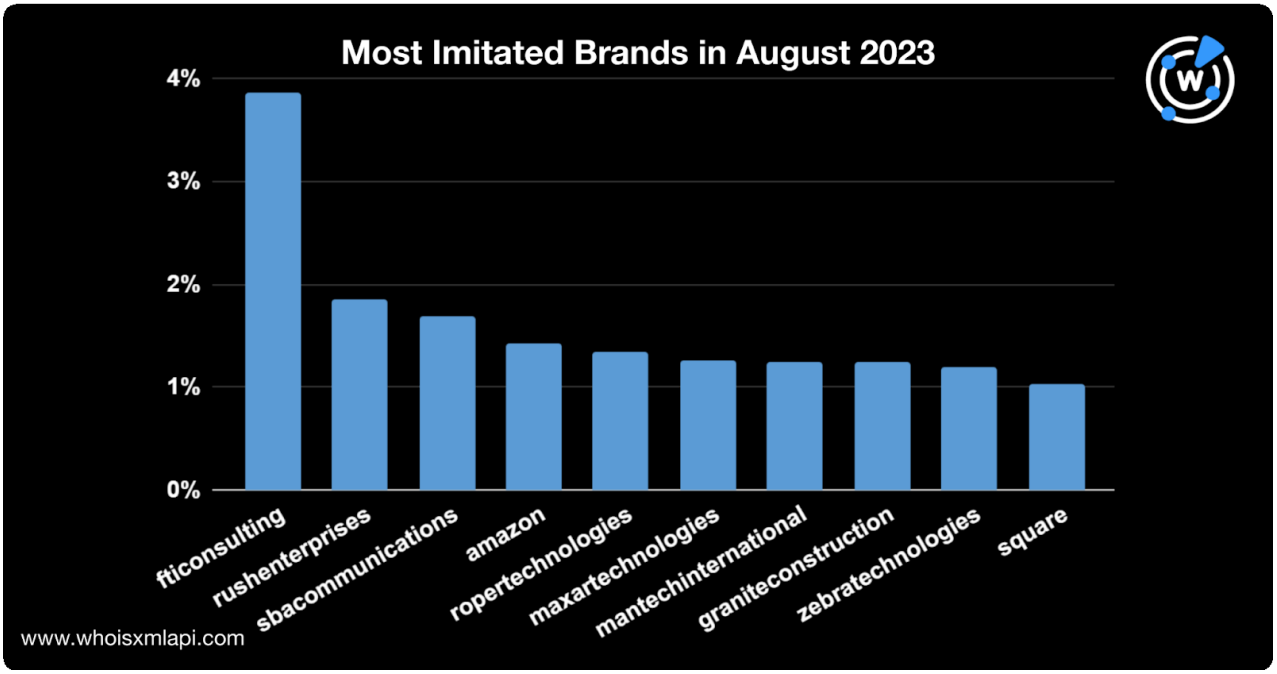
登録者数上位10カ国が調査対象のNRDの87%を占めました。残りのドメイン名は130を超える他の国に分散していました。

第2レベルドメイン（SLD）に共通して見られる文字列

8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、**app**、**online**、**service**、**digital**などです。**loan**、**job**、**home**も注目に値します。また、**xn**も引き続き多く見られました。国際化ドメイン名（IDN）が継続的に使用されていることがうかがえます。

Early Warning Phishing Feedによる早期検出

さらに、最も模倣されたブランドを特定するため、当社のEarly Warning Phishing Feedでフィッシングドメインとして検出した数千のドメイン名のサンプルを分析しました。データフィードで調べた495の検索文字列のうち最も多くのNRDに見られたのは**fticonsulting**で、サンプル全体の4%を占めました。次いで多かったのは**rushenterprises**（2%）、**sbacommunications**（2%）、そして**amazon**、**ropertechnologies**、**maxartechnologies**、**mantechinternational**、**graniteconstruction**、**zebratechnologies**、**square**（各1%）でした。



DNSのレンズで見るサイバーセキュリティ

当社が8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。

- **Redisは脅威アクターに狙われ続けるのか？**： WhoisXML APIの研究者が、「CVE-2022-0543」または「Redis Lua Sandbox Escape and Remote Code Execution Vulnerability 」として知られる脆弱性に関係したセキュリティ侵害インジケーター（IoC）を調査し、**redis**という文字列を含む20,000あまりのウェブプロパティを新たに検出しました。

- **WyrmSpy・DragonEggとAPT41の繋がりをDNSで発見**： 公開されているIoCを分析し、APT41とWyrmSpyおよびDragonEggの結びつきを特定しました。

- **JumpCloudサプライチェーン攻撃の痕跡をDNSで発見**：DNSインテリジェンスを駆使してJumpCloudサプライチェーン攻撃のIoCを詳しく調査し、潜在的に関連性のある数百ものアーティファクトを発見しました。

- **AIツールの人気は悪意あるキャンペーンの好機？**： WhoisXML APIとBayse Intelligence が共同で調査を実施し、2023年ベストAI生産性向上ツールのうち8つを標的にした攻撃と関連しているかもしれないウェブプロパティを特定しました。

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。