ドメイン名動向ハイライト：2023年2月

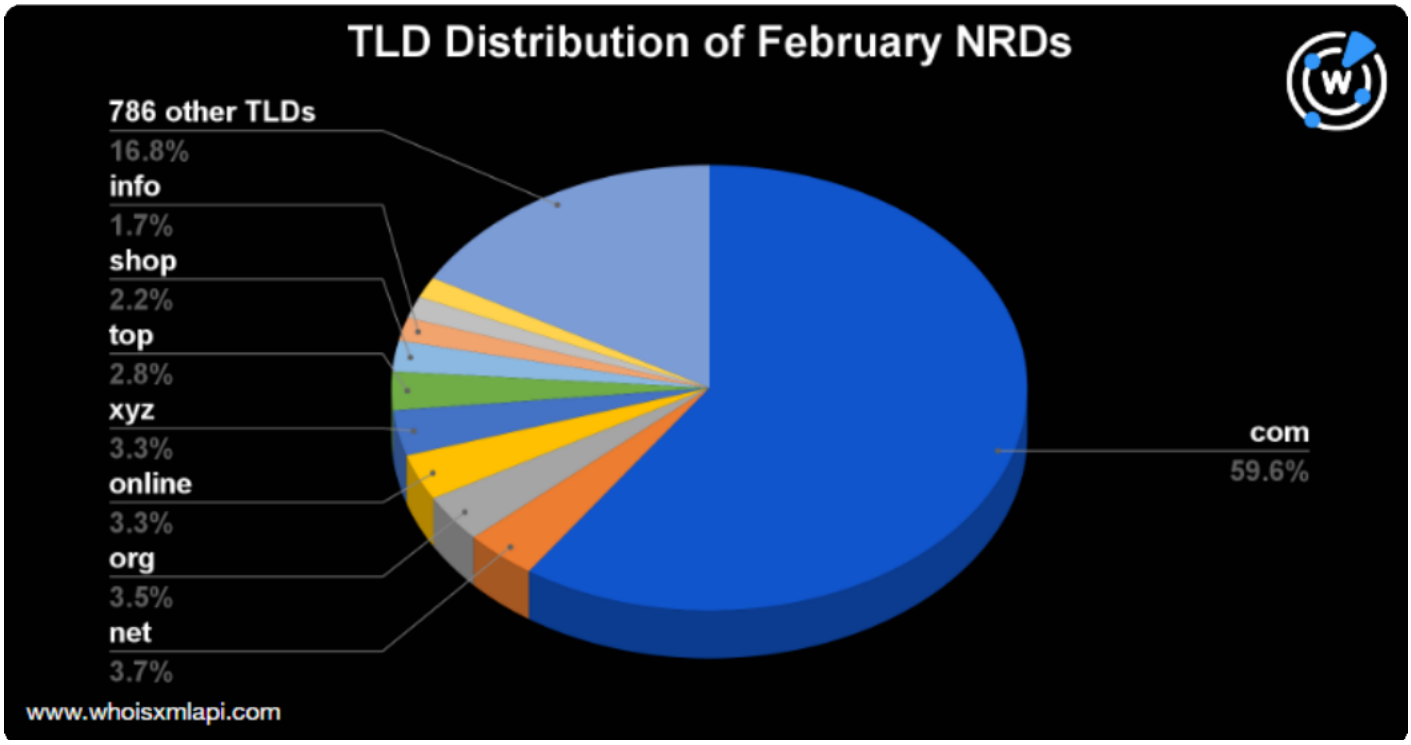
2023年3月7日

WhoisXML APIでは、2023年2月1日から28日までの間に新規登録された数百万個のドメイン名の中から28,000個を無作為に抽出、分析し、レジストラ、登録者の国およびTLDの分布を明らかにしました。また、ドメイン名に含まれるテキスト文字列の使用状況を調査し、新たなトレンドの可能性を発見しました。この調査の結果を以下に示します。また、ドメイン名、DNSおよびIPアドレスのインテリジェンスを駆使した当社の脅威リサーチへのリンクも掲載しています。

2月の新規登録ドメイン名（NRD）をクローズアップ

TLDの分布

2月に登録されたドメイン名のうち最も多かったのは引き続き.comドメイン名で、全体の59.6%を占めました。これに.net（3.7%）、.org（3.5%）、.onlineと.xyz（各3.3%）、.top（2.8%）、.shop（2.2%）、.info（1.7%）が続いており、残りのドメイン名は他の786種類のTLDに分散していました。主な内訳は以下のグラフの通りです。



最も不正利用されているTLDのドメイン名登録数

また、2023年3月3日にSpamhausが特定した、最も悪用されているTLDとそれらのドメイン名登録数に注目してみました。以下の表は、当該TLDと、Spamhausの算出による各TLDのドメイン名登録総数に占める不正利用ドメイン名の割合、および2月の新規登録ドメイン名（NRD）総数に当該各TLDのドメイン名が占めている割合を示しています。

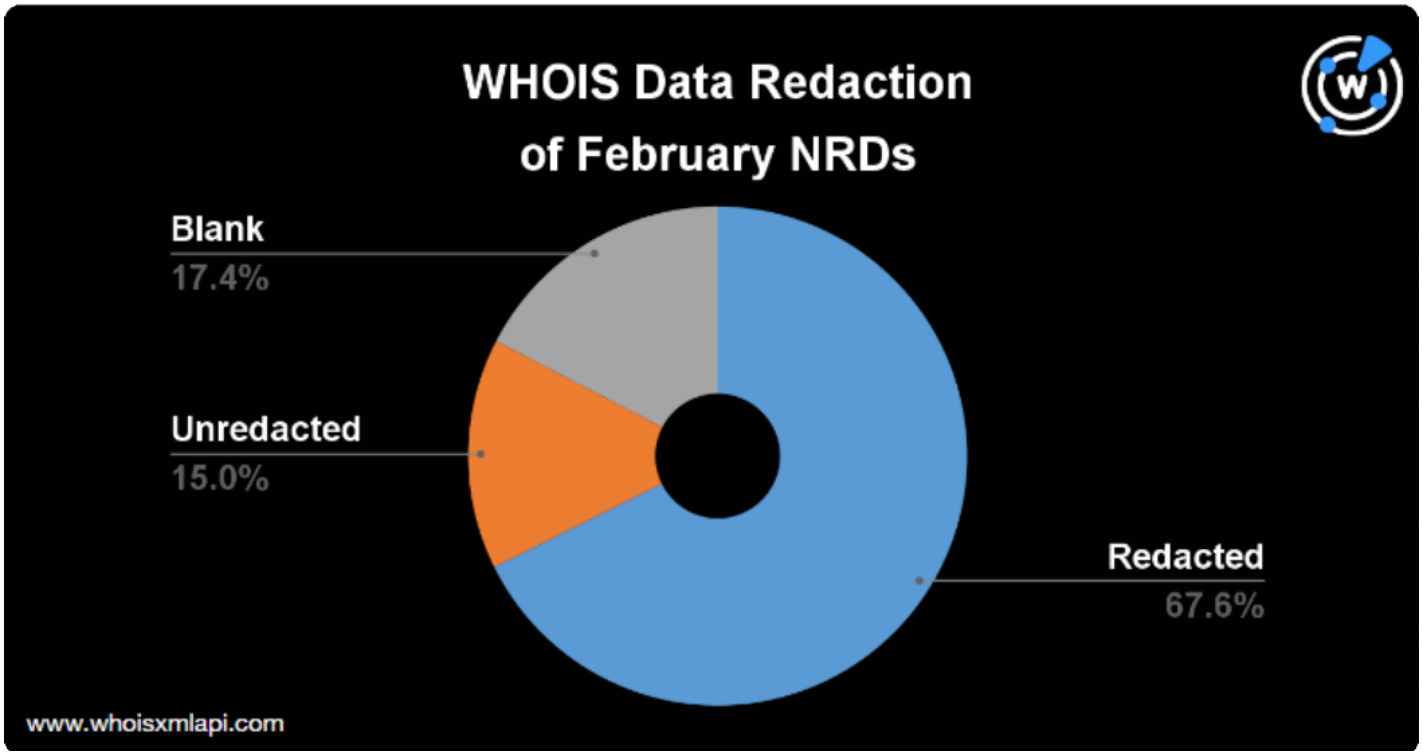
TLD	各TLDのドメイン名登録数に対する不正利用ドメイン名の割合（算出：Spamhaus）	2月のNRD総数に対する各TLDのドメイン名登録数のシェア
.live	31.0%	0.542%
.beauty	25.1%	0.076%
.fyi	21.0%	0.063%

.fit	24.7%	0.029%
.zone	28.5%	0.015%
.bar	27.6%	0.012%
.rest	71.7%	0.005%
.okinawa	69.6%	0.001%

NRD総数に対する各TLDのドメイン名登録数は1%未満ですが、2月のNRD総数が数百万個におよんだことから、不良化する可能性のあるNRDは数千個に達する可能性があります。

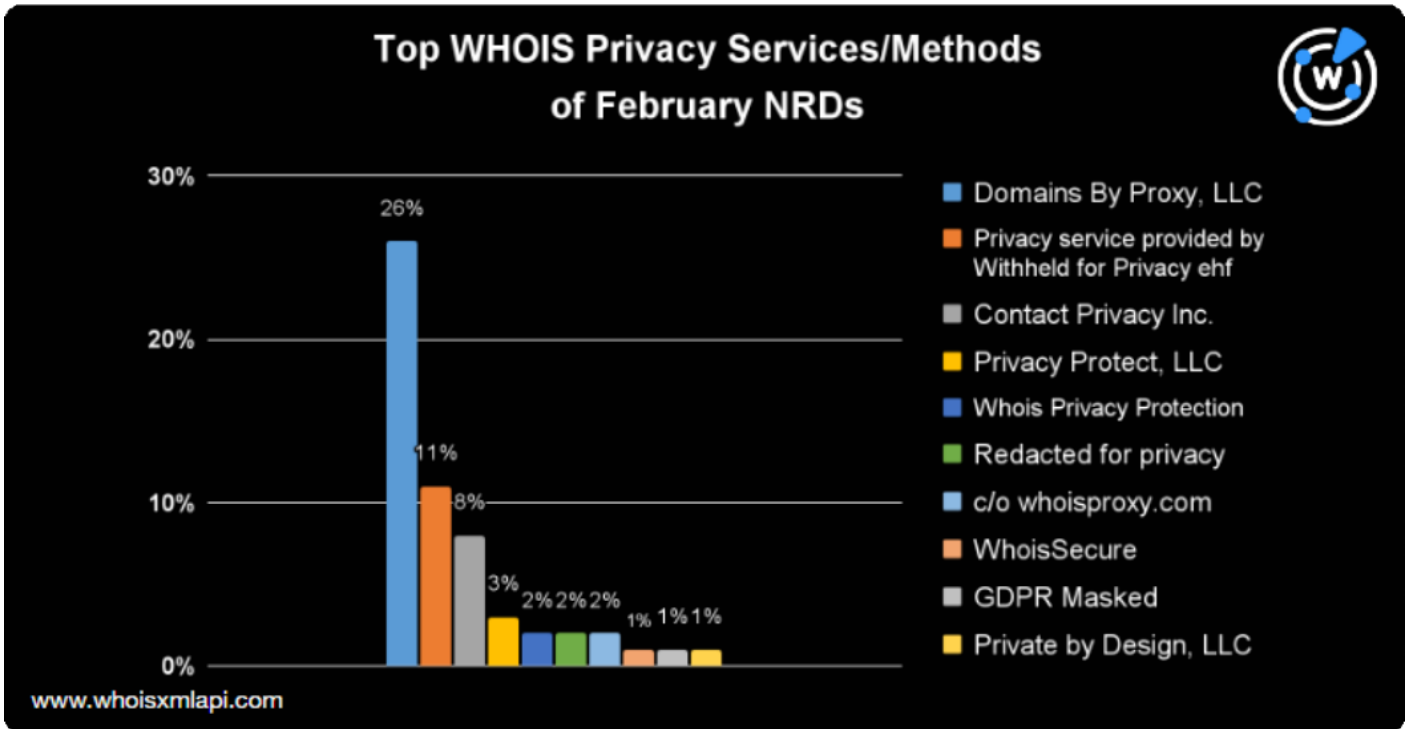
WHOISデータの非公開化

WHOISデータの非公開化は長年にわたって世界中で大規模に実施されており、2月のNRDもその例に漏れません。WHOISレコードを公開しているドメイン名は全体の15%に過ぎず、メールアドレスを公開しているドメインはさらに少なくなっています。



WHOISの登録者のOrganizationレコードから、約67.6%のドメイン名でプライバシー保護サービスを利用していることがわかりました。そこで、最も多くの登録者が利用したWHOISプライバシー保護サービスを調べました。その結果、Domains By Proxy, LLCが最も多く利用されており、2月のNRDの4分の1以上のレコードを保護していることが判明しました。

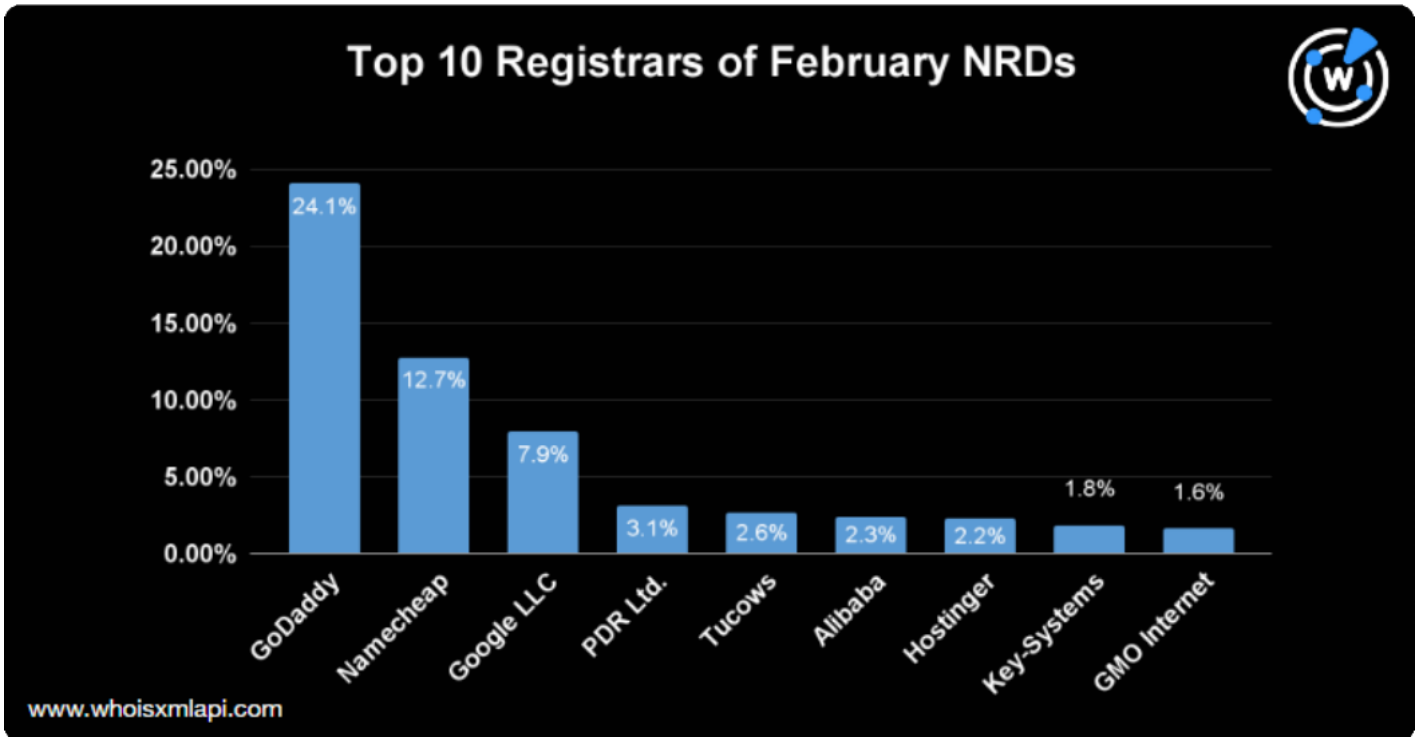
これにWithheld for Privacy EHFが11％、Contact Privacy, Inc.が8％で続いています。その他、Privacy Protect, LLC、お名前.comのWhois情報公開代行、whoisproxy.comのRedacted for Privacy、WhoisSecure、GDPR MaskedおよびPrivate by Design, LLCによるOrganizationレコードの保護サービスが確認されました。これらをまとめたのが以下のグラフです。



レジストラの分布

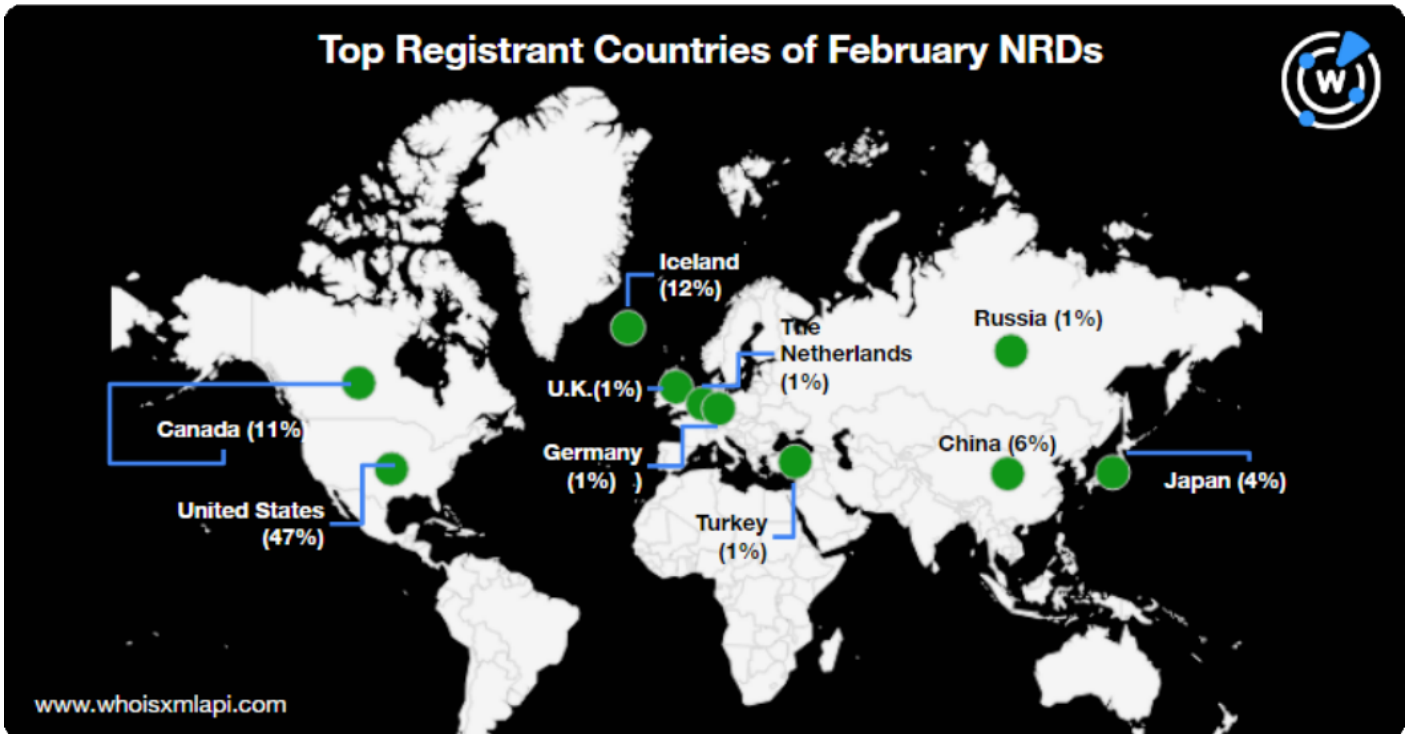
ドメイン名登録数に対するレジストラのシェアを比較したところ、GoDaddyが約24％で引き続き大半を占めていたことがわかりました。それに次いでNamecheapが12.7%、Googleが7.9%、PDR Ltd.が3.1%、Tucowsが2.6%、Alibabaが2.3%、Hostingerが2.2%、Key-Systemsが1.8%、GMOインターネットが1.6%となっています。

上位10社のレジストラが全体の半数以上のドメイン名を管理していることがわかりました。残りの半分弱は、他の409社のレジストラに分散して管理されています。



登録者数上位の国

2月のNRDのほぼ半数が米国で、12%はアイスランド、11%がカナダで登録されたことがわかりました。登録者が多いその他の国としては、1月のリストに掲載された中国、日本、英国、ロシア、ドイツがあります。なお、2月はインドネシアとインドに代わってオランダとトルコがランクインしました。以下の地図は、これらの国とドメイン名登録数のシェアを示しています。



第2レベルドメインに共通して見られる文字列

NRDの文字列を見ると、インターネットに関連した一般名詞が引き続き多く使われたことがわかります。例えば、***online***、***shop***、***market***、***info***、***tech***、***app***などです。また、***AI***もよく見られる文字列です。

さらに、***XN***が頻繁に使われたことから、国際化ドメイン名（IDN）に依然として人気があることもわかりました。以下のワードクラウドは、2月のNRDによく見られた文字列を示しています。

DNSのレンズで見るサイバーセキュリティ

以下に、当社が2月に公開した脅威リサーチ報告の一部をご紹介します。

- **Hiveランサムウェアとの戦いは終わっていない? –未確認のアーティファクトを発見 –**：ランサムウェアグループ「Hive」が使用した6つのセキュリティ侵害インジケーター（IoC）をもとに当社で調査し、この脅威に関わっているドメイン名をさらに950個あまり発見しました。

- **著名なサイバー・ジハーディストのIoCリストを拡充**：WhoisXML APIの脅威リサーチャーであるDancho Danchevが最近、サイバー・ジハーディストに繋がる6つのメールアドレスを特定しました。そして、それらのIoCをもとに2,200個を超えるメールアドレスと5,551個のIPアドレスが判明しました。

- **脅威ベクトルの特定で正規のツールを偽るBatloaderを発見**：BatloaderのIoCとされた17個のドメイン名を出発点として当社で調査し、5,000個を超える関連ドメイン名を発見しました。そのうちの複数のドメイン名がマルウェアをホストしていたことも確認されました。

- **IoCリストをもとに調査を展開、Gigabud RATの脅威の規模を測定**：10個のGigabud RATのIoCをもとに当社で調査したところ、さらに1,000個以上の関連ドメイン名が明らかになりました。そのうち数百個のドメイン名は、Banco de Comercio、Advice、Thai Lion Air、Shopee Thailand、SUNATおよびKasikornbankといった組織名の文字列を含むものでした。

- **Google広告で拡散した不正ソフトの繋がりをたどる**：オープンソースソフトウェアのダウンロードサイトを訪問するユーザーを狙った最近の不正行為を当社で詳細に調べ、関与が公にされたIoCをもとに、数百にのぼるアーティファクトを発見しました。

当社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確認で使用した当社の商品と機能につきましては、こちらまでお気軽にお問い合わせください。