ドメイン名動向ハイライト：2024年1月

WhoisXML APIの研究者がこのほど、2024年1月1日～31日に新規登録された700万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。

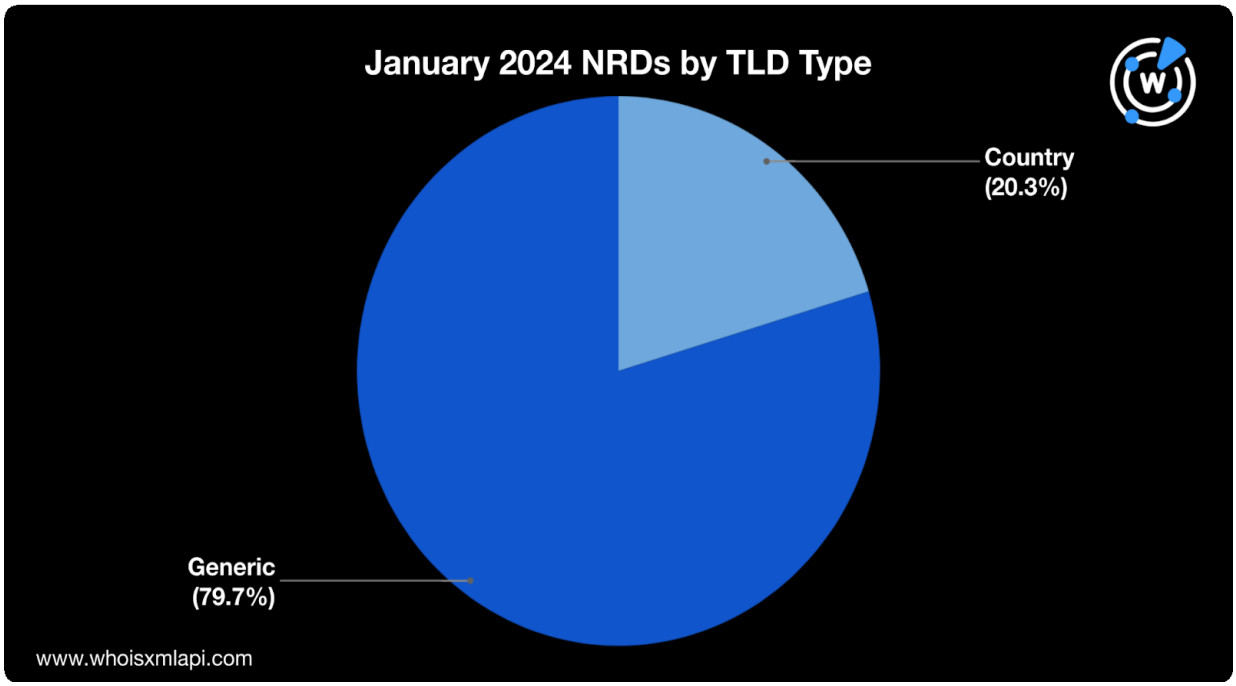
また、2024年1月にセキュリティ侵害インジケーター（IoC）としてタグ付けされた110万超のドメイン名について、そのTLDの使用状況や脅威の種類を調査しました。

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。

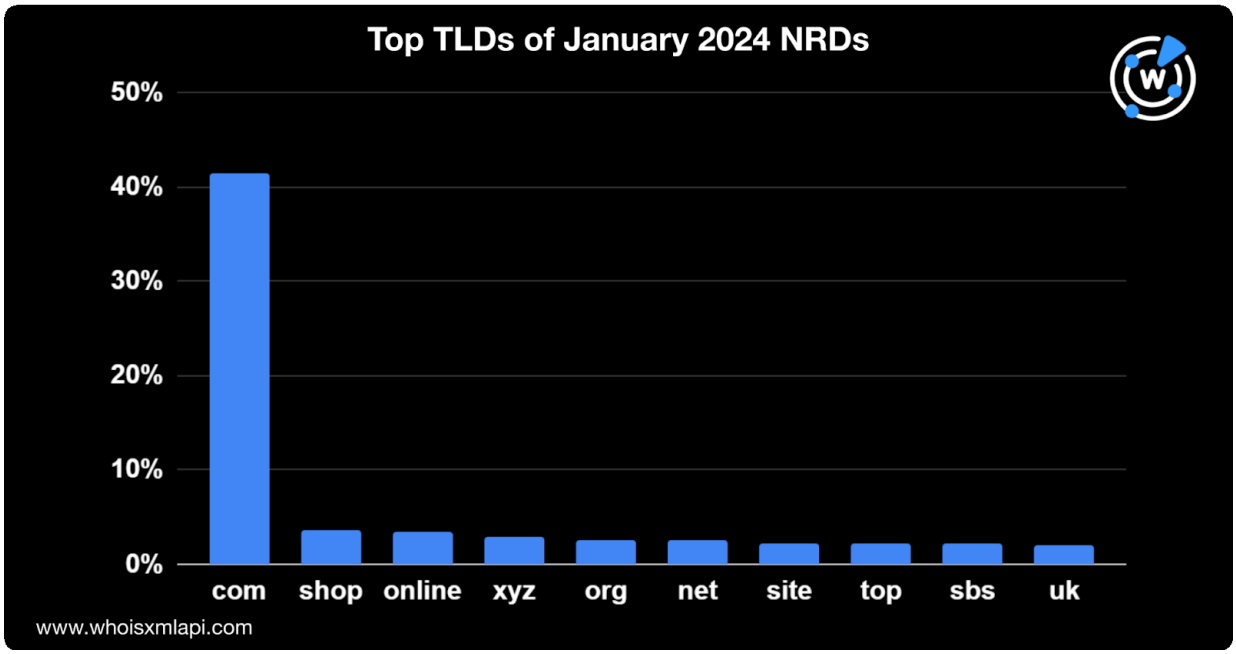
1月の新規登録ドメイン名（NRD）をクローズアップ

TLDの分布

2024年1月に登録された700万ドメイン名のうち、79.7%は分野別TLD（gTLD）、20.3%は国コードTLD（ccTLD）を使ったドメイン名でした。



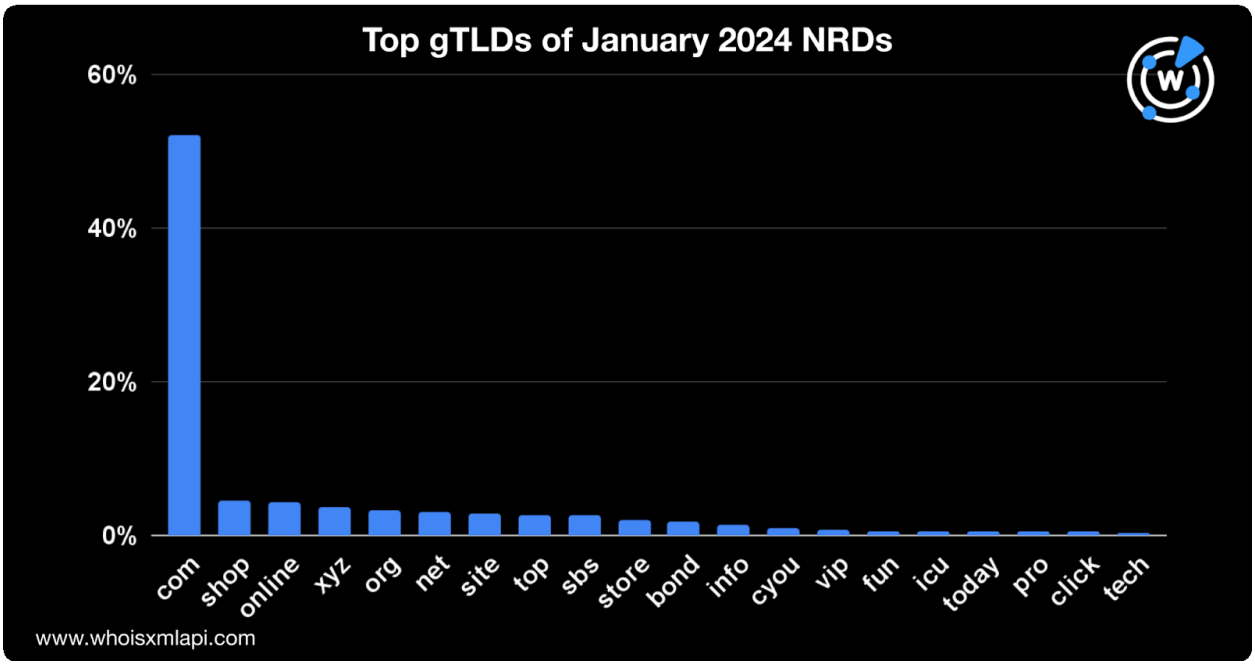
新規登録ドメイン名（NRD）に最も多く使われていたTLDは、NRD全体の約41.5%を占めた.comでした。次いで多かったのは、.shop（3.6%）、.online（3.5%）、.xyz（3%）、.orgと.net（各2.5%）、siteと.top（各2.2%）、.sbs（2.1%）、.uk（2%）です。



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。

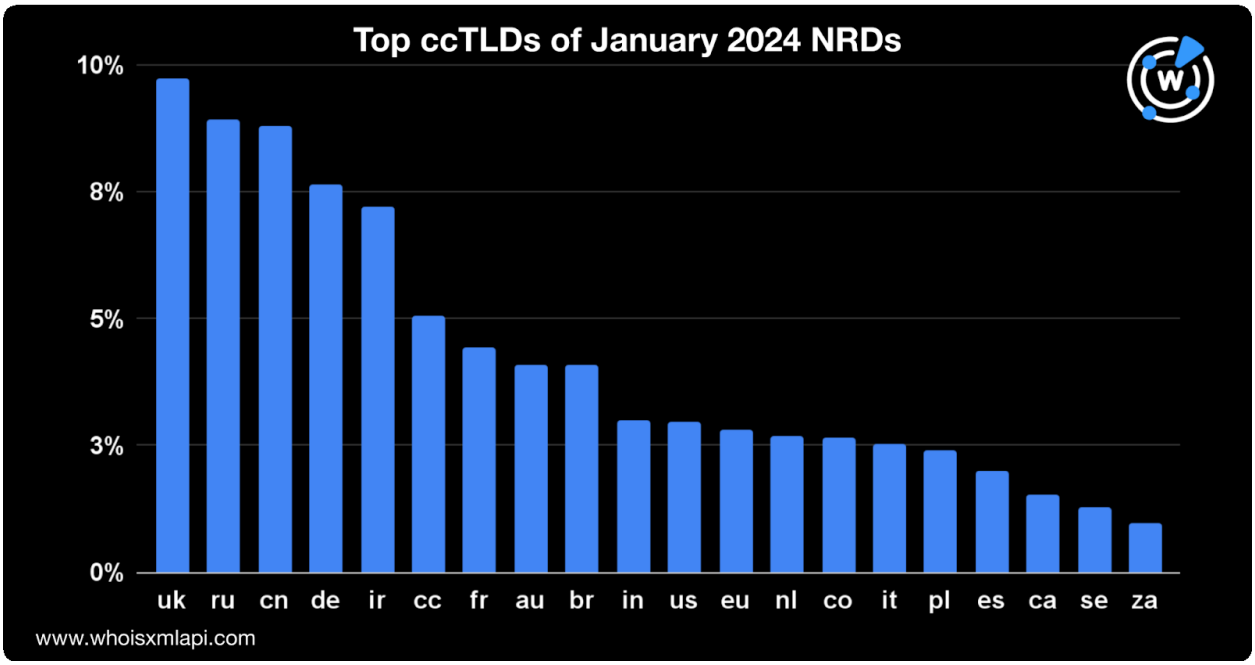
625あまりのgTLDの中で最も使われていたのは.comで、gTLD下に登録されたNRD総数の52.1%を占めました。

2位以下は.comに大差をつけられました。2位はeコマース関連の.shop（4.5%）、3位は.online（4.4%）でした。そして、これに.xyz（3.8%）、.org（3.2%）、.net（3.1%）、.site（2.8%）、.topと.sbs（各2.7%）、.store（2%）、.bond（1.8%）、.info（1.4%）、.cyou（1%）、.vip（0.8%）、.funと.icu（各0.6%）、.today、.proおよび.click（各0.5%）、.tech（0.4%）が続きました。



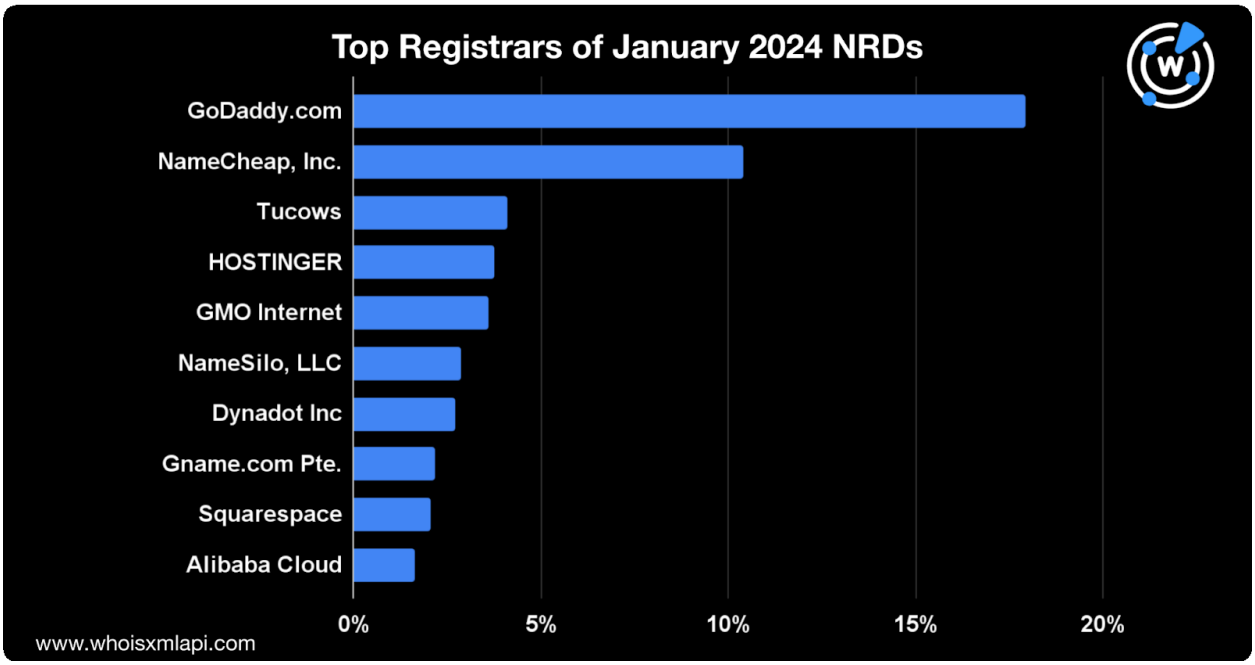
他方、230超存在するccTLDの中で最も人気が高かったのは.ukで、ccTLD下で登録されたNRDの9.7%でした。

次いで多かったのは、.ru（8.9%）、.cn（8.8%）、.de（7.7%）、.ir（7.2%）、.cc（5%）、.fr（4.4%）、.auと.br（各4.1%）、.inと.us（各3%）、.eu（2.8%）、.nlと.co（各2.7%）、.it（2.5%）、.pl（2.4%）、.es（2%）でした。残りのトップ20は、.ca（1.5%）、.se（1.3%）、.za（1%）となりました。以上を合計すると、1月のccTLDによるNRDの84.8%になります。



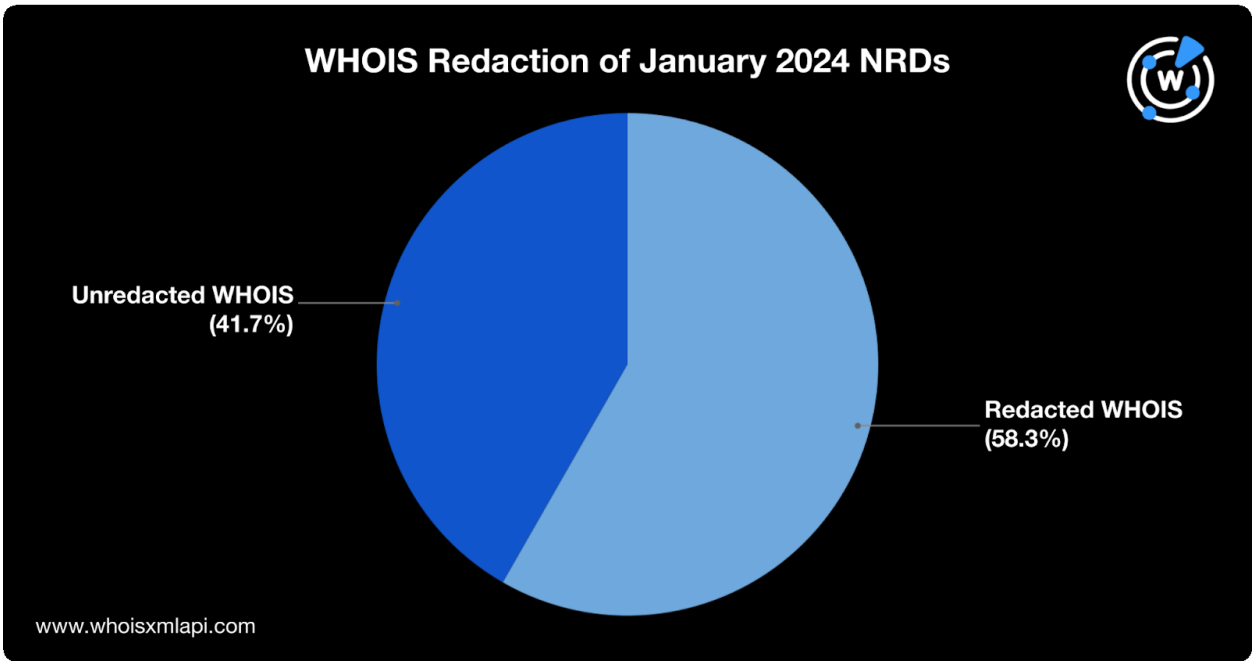
レジストラの分布

2023年12月と同様に、2024年1月のNRDで最も多く利用されたレジストラはGoDaddy（全NRD登録数の18%）で、2位はNamecheap, Inc.（10.4%）でした。トップ10の残りは、Tucows（4.1%）、HOSTINGER（3.8%）、GMOインターネットグループ（3.6%）、NameSilo LLC（2.9%）、Dynadot, Inc.（2.7%）、Gname.com Pte. Ltd.（2.2%）、Squarespace Domains LLC（2.1%）、Alibaba Cloud Computing Ltd.（1.6%）となりました。



WHOISデータの非公開化

1月のNRDの58.3%は、WHOISレコードを編集・非公開化していました。他方、41.7%はWHOISレコードを未編集の状態で公開していました。

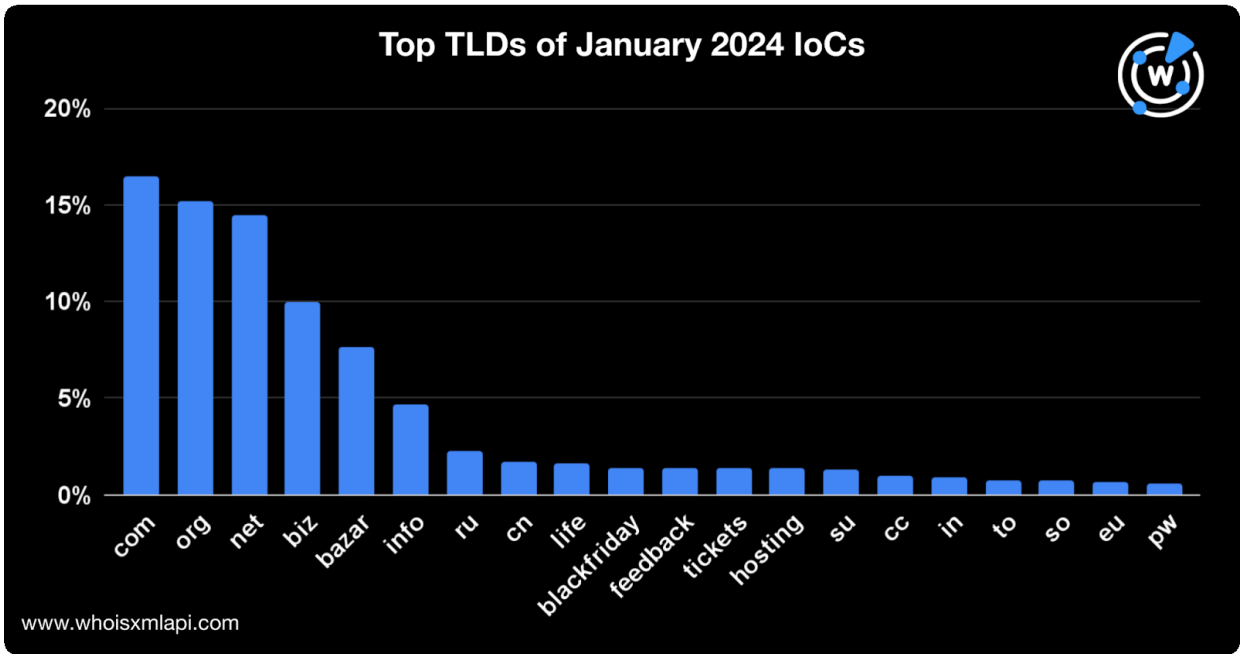


DNSのレンズで見るサイバーセキュリティ

1月のIoCのトップTLD

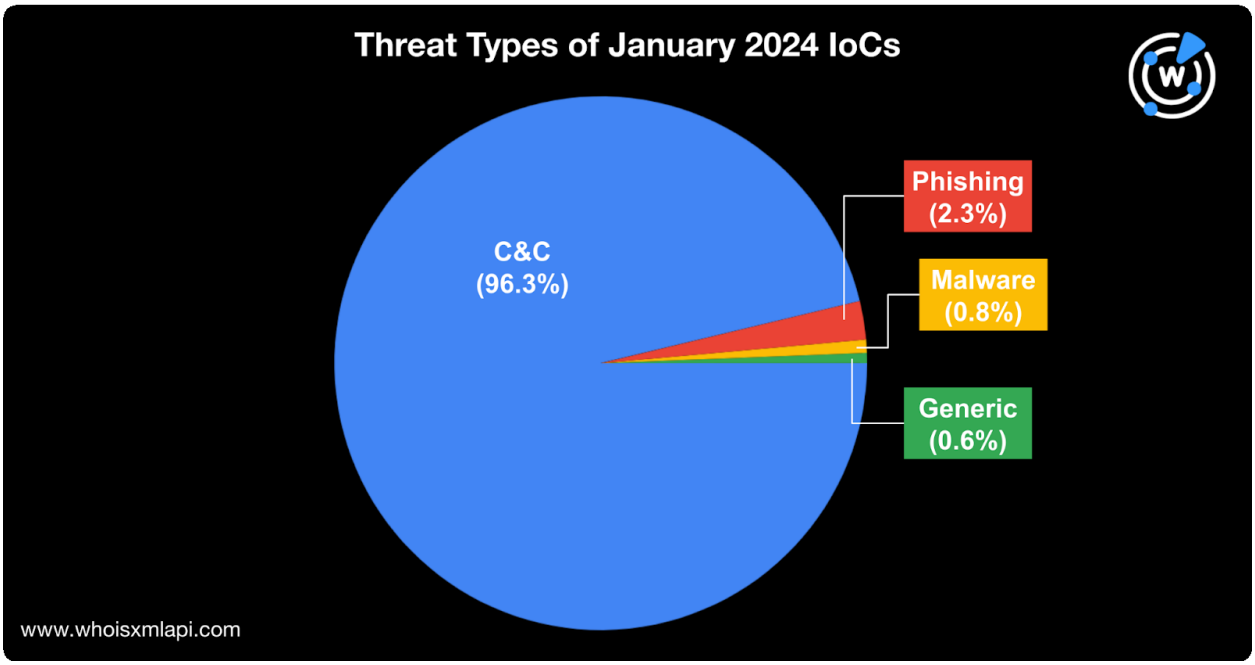
次に、さまざまな脅威との関連で1月にIoCと特定された110万超のドメイン名を分析しました。

IoCに最も多く見られたTLDは.comで、全体の16.5%を占めていました。次いで多かったのは.org（15.2%）、.net（14.4%）、.biz（10%）でした。また、.ru（2.3%）、.cn（1.7%）、.su（1.3%）など、ccTLDを使ったIoCもありました。



1月のIoCの脅威タイプ別内訳

1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、そのほとんど（96.3%）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（2.3%）、マルウェア配布（0.8%）およびその他のサイバー攻撃（0.6%）でした。



脅威レポート

当社が1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インテリジェンスでEpsilon Stealerの足跡を辿る**：WhoisXML APIの研究チームが、Epsilon Stealerに関与した133個のセキュリティ侵害インジケーター（IoC）から76個のドメイン名を抽出し、それらをもとに1,700超の潜在的関連アーティファクトを明らかにしました。
- **PikaBotのインフラをDNSで分析**：マルバタイジングによるPikaBotの配布に関わった11個のIoCを出発点として調査を行い、IoCと同じメールアドレスまたはIPアドレスを使用していた数百にのぼる関連ドメイン名を発見しました。
- **不正広告「UNC2975」のインフラを調査**：UNC2975のマルバタイジングキャンペーンに関連する28個のIoCを当社で分析し、関連性が疑われる3,000超のアーティファクトを特定することができました。

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。