ドメイン名動向ハイライト：2023年11月

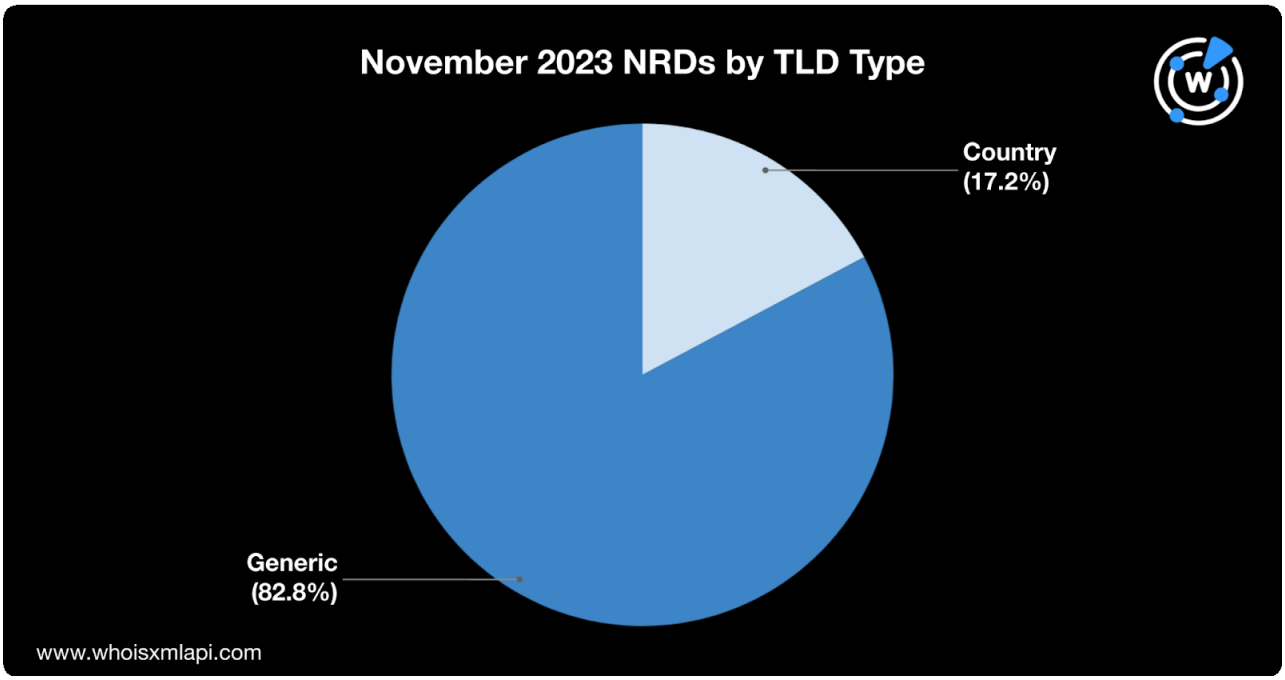
WhoisXML APIの研究者がこのほど、2023年11月1日から30日の間に新規登録された870万を超えるドメイン名を分析し、最も多く使われていたトップレベルドメイン（TLD）やレジストラなどの傾向を調べました。

また、11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110万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。

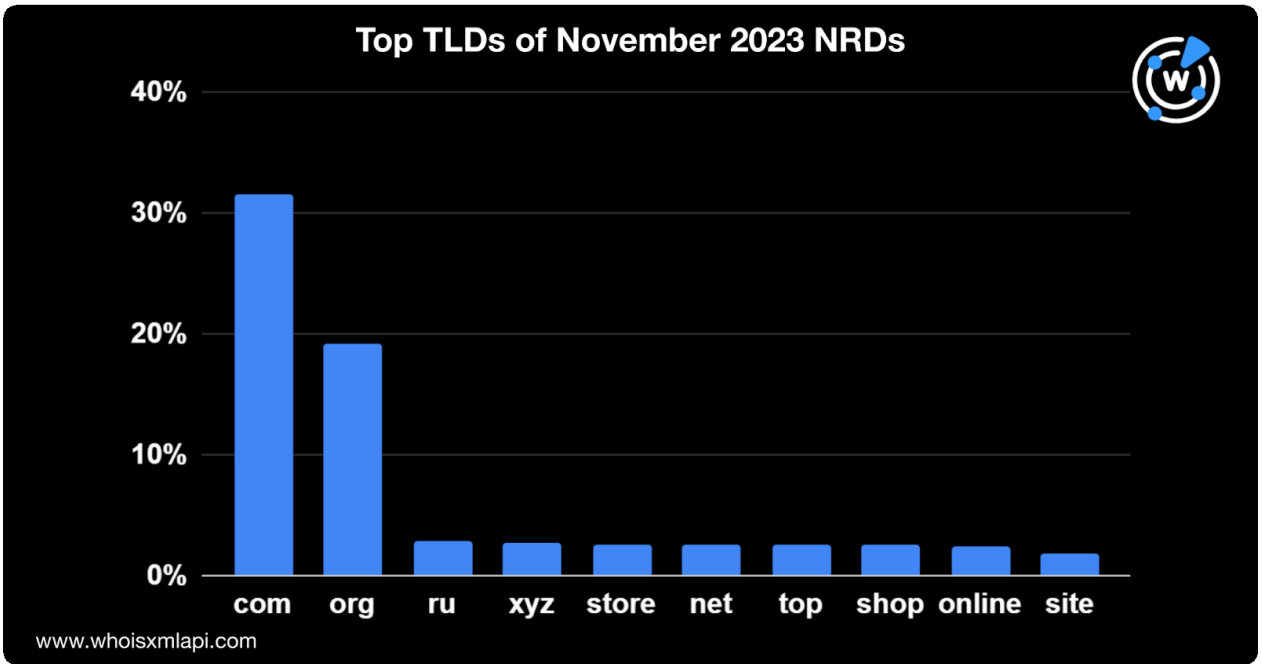
11月の新規登録ドメイン名（NRD）をクローズアップ

TLDの分布

11月に登録されたドメイン名の82.8%は分野別TLD（gTLD）、17.2%は国コードTLD（ccTLD）を使ったドメイン名でした。

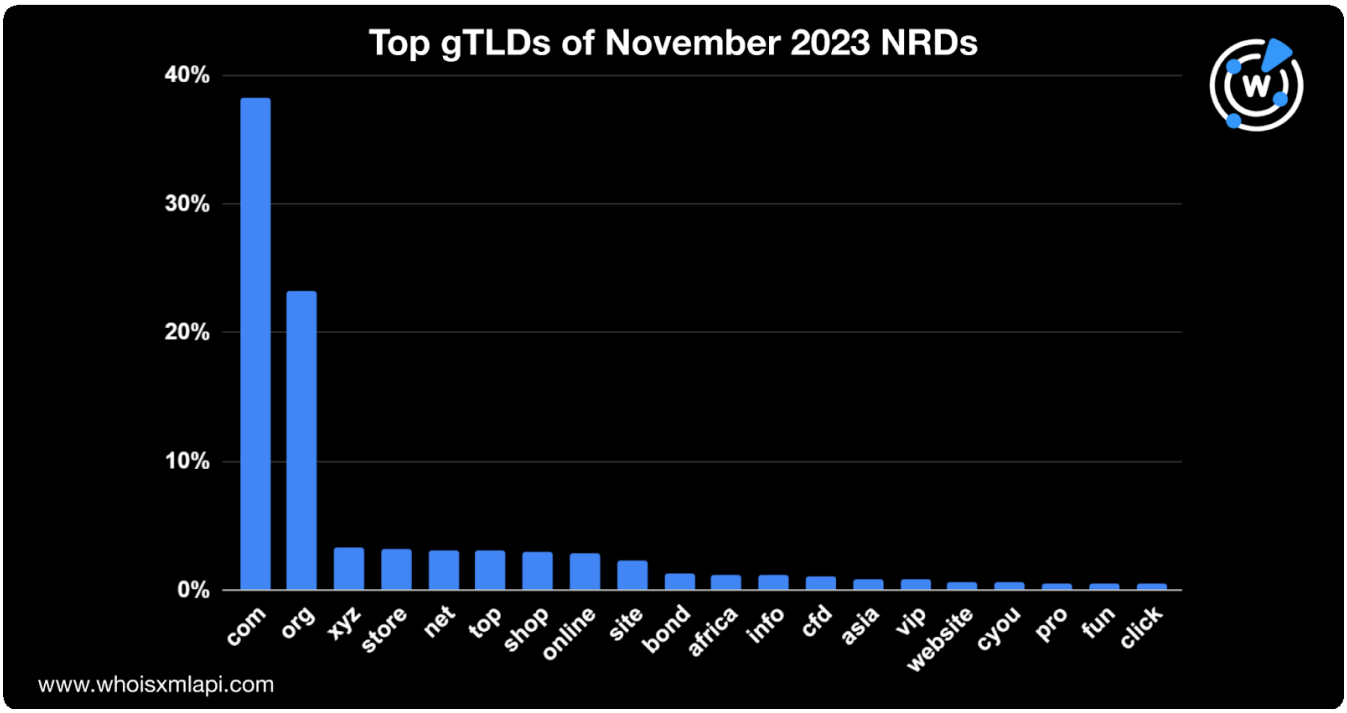


新規登録ドメイン名（NRD）に最も多く使われていたTLDは、31.6%を占めた.comでした。トップ10の2位以下は、.org（19.2%）、.ru（2.8%）、.xyz（2.7%）、.store（2.6%）、.net（2.5%）、.top（2.5%）、.shop（2.5%）、.online（2.4%）、.site（1.9%）でした。

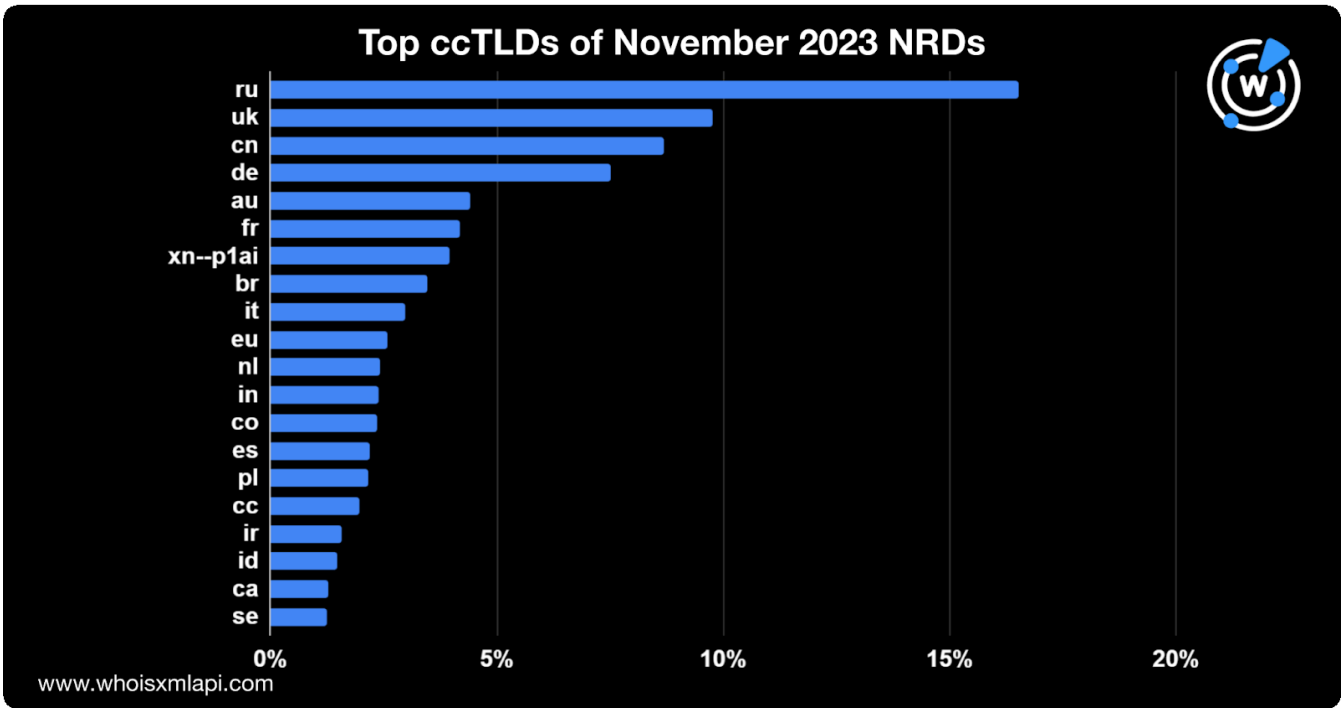


次に、NRDにおけるgTLDとccTLDの利用を別々に分析し、gTLDとccTLDそれぞれについて最も人気のあるTLDを特定しました。

635超のgTLDの中で最も使用されていたのは.com で、gTLDのNRD総数の38.2%を占めました。次に多かったのは.orgで、23.2%でした。さらに、.xyz（3.3%）、.store（3.2%）、.net（3.1%）、.top（3%）、.shop（3%）、.online（2.9%）、.site（2.3%）、.bond（1.3%）が続きました。トップ20の残りは以下のグラフの通りです。

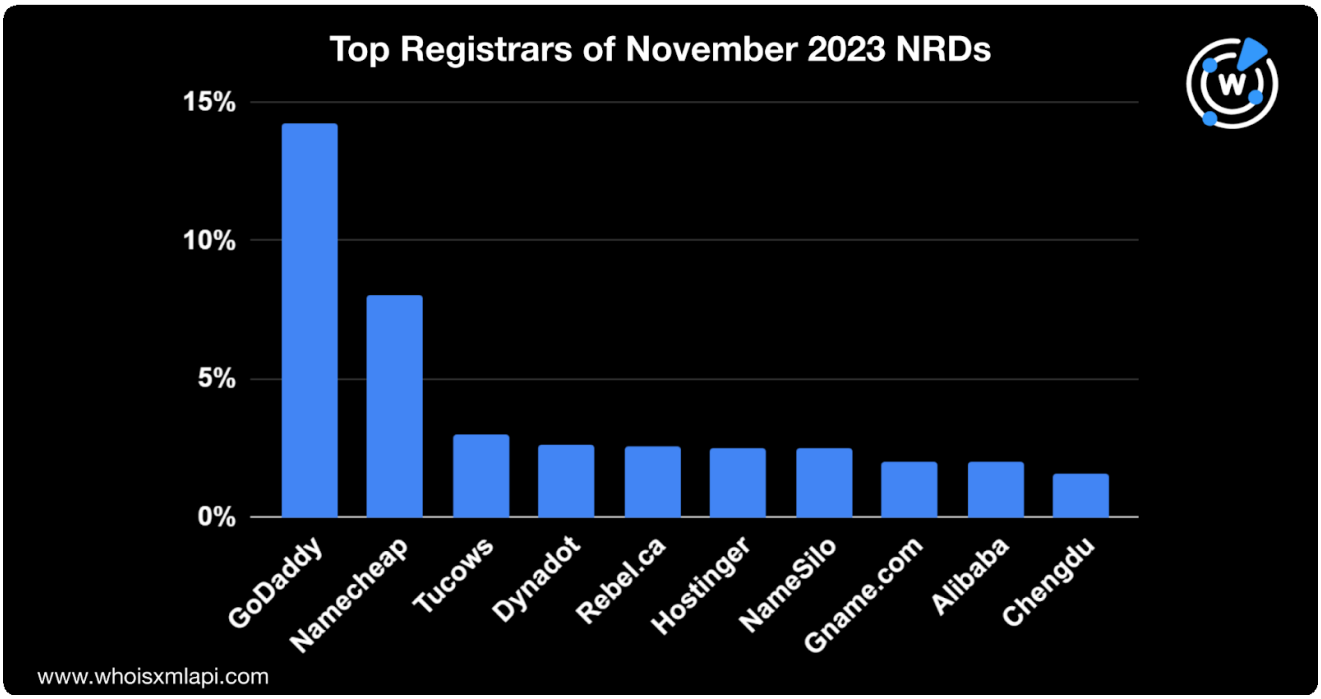


240を超えるccTLDの中で最も人気が高かったのは.ruで、11月のNRDにおけるシェアは16.5%でした。次いで、.uk（9.8%）、.cn（8.7%）、.de（7.5%）、.au（4.4%）、.fr（4.2%）、.xn--p1aiまたは.pф（4%）、.br（3.5%）、.it（3%）、.eu（2.6%）の順となりました。トップ20は以下のグラフの通りです。



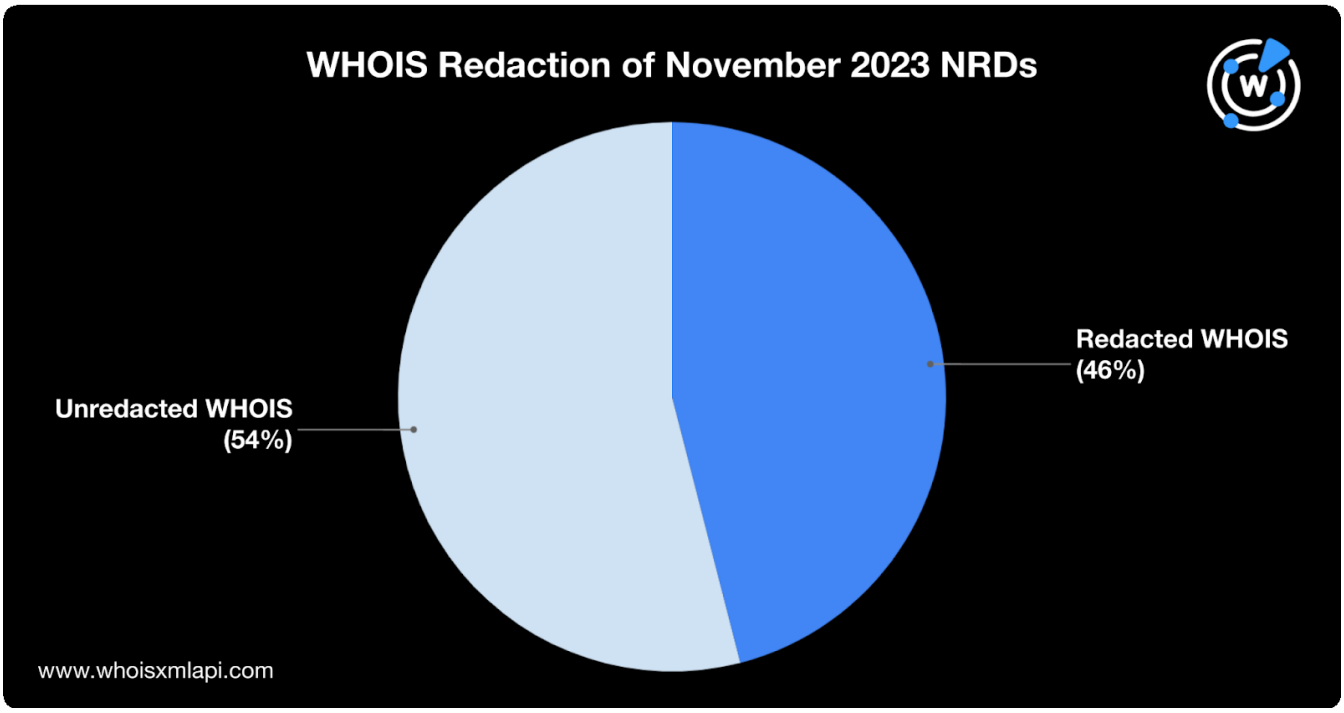
レジストラの分布

2,900を超えるレジストラの中でトップの地位を獲得したのはGoDaddyで、NRDの14.2%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, Inc.（8.1%）、Tucows Domains, Inc.（3%）、Dynadot, Inc.（6%）、Rebel.ca Corp.（6%）、Hostinger Operations, UAB（2.5%）、NameSilo, LLC（2.5%）でした。トップ10の残りは、Gname.com Pte. Ltd.（2%）、Alibaba Cloud Computing Ltd.（2%）、Chengaba Cloud Computing LLC（2%）、Chengdu West Dimension Digital Technology Co. Ltd.（1.6%）でした。



WHOISデータの非公開化

11月のNRDの半数以上は、WHOISレコードを公開、または未編集の状態で表示していました。他方、46%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。

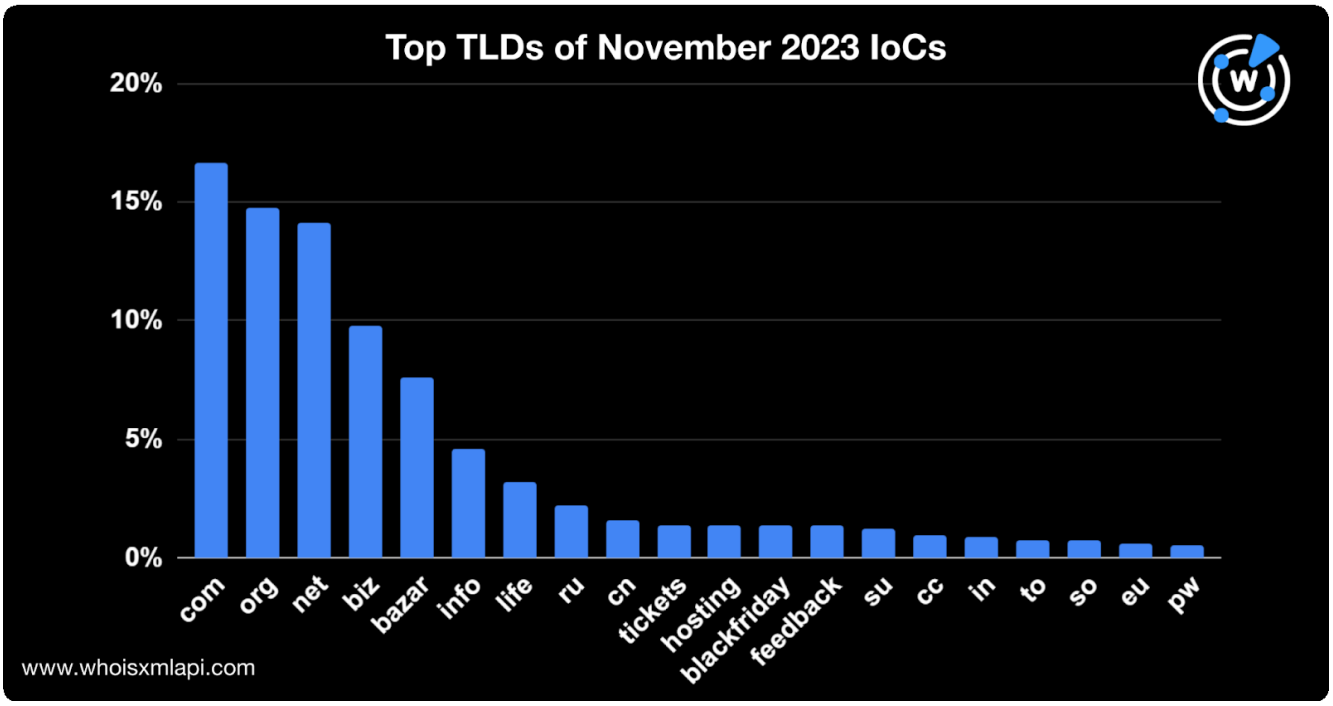


DNSのレンズで見るサイバーセキュリティ

11月のIoCのトップTLD

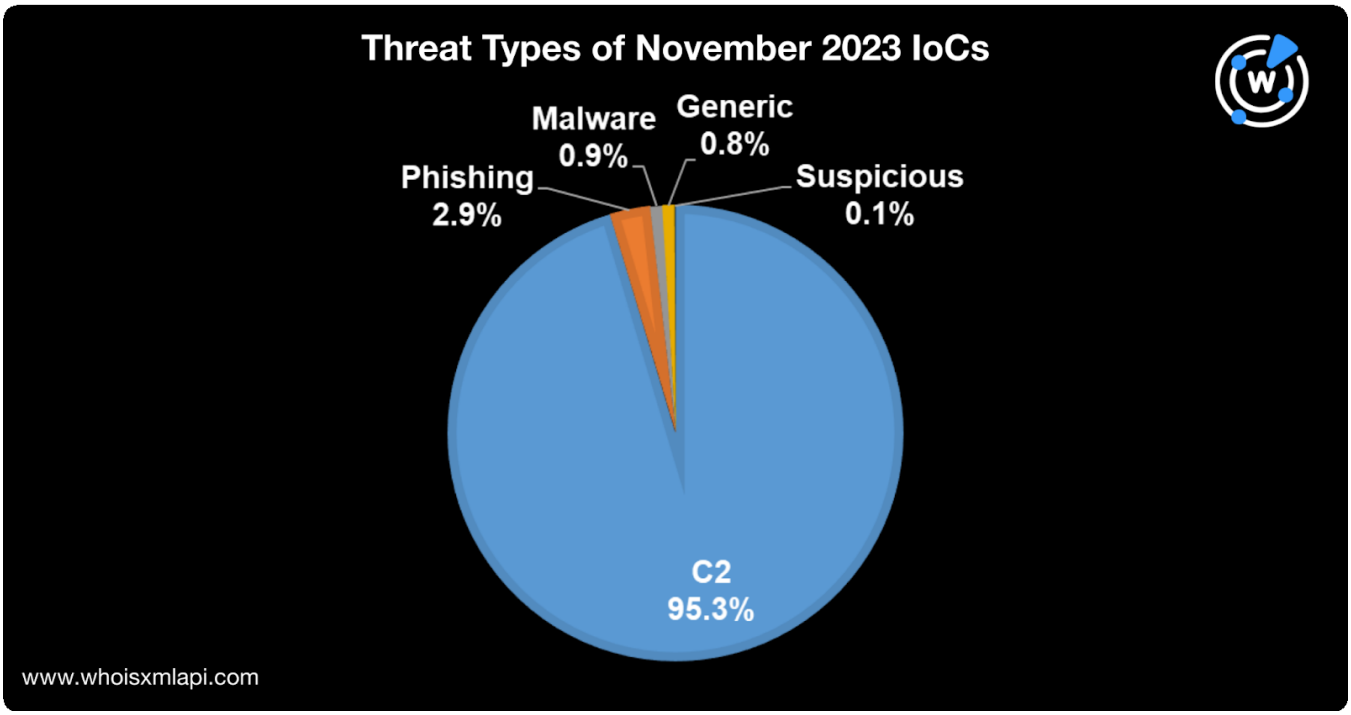
11月にIoCとして検出された110万のドメイン名のTLDを当社で分析したところ、最も多く利用されていたTLDはIoCの16.6%を占める.comとわかりました。

また、約14.8%は.orgを、14.1%は.netを使用していました。.biz（9.8%）、.bazar（7.6%）、.info（4.6%）、.life（3.2%）、.tickets（1.4%）など、新gTLDを使用するドメイン名も見られました。その一方で、.ru（2.2%）と.cn（1.6%）を筆頭にccTLDを使用したものもありました。IoCで使用された上位20のTLDは、ほとんどがccTLDと新gTLDでした。



11月のIoCの脅威タイプ別内訳

WhoisXML APIの脅威インテリジェンスを用いて、110万件のIoCを脅威の種類に基づいて分類しました。その結果、ほとんどのIoCはコマンド&コントロール（C&C）サーバーとしてタグ付けされ（95.3%）、2.9%はフィッシングキャンペーン、0.9%はマルウェアの配布に関与していました。約0.8%はその他の形態のサイバー攻撃に関与しており、0.1%は不審な活動に関与していました。脅威の種類別の内訳は下表の通りです。



脅威レポート

当社が11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。

- **不正な防弾ホスティングは今も健在：DNS調査から**：不正な防弾ホスティングサービスプロバイダーに関連するドメイン名を調査し、公開メールアドレス130超、共通のメールアドレスまたはIPアドレスを使用しているドメイン名5,000超を特定しました。

- **カーディングは今も盛況：DNSインテリジェンスで判明**：カーダーが所有していると思われる220のメールアドレスのリストをもとに、1,700を超える潜在的なアーティファクトを発見しました。

- **BreachForumsドメインのDNS徹底調査**：当社の脅威リサーチャーであるDancho Danchevが、BreachForumsのメンバーに属すると思われる570超のドメイン名を発見しました。そこで、そのIoCリストをもとに、2023年3月にFBIによって閉鎖されたフォーラムがオンラインに戻ったという報告について調査しました。

- **DNSの徹底調査でBlackNet RATの履歴を追跡**：当社の研究者がBlackNet RAT IoCのリストを収集し、DNSインテリジェンスを使用して分析しました。この分析の結果、共通のメールアドレスまたはIPアドレスを使用していたドメイン名が5,800超検出されました。

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。