ドメイン名動向ハイライト：2024年3月

WhoisXML APIの研究者がこのほど、2024年3月1日～31日に新規登録された730万超のドメイン名を分析し、最も人気のあったレジストラ、ドメイン名登録者の国、最も多く使われていたトップレベルドメイン（TLD）を含むドメイン名登録の世界的な傾向を分析しました。

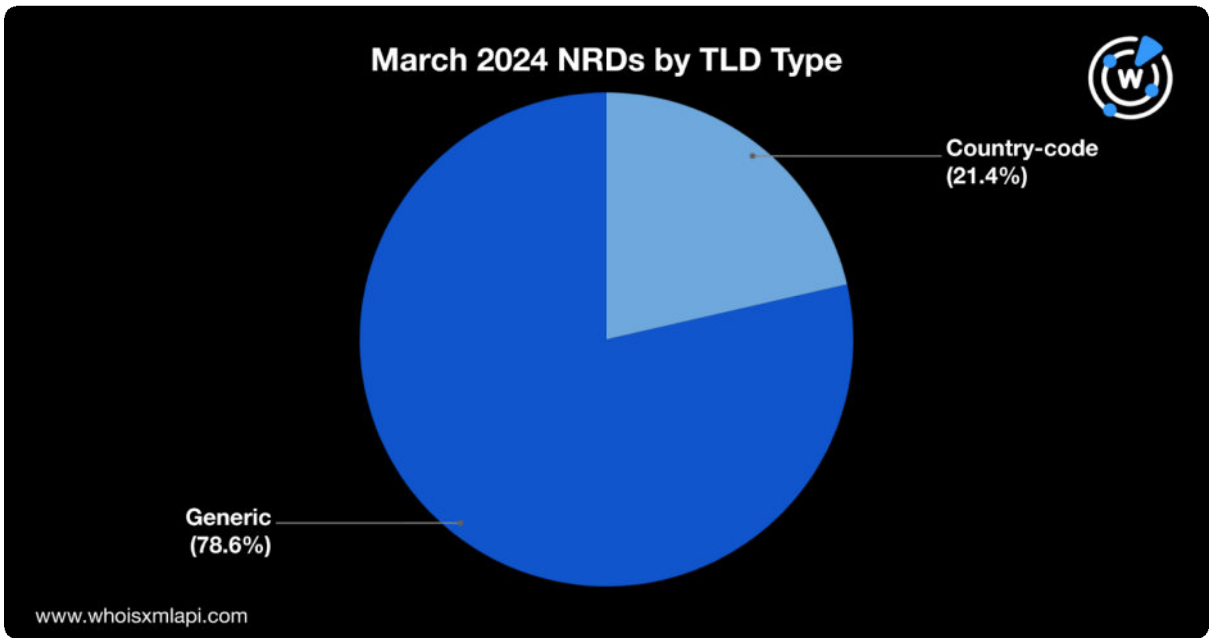
また、2024年3月にセキュリティ侵害インジケーター（IoC）として検出された110万超のドメイン名について、そのTLDの使用状況や脅威の種類を調査しました。

本調査の結果と、DNS、IPアドレス、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。

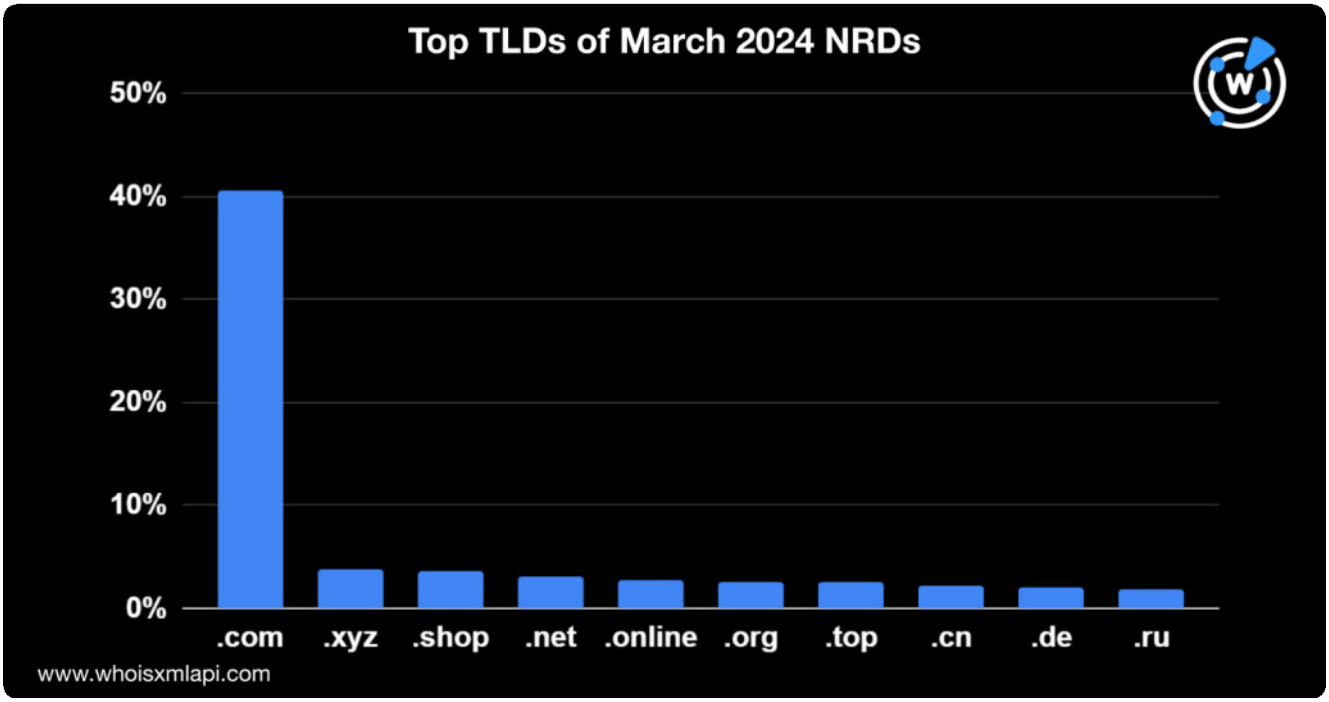
3月の新規登録ドメイン名（NRD）をクローズアップ

TLDの分布

2024年3月に新たに登録された730万ドメインのうち、78.6%は分野別TLD（gTLD）、21.4%は国コードTLD（ccTLD）を使ったドメイン名でした。



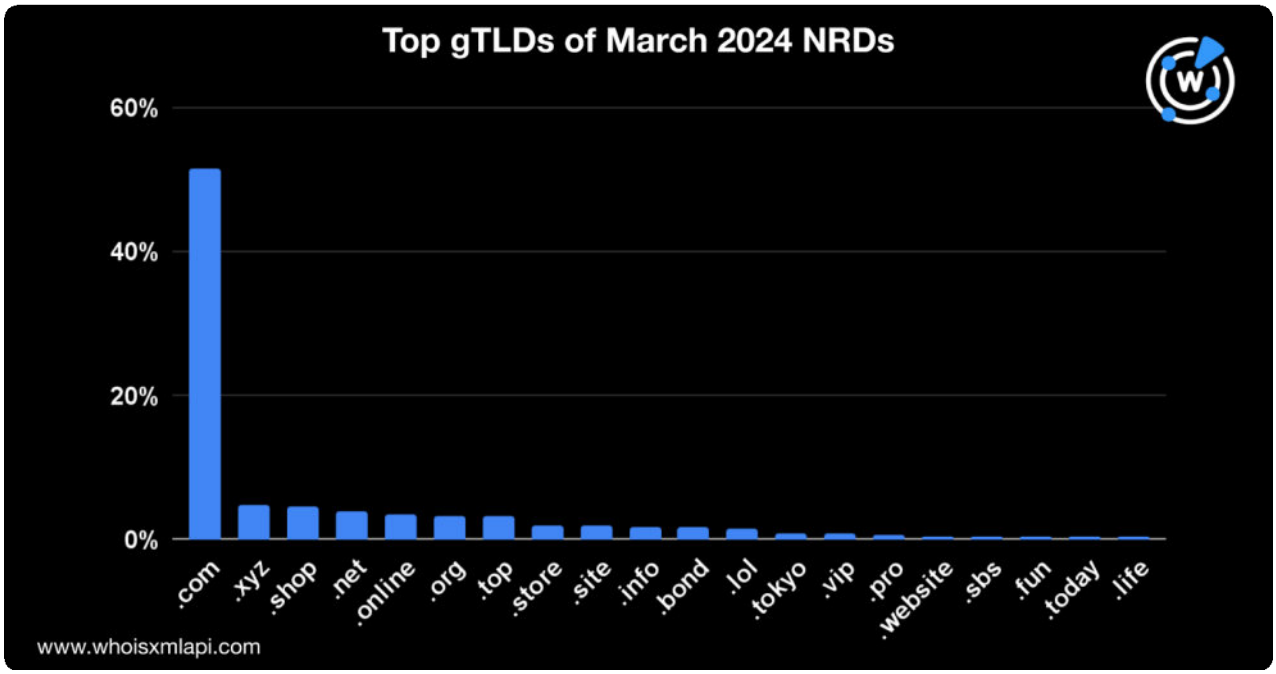
2月の傾向と変わらず、3月の新規登録ドメイン名（NRD）に最も多く使われていたTLDは、全体の40.5%を占めた.comでした。次いで多かったのは.xyz（3.8%）、.shop（3.7%）、.net（3%）、.online（2.7%）、.org（2.6%）、.top（2.5%）、.cn（2.2%）、.de（2.1%）および.ru（1.9%）です。



次に、NRDをgTLDとccTLDに分け、それぞれのグループで最も人気のあったTLDを特定しました。

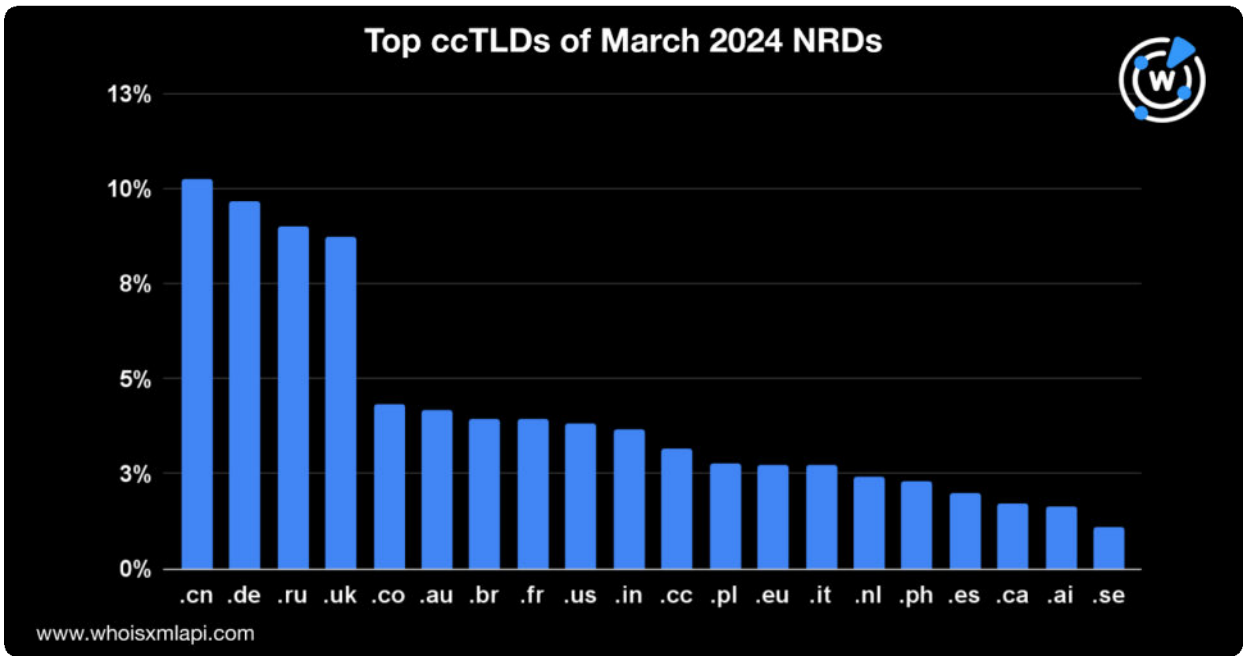
650あまりのgTLDの中で最も使われていたのは.comで、gTLD下に登録されたNRD総数の51.3%を占めました。2位以下は.comに大差をつけられました。

2位は.xyz（4.9%）、3位はeコマース関連の.shop（4.7%）でした。これに.net（3.9%）、.onlineと.org（各3.4%）、.top（3.2%）、.storeと.site（各1.9%）、.info（1.8%）、.bond（1.7%）、.lol（1.5%）、.tokyo（0.9%）、.vip（0.8%）、.pro（0.6%）、.website、.sbs、.fun、.todayおよび.life（各0.5%）が続きました。



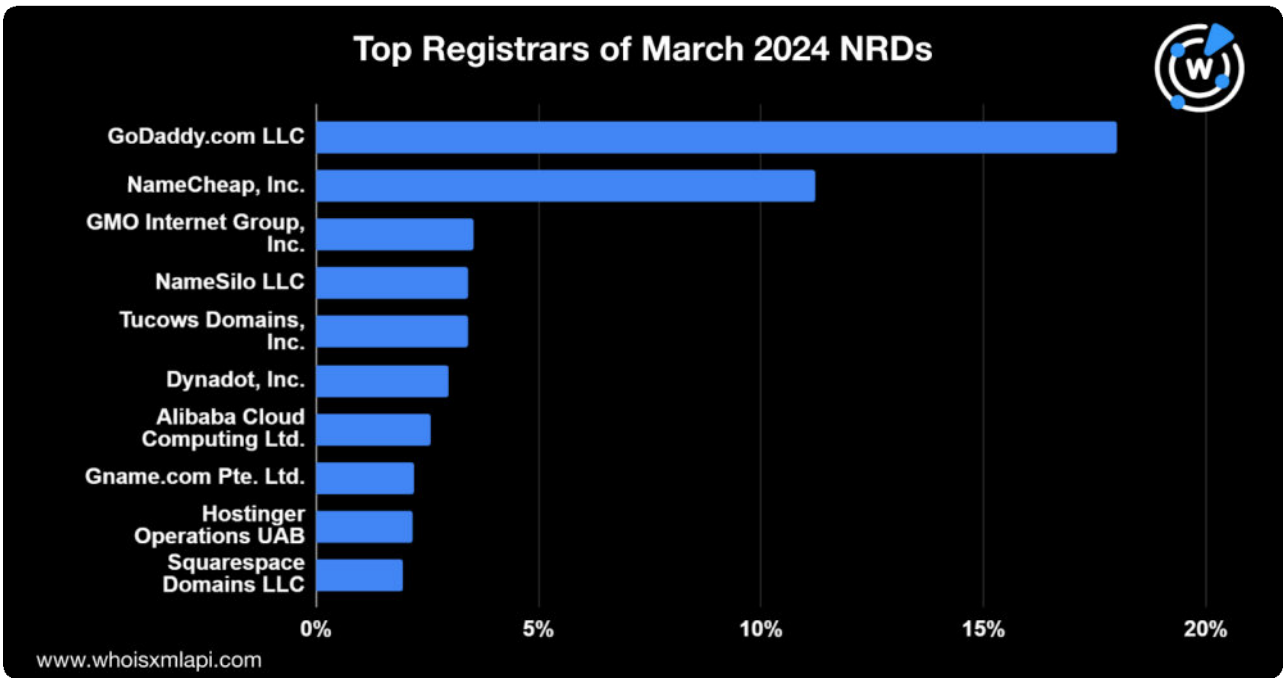
他方、230超存在するccTLDの中で最も人気が高かったのは.cnで、ccTLD下で登録されたNRDの10.3%を占めました。

次いで多かったのは.de（9.7%）、.ru（9%）、.uk（8.7%）、.co（4.3%）、.au（4.2%）、.br（4%）、.fr（3.9%）、.us（3.8%）、.in（3.7%）、.cc（3.2%）、.plと.eu（各2.8%）、.it（2.7%）、.nl（2.4%）、.ph（2.3%）、.es（2%）、.caと.ai（1.7%）、.se（1.1%）となりました。
以上を合計すると、3月のccTLDによるNRDの84.2%になります。



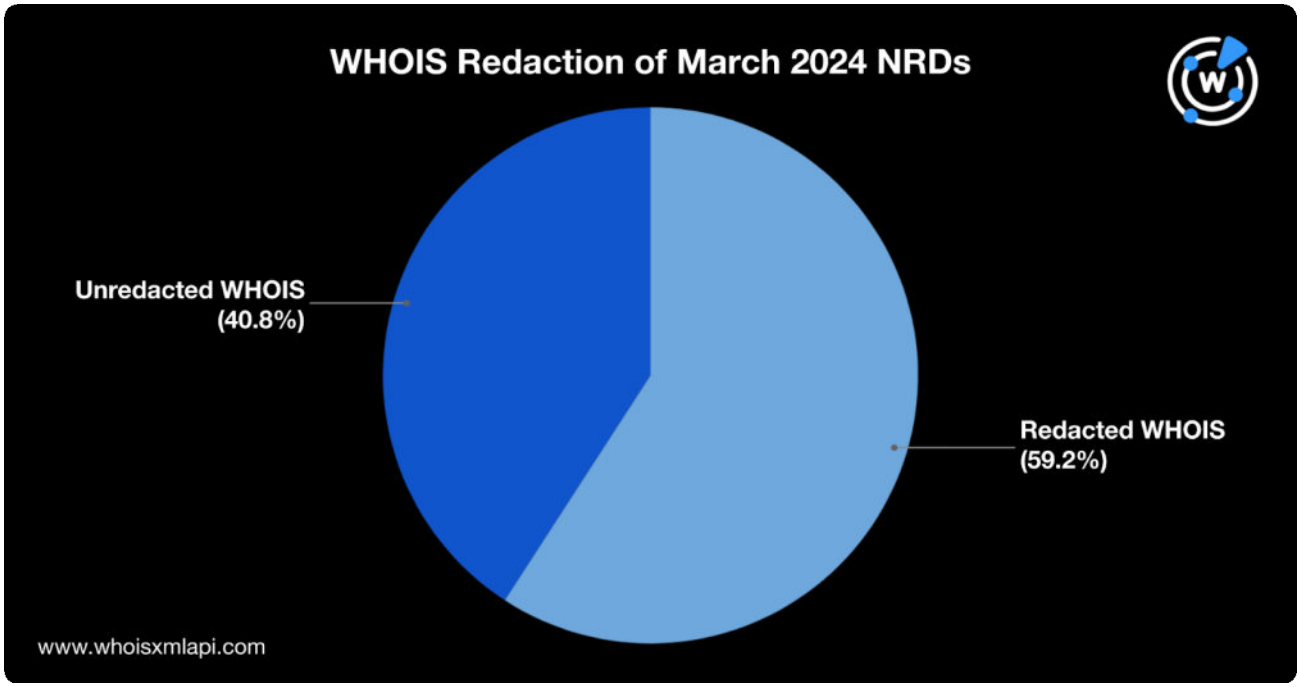
レジストラの分布

2024年3月のNRDで最も多く利用されたレジストラはGoDaddy.com LLC（全NRD登録数の18%）でした。トップ10の残りは、Namecheap, Inc.（11.2%）、GMOインターネットグループ（3.6%）、NameSilo LLCとTucows Domains, Inc.（各3.4%）、Dynadot（3%）、Alibaba Cloud Computing Ltd.（2.6%）、Gname.com Pte. Ltd.とHostinger Operations UAB（各2.2%）、Squarespace Domains LLC（1.9%）となりました。



WHOISデータの非公開化

非公開化されたWHOISレコードが増加しています。プライバシー保護のためWHOISレコードを編集・非公開化していたNRDは、2月には全体の58.6%でしたが3月は59.2%に増加しました。他方、40.8%はWHOISレコードを未編集の状態で公開していました。

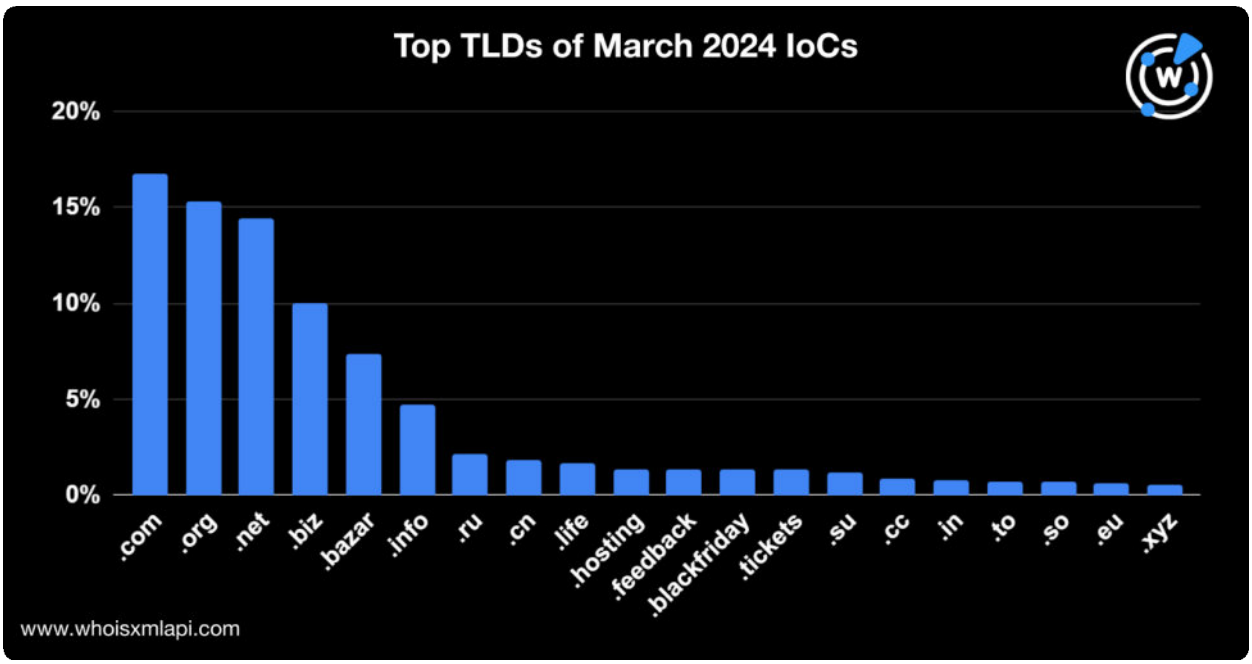


DNSのレンズで見るサイバーセキュリティ

3月のIoCのトップTLD

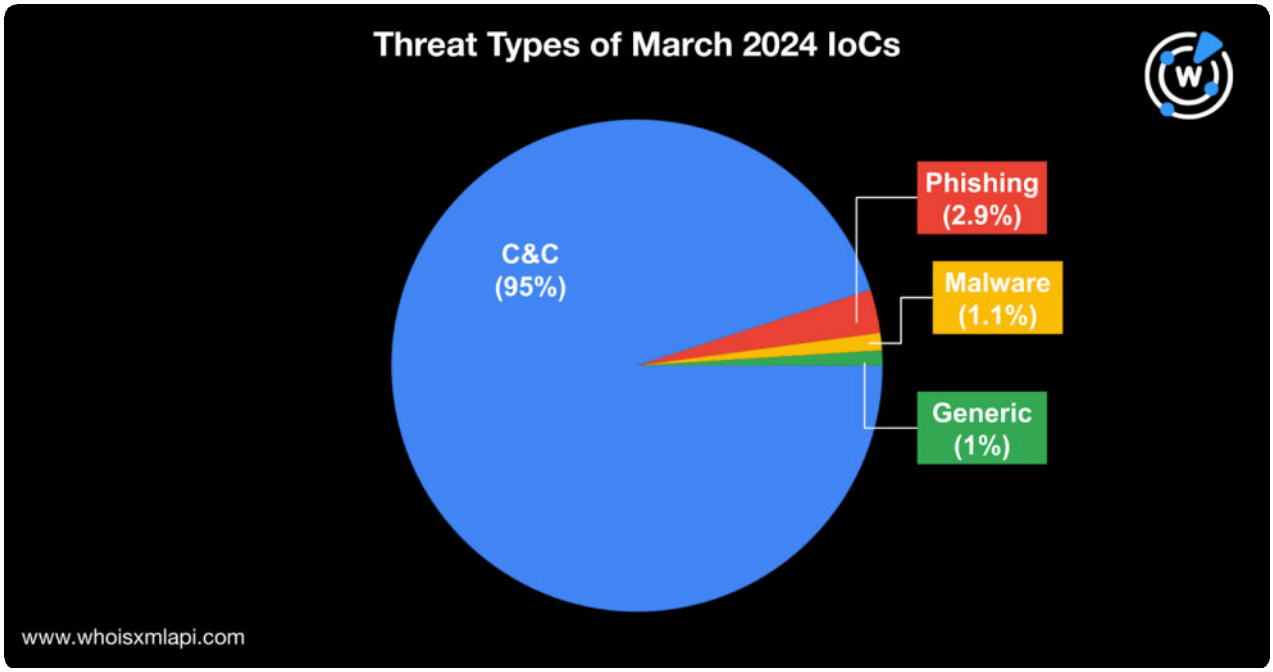
次に、脅威との関連で3月にIoCとしてタグ付けされた110万超のドメイン名を分析しました。

IoCに最も多く見られたTLDは.comで、全体の16.8%を占めました。次いで多かったのは、.org（15.3%）、.net（14.4%）、.biz（10%）でした。また、.ru（2.2%）、.cn（1.8%）、.su（1.2%）、.in（0.8%）など、ccTLDを使ったIoCもありました。



3月のIoCの脅威タイプ別内訳

3月に検出されたIoCを関連している脅威のタイプ別に分類したところ、95%がコマンド＆コントロール（C&C）サーバーでした。残りは、フィッシングキャンペーン（2.9%）、マルウェア配布（1.1%）およびその他のサイバー攻撃（1%）に分類されました。



脅威レポート

当社が3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。

- **アプリインストーラーの悪用につながる不審なダウンロードページを特定**：Microsoftのアプリインストーラーを悪用したキャンペーンのIoCリストをもとに、WhoisXML APIの研究者が1,100を超える関連アーティファクトを特定しました。

- **ResumeLootersのさらなる兆候をDNSでチェック**：ResumeLootersに関連する15個のIoCを分析し、数百の関連アーティファクトを発見しました。

- **macOSバックドアの台頭をDNSで追跡**：RustDoorおよびKandyKornというmacOSのバックドアに関与したIoCを分析し、IoCとされたドメイン名と同じメールアドレスを使用していたドメイン名5個、IoCとされたIPアドレスを使用していたドメイン名28個を検出しました。

- **DNSで潜在的なプロパガンダツールの存在を調査**：PAPERWALLのIoC 132個を当社で分析し、PAPERWALLのドメインIoCと同じメールアドレスを使用しているドメイン名681個を含む多数の関連アーティファクトを探し出しました。

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。