ドメイン名動向ハイライト：2023年12月

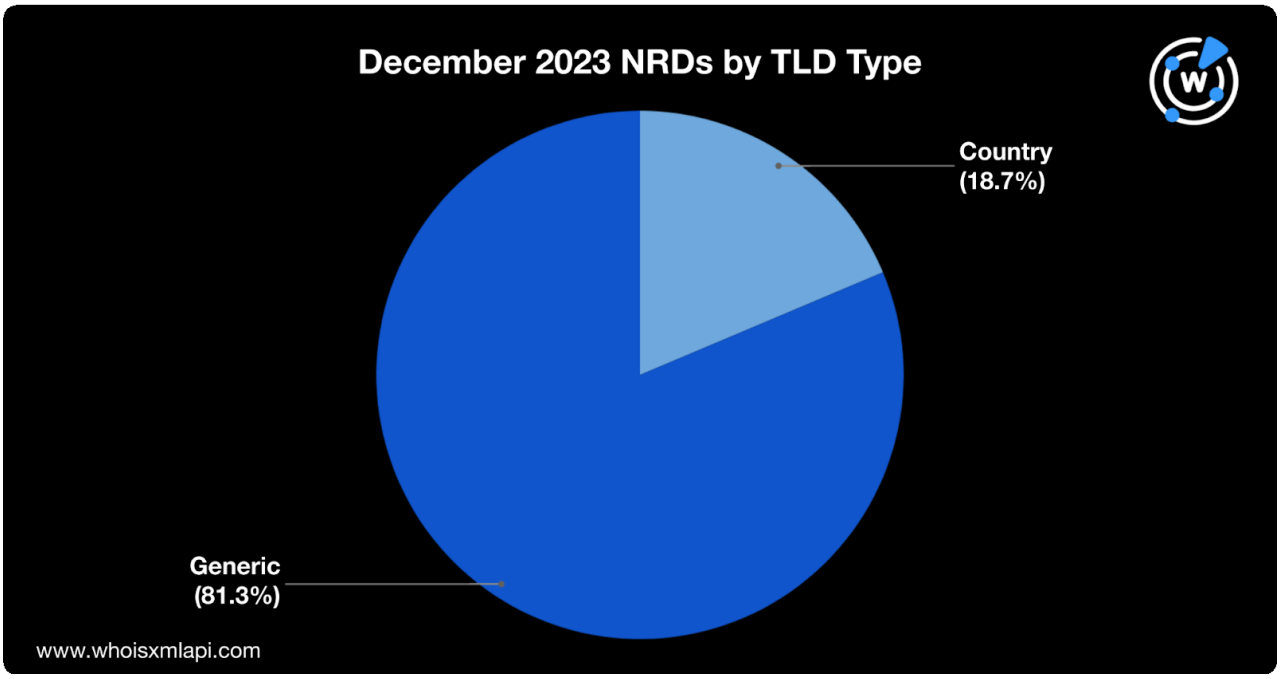
WhoisXML APIの研究者がこのほど、2023年12月1日～31日に新規登録された960万を超えるドメイン名を分析し、最も多く使われていたトップレベルドメイン（TLD）やレジストラを含むドメイン名登録の傾向を分析しました。

また、12月にセキュリティ侵害インジケーター（IoC）としてタグ付けされた約150万のドメイン名について、そのTLDの使用状況や脅威の種類を調査しました。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。

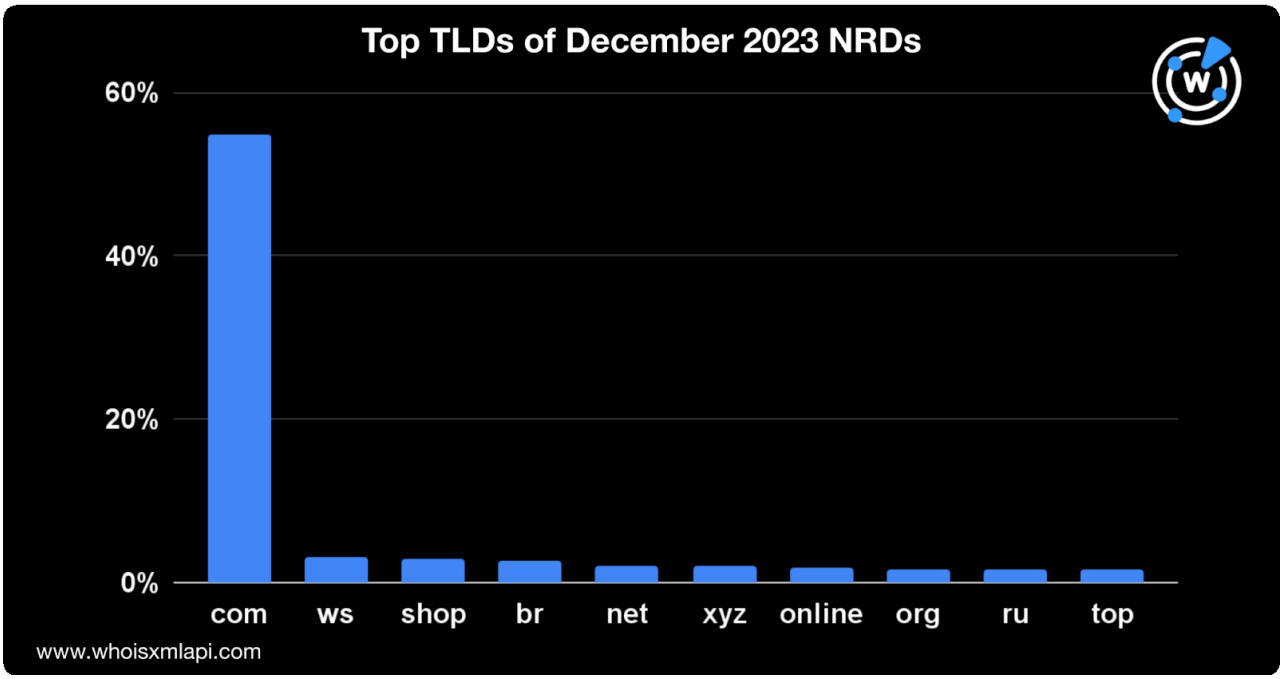
12月の新規登録ドメイン名（NRD）をクローズアップ

TLDの分布

12月に登録されたドメイン名の約81.3%は分野別TLD（gTLD）、18.7%は国コードTLD（ccTLD）を使ったドメイン名でした。

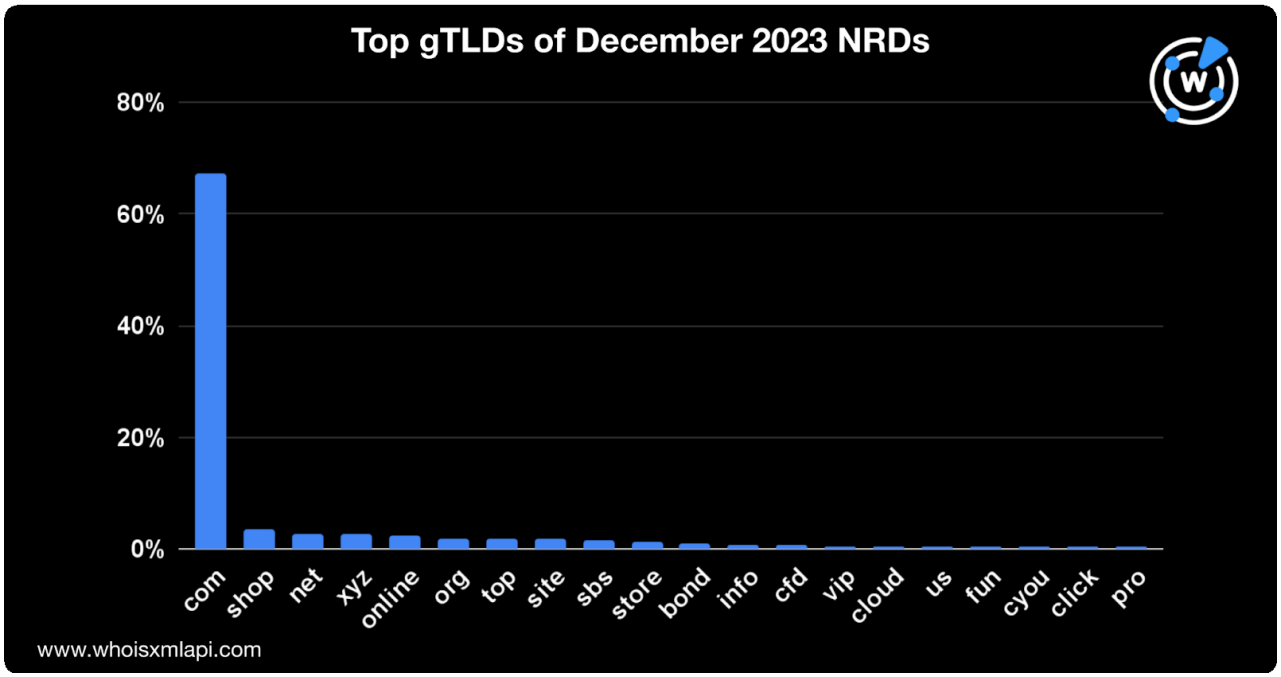


新規登録ドメイン名（NRD）に最も多く使われていたTLDは、54.8%を占めた.comでした。次いで多かったのは、.ws（3.1%）、.shop（3%）、.br（2.7%）、.netと.xyz（各2.1%）、.online（1.9%）、.org（1.6%）、.ruと.top（各1.5%）です。

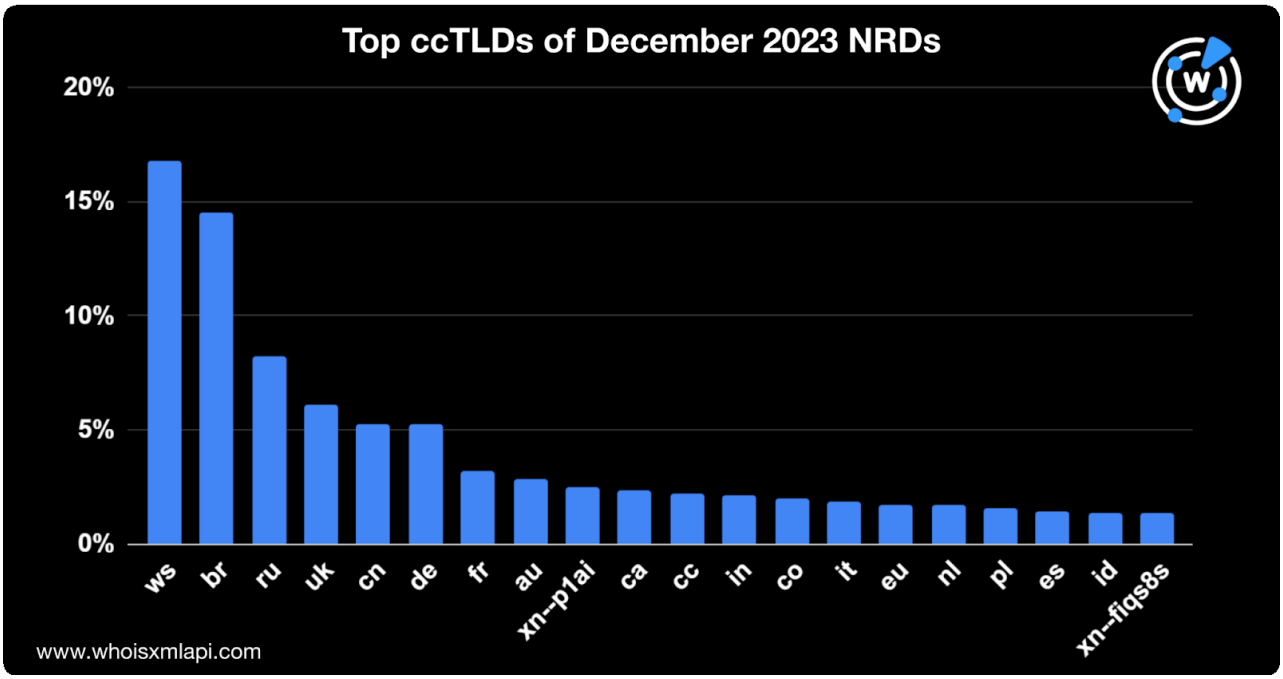


次に、NRDにおけるgTLDとccTLDの利用を分析し、gTLDとccTLDそれぞれについて最も人気のあるTLDを特定しました。

625あまりのgTLDの中で最も使用されていたのは.com で、gTLDを使ったNRD総数の67.3%を占めました。次に多かったのは.shop（3.7%）、.netと.xyz（各2.6%）、.online（2.4%）、.orgと.top（各1.9%）、.site（1.8%）、.sbs（1.6%）、.storeと.bond（各1.2%）、.info（0.9%）、.cfd（0.7%）、.vip、.cloud、.us、.fun（各0.5%）、.cyou、.click、.pro（各0.4%）でした。

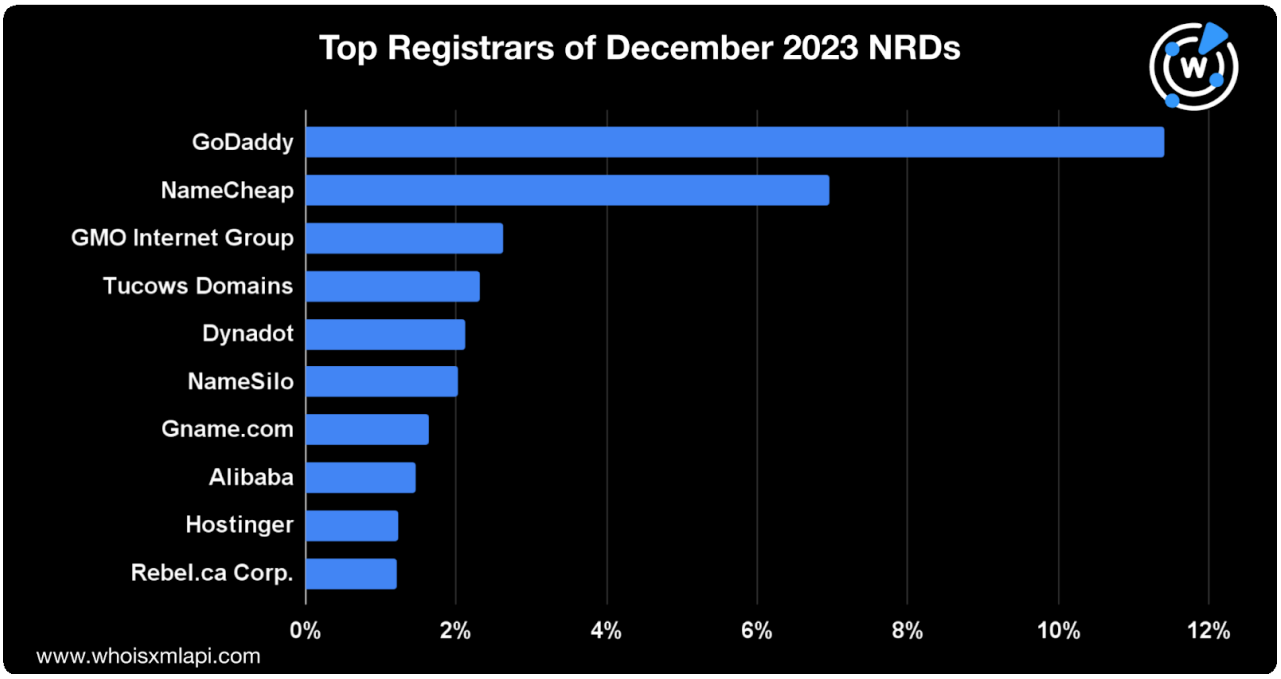


他方、240超のccTLDの中で最も人気が高かったのは.wsで、12月のNRDにおけるシェアは16.8%でした。次いで、.br（14.6%）、.ru（8.3%）、.uk（6.1%）、.cnと.de（各5.2%）、.fr（3.2%）、.au（2.8%）、.xn--p1ai（2.5%）、.ca（2.4%）、.cc（2.2%）の順となりました。ccTLDのトップ20は以下のグラフの通りです。



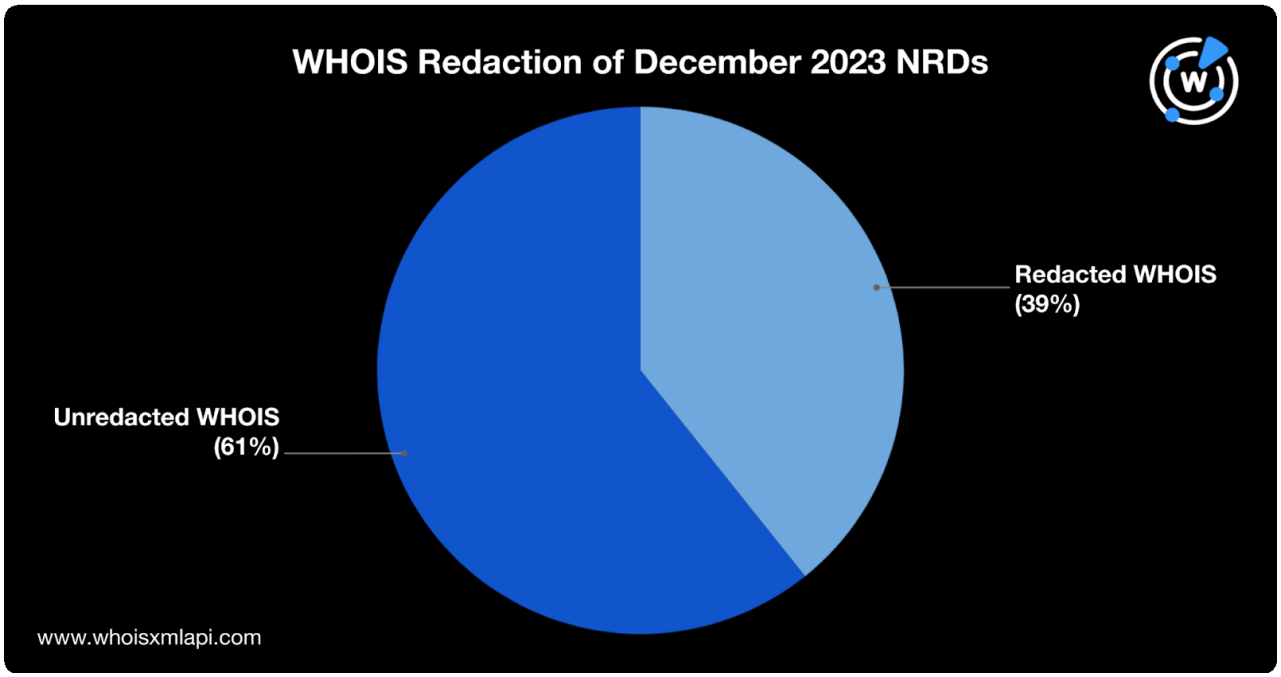
レジストラの分布

12月のNRDで最も多く使われていたレジストラはGoDaddyで、全NRD登録数の11.4%を占めました。次いで管理ドメインが多かったレジストラはNamecheap（7%）、GMO Internet（2.6%）、Tucows（2.3%）、Dynadot（2.1%）、NameSilo（2%）、Gname（1.6%）、Alibaba Cloud Computing（1.5%）、HostingerとRebel.ca（各1.2%）でした。



WHOISデータの非公開化

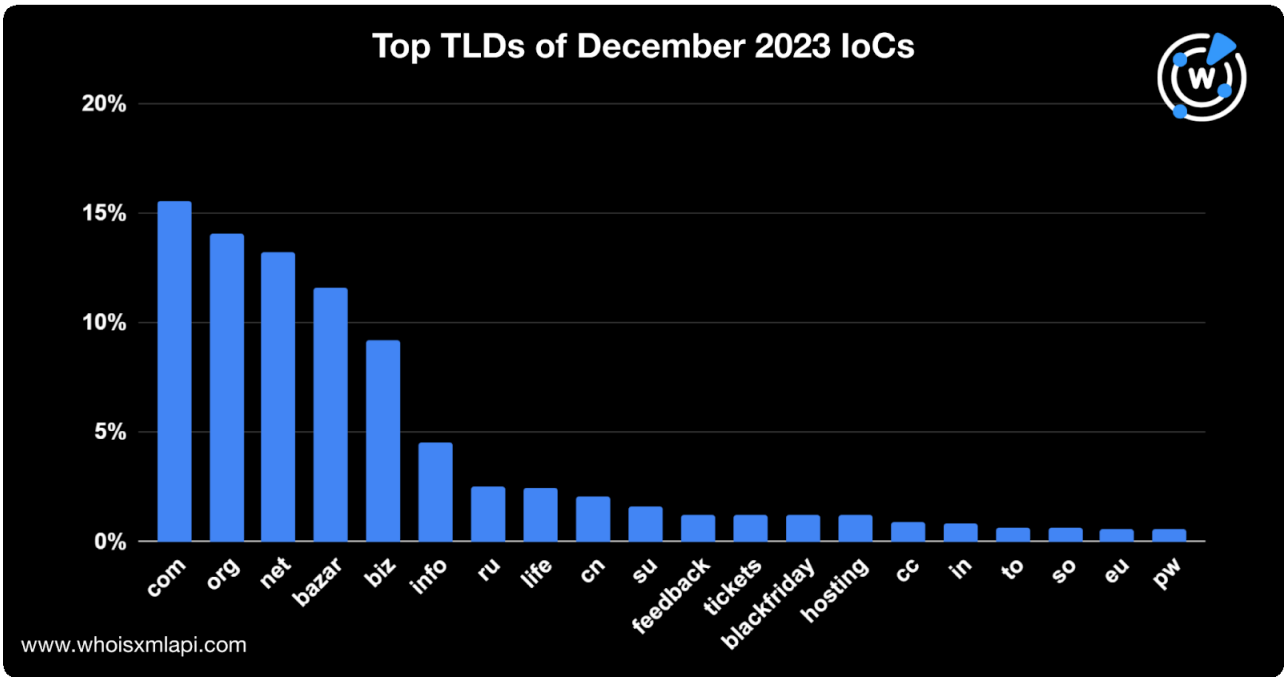
12月のNRDの約61%は、WHOISレコードを未編集の状態で公開していました。他方、39%はプライバシー保護を目的とした編集・非公開化を行っていました。



DNSのレンズで見るサイバーセキュリティ

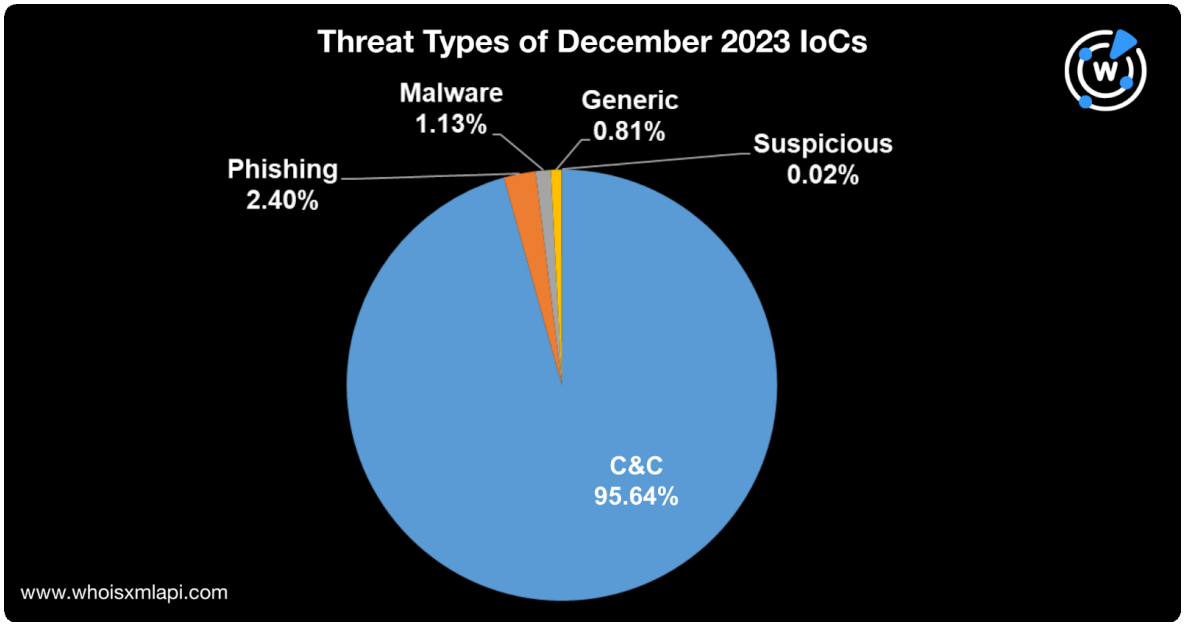
12月のIoCのトップTLD

12月にIoCとして検出された150万近くのドメイン名を当社で分析したところ、そのうちの16%は.comのドメイン名でした。また、14%は.orgを、13%は.netを使用していました。.bazar（12%）、.biz（9%）、.info（5%）、.life（2%）などの新gTLDを使用しているドメイン名も見られました。また、.ru（3%）、.cnと.su（各2%）などのccTLDを使ったドメイン名もありました。IoCで使用されていたTLDのトップ20は、以下のグラフの通りです。



12月のIoCの脅威タイプ別内訳

12月に検出されたIoCを当社で脅威タイプ別に分類したところ、そのほとんど（95.64%）がコマンド＆コントロール（C&C）サーバーと判明しました。また、フィッシングキャンペーンが2.4%、マルウェアの配布が1.13%でした。約0.8%がその他のサイバー攻撃に関与しており、0.02%が不審なアクティビティにタグ付けされていました。脅威の種類ごとの内訳は下表の通りです。



脅威レポート

当社が12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。

- **姿の見えないWailingCrabをDNSで解明**：WailingCrabマルウェアの配布に関与した24個のIoCのリストから、3,000超の潜在的関連アーティファクトを検出しました。
- **Atomic Stealerのインフラの裏側に迫る**：Atomic Stealerに関連するIoCをWhoisXML APIの研究者が詳細に調査し、共通のIPアドレス/メールアドレスを使用している数十のアーティファクトを発見しました。
- **DNSのレンズで見るフェイクID市場**：脅威リサーチャーのDancho Danchevがフェイク ID販売業者のメールアドレスを特定したことを受け、当社の研究チームが詳細な調査を行いました。その結果、潜在的なアーティファクトが検出されました。

- **Genesis Marketインフラの裏側：DNSの徹底分析**：Genesis Marketのサイバー犯罪インフラの一部である可能性のあるドメイン名とIPアドレスを当社の研究チームが発見しました。

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。