ドメイン名動向ハイライト：2023年4月

投稿日：2023年5月4日

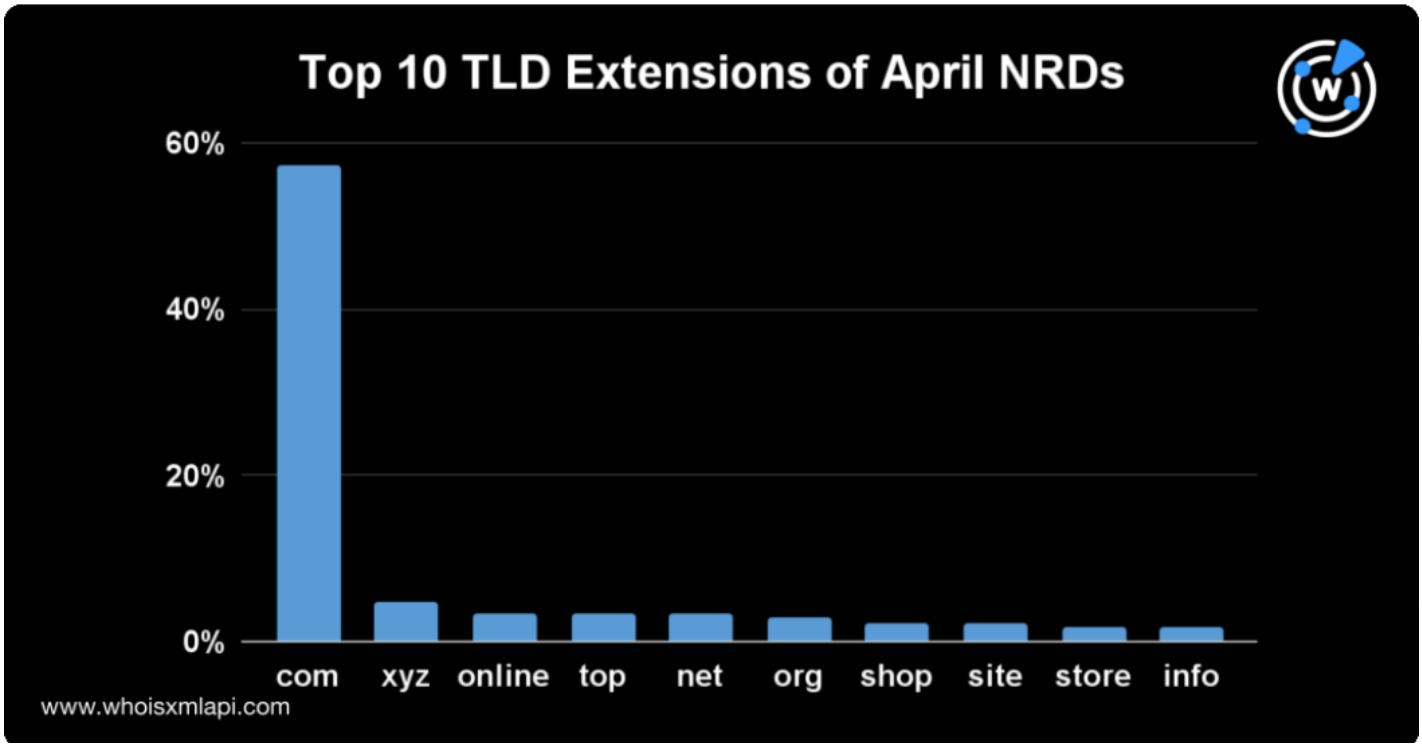
WhoisXML APIの研究者がこのほど、2023年4月1日から4月30日の間に登録された数百万のドメイン名のうち29,000個を無作為に抽出し、登録者の所在国、レジストラおよびTLDの共通点を明らかにしました。また、最もリスクの高い、あるいは最も悪用されているTLDのドメイン名登録数を調べるとともに、ドメイン名の文字列の使用状況を調査し、潜在的な新傾向を明らかにしました。

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作成した脅威レポートへのリンクを以下に示します。

4月の新規登録ドメイン名（NRD）をクローズアップ

TLDの分布

4月に最もNRD数が多かったTLDは引き続き.comで、全NRDの57%を占めました。2位以下のシェアは.comに大きく水をあけられ、.xyzで5%、.online、.top、.net、.orgでそれぞれ3%、.infoが2%となりました。eコマースに特化した.shop、.site、.storeもトップ10に入りましたが、それぞれ総登録数の2%でした。

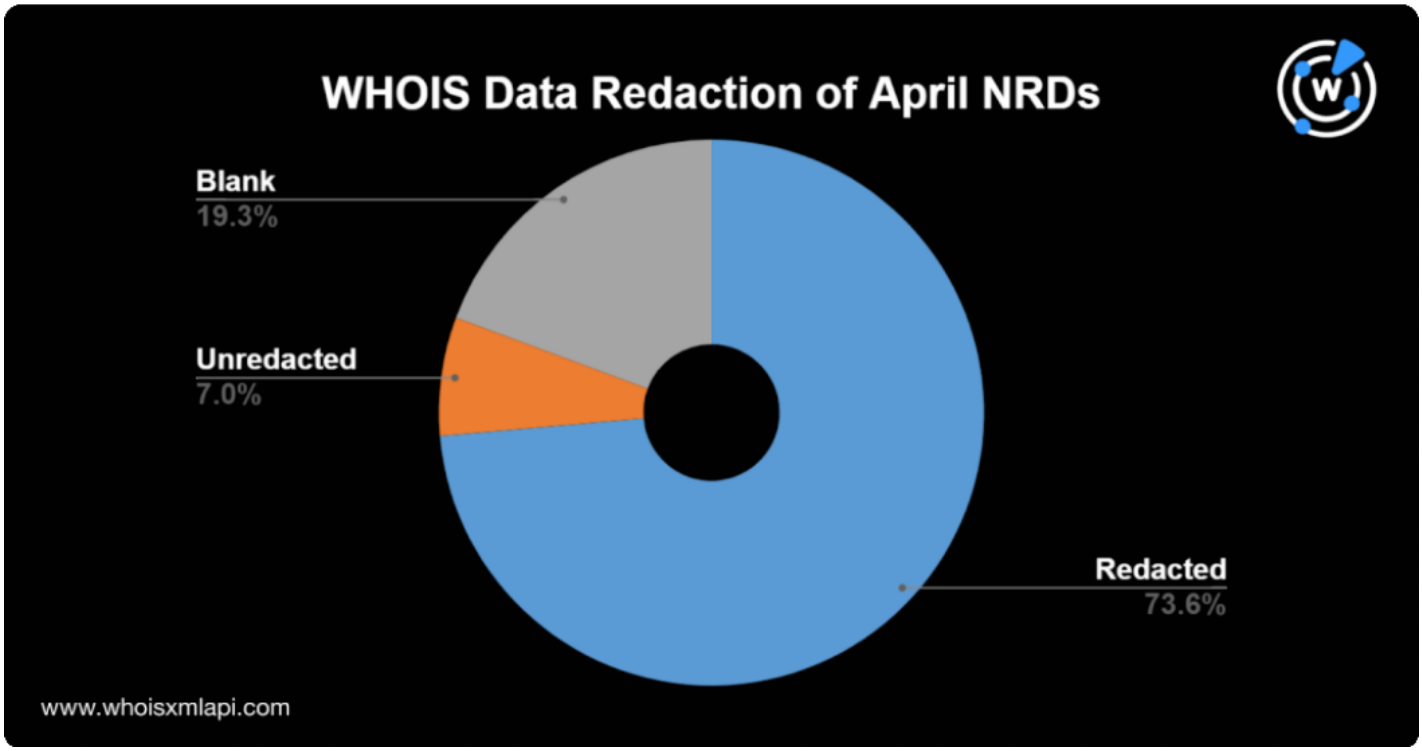


4月のNRDのうち、Infoboxが「Q4 2022 Cyber Threat Report」で指摘した最もリスクの高いTLDのドメイン名は約11.4%ありました。それらのTLDは悪意あるドメイン名を大量に抱えており、高い確度で高リスクと判定されています。以下の表は、そうしたTLDの例を示したものです。

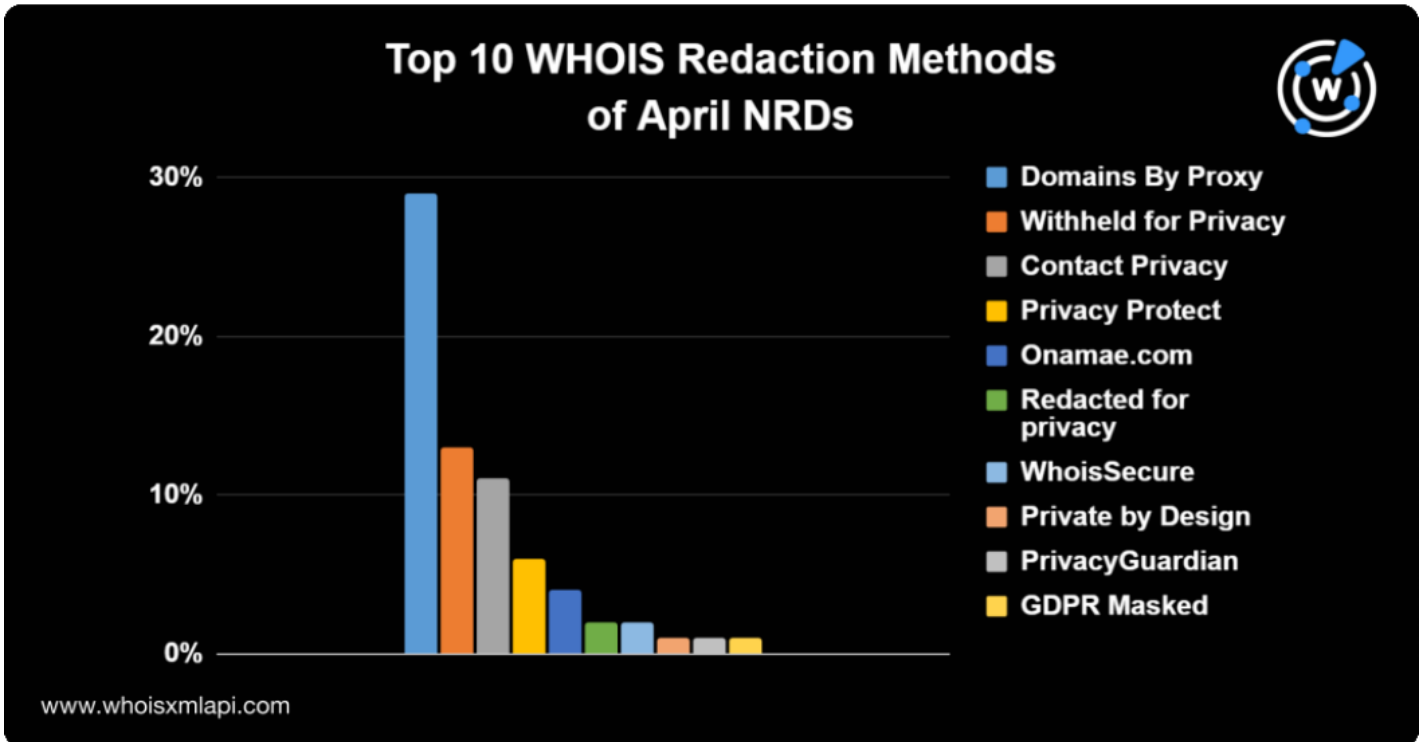
TLD	4月のNRD総数に対する各TLDのドメイン名登録数の割合
.xyz	4.785%
.top	3.395%
.click	0.724%
.buzz	0.613%
.live	0.501%

WHOISデータの非公開化

NRDの登録組織を調べたところ、74%のドメイン名でWHOISレコードが非公開にされていました。この割合は先月から若干減少しています。登録者の19%は登録組織名のフィールドを空欄にしていた一方、登録者情報を公開していたドメイン名は7%しかありませんでした。

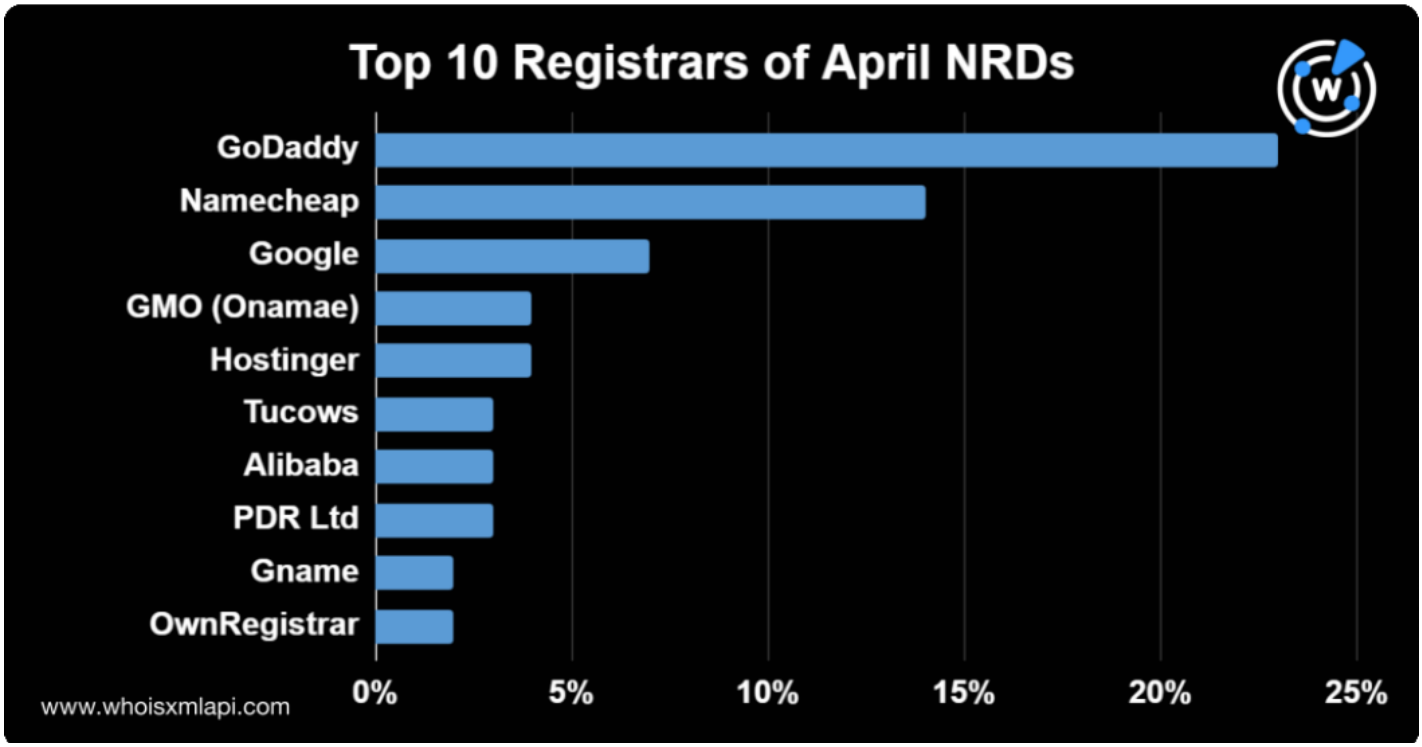


WHOISプライバシー保護業者で最もシェアが高かったのはDomains By Proxy（30%）で、これにWithheld for Privacy EHF（13%）、Contact Privacy, Inc.（8%）、Privacy Protect LLC（6%）が続きました。よく使われているプライバシー保護業者のトップ10を以下に示します。



レジストラの分布

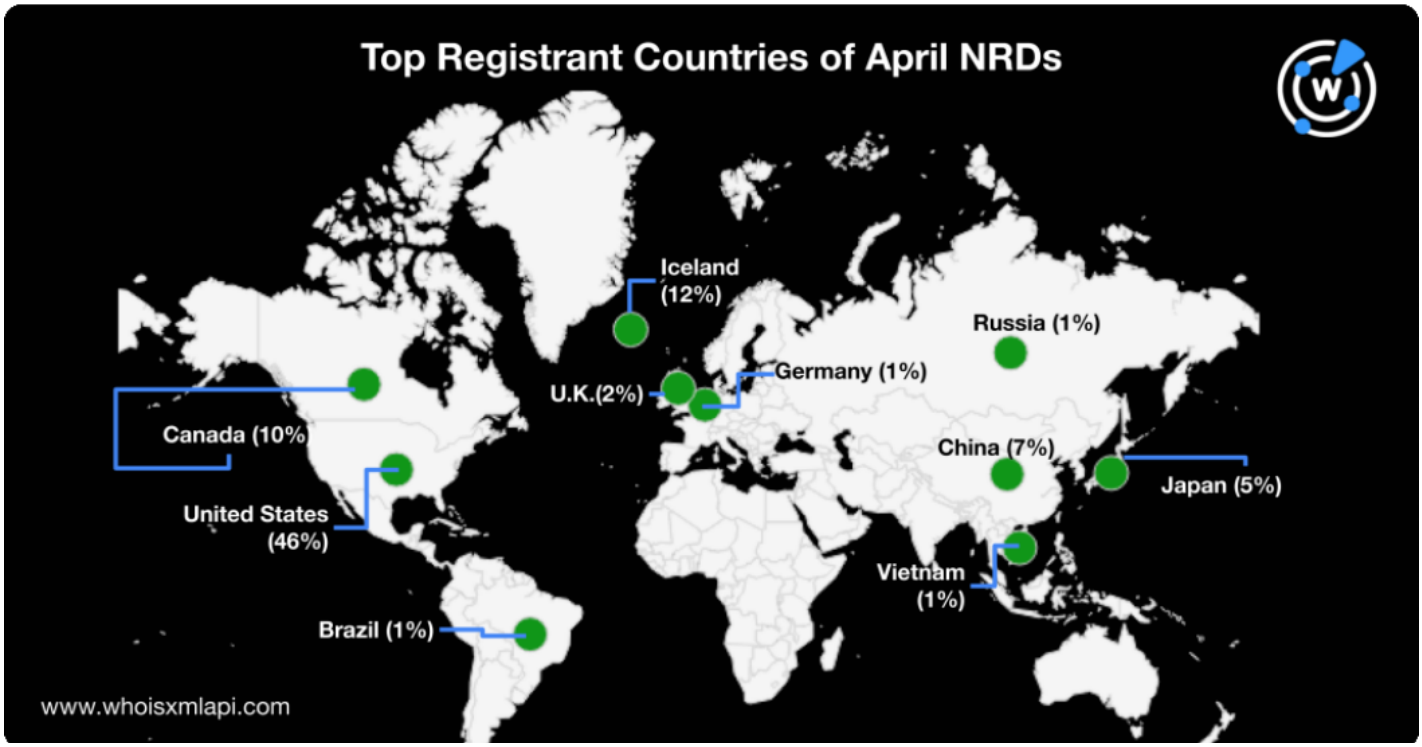
2023年4月にドメイン名の登録数が最も多かったレジストラは先月に続きGoDaddyで、全体の23%を占めました。2位はNamecheapで14%、次いでGoogle（7%）、HostingerとGMO Internet （各4%）、Tucows（3%）、Alibaba（3%）、Gname.com（2%）、OwnRegistrar（2%）の順となりました。



4月はトップ10のレジストラが総登録数の65%を占めました。残りのドメイン名は、他の350を超えレジストラに分散していました。

登録者数上位の国

4月のNRDの約46%が米国で登録され、12%がアイスランド、10%がカナダで登録されたものでした。その他、4月の登録者数上位10カ国には、中国、日本、英国、ロシア、ドイツ、ブラジル、ベトナムがランクインしました。



第2レベルドメイン（SLD）に共通して見られる文字列

NRDに最も多く使われた文字列の一つは、前月に続き***xn***でした。国際化ドメイン名（IDN）の人気が続いていることを示しています。また、***app***や***ai***といった技術用語もよく見られました。***Gpt***も繰り返し使われていました。

その他、***game***、***bet***、***best***および***job***も注目されました。それらを含む、NRDによく使われていた文字列は以下の通りです。

DNSのレンズで見るサイバーセキュリティ

当社が4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。

- **DNS情報からBECの潜在的媒体を発見**：企業経営者を狙うBECに関わったと報告された7つのセキュリティ侵害インジケーター（IoC）をWhoisXML APIの研究者が分析し、さらに数千のアーティファクトを新たに発見しました。

- **ソーシャルメディアを利用したセレブ詐欺の痕跡をDNSで追跡**：政治家や著名人を騙る不正行為に使われたIoCを当社で調査した結果、それらに繋がる別のアーティファクトが1,600個あまり見つかりました。

- **中南米・カリブ海地域に特有の潜在的詐欺ドメインを検出**：ラテンアメリカ・カリブ海地域で急増している不正行為を調査したところ、同地域の航空業界やデジタルウォレット業界を標的とした約10,000のサイバースクワッティングドメインが発見されました。

- **DNSの痕跡からSYS01とDucktailを明確に区別**：Facebookビジネスアカウントのオーナーや広告主を狙うマルウェアファミリーとして発見されたSYS01とDucktailについて、DNSの観点で共通点があるかを調べました。その結果、共通のIPアドレスを使っていた3,000のドメイン名にたどり着きました。

- **Black BastaランサムウェアのDNS調査でOneNoteと宅配便のなりすましを発見**：ランサムウェア「Black Basta」に関連するIoCを当社で調査し、WHOIS情報がIoCドメインと共通していた約1,000のドメイン名を特定しました。その中には、OneNoteや宅配便を装った悪意あるドメイン名もありました。

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ユースケースの支援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。