ドメイン名動向ハイライト：2023年3月

2023年4月5日

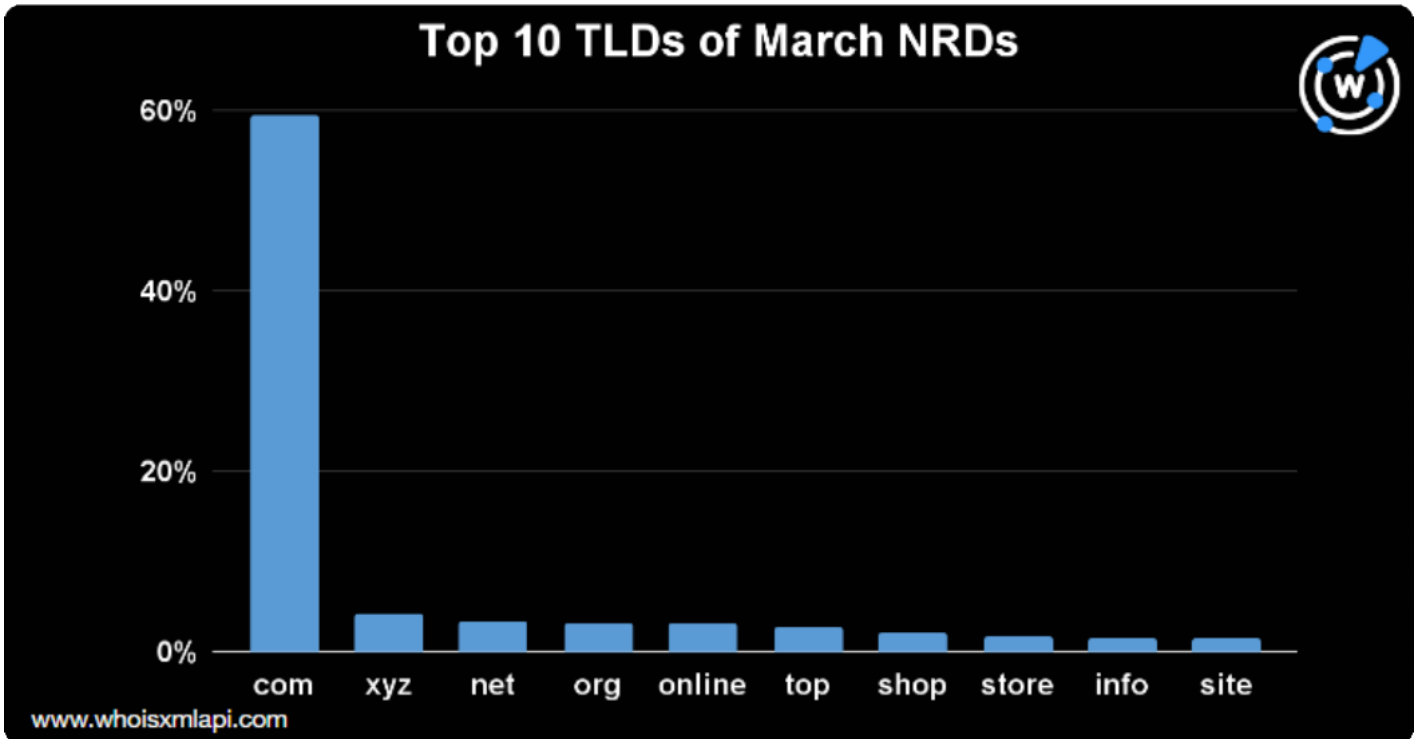
WhoisXML APIではこのほど、2023年3月1日から31日までの期間に登録された数百万個のドメイン名から31,000個を無作為抽出し、登録者の所在国、レジストラおよびTLDの共通点を明らかにしました。また、最もリスクの高い、または最も悪用されているTLDのドメイン名登録数の集計とドメイン名文字列の使用状況の分析も行い、潜在的な新傾向を検出しました。

調査の結果は以下の通りです。また、ドメイン名、DNSおよびIPアドレスのデータを用いて当社研究員が作成した脅威レポートへのリンクを末尾に掲載しています。

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

3月に新規登録されたドメイン名（NRD）で最も多かったTLDは.comで、3月のNRD全体の60％を占めました。.comに次いで多かったのは.xyzと.netで、それぞれ4％でした。そして、.org、.online、.topがそれぞれ3%と、僅差で続きました。電子商取引に特化した.shopと.storeもトップ10に入り、それぞれ2％を占めました。トップ10の最後には、.infoと.siteがそれぞれ2％のシェアでランクインしています。



3月のNRDの約10.6%は、InfobloxがQ4 2022 Cyber Threat Reportで指摘していた最もリスクの高いTLDのドメイン名でした。以下は、悪意あるドメイン名の数が最も多い、高い確度で高リスクと判定されたTLDリストの一部を示しています。

3月のNRD総数に対する各TLDのドメイン名登録数の割合

xyz 4.227%

top 2.855%

buzz 0.777%

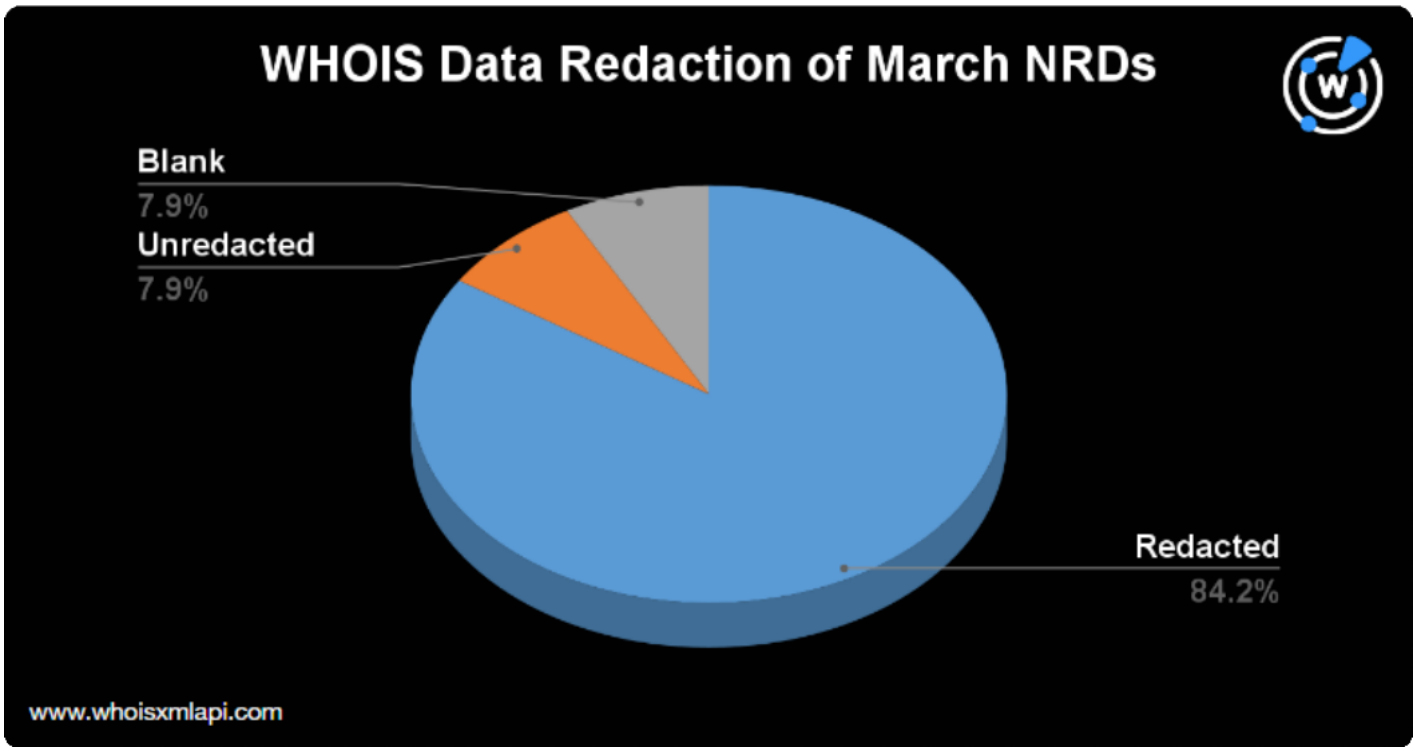
click 0.723%

live 0.579%

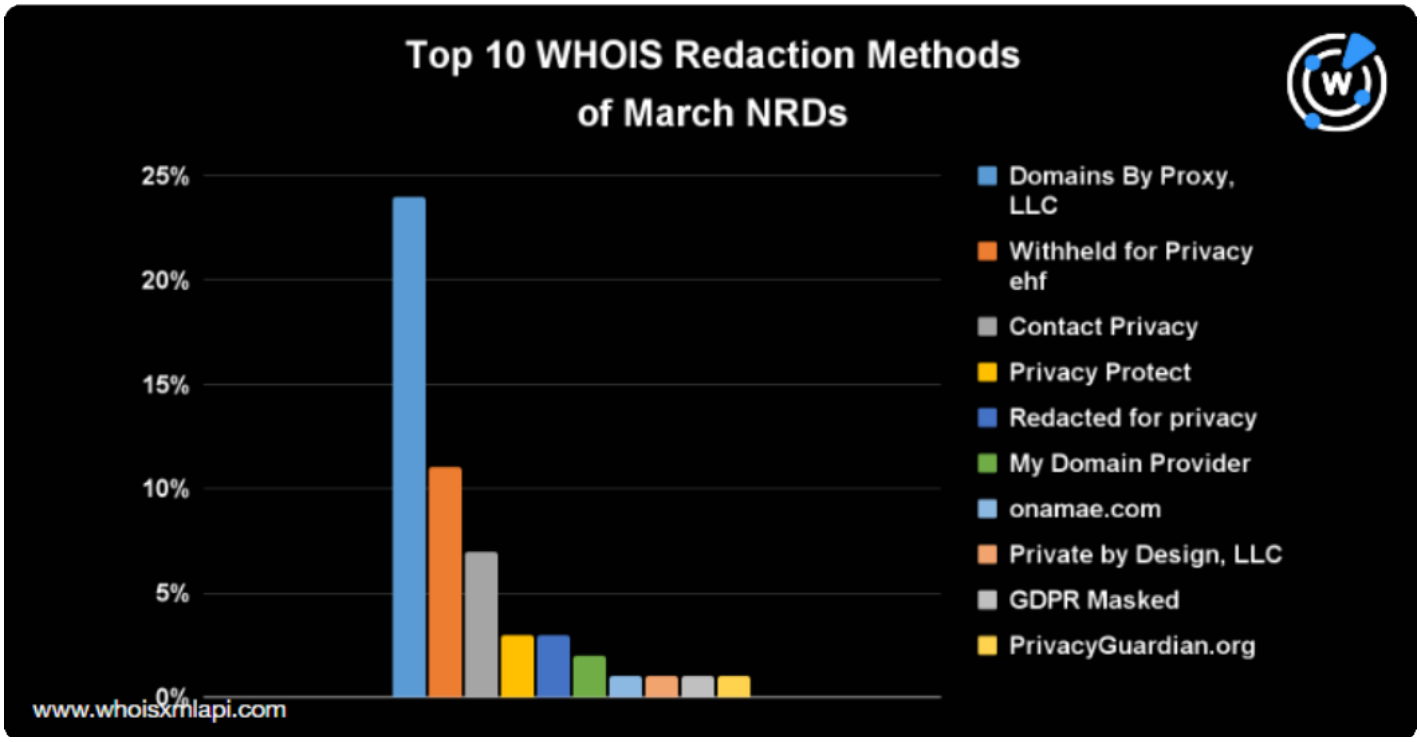
全リストをご覧になりたい方は、こちらまでお問い合わせください。

WHOISデータの非公開化

3月のNRDのうち登録者の情報が公開されていたものはわずか8%で、WHOISデータの非公開化が大規模に実施されていることが浮き彫りになりました。

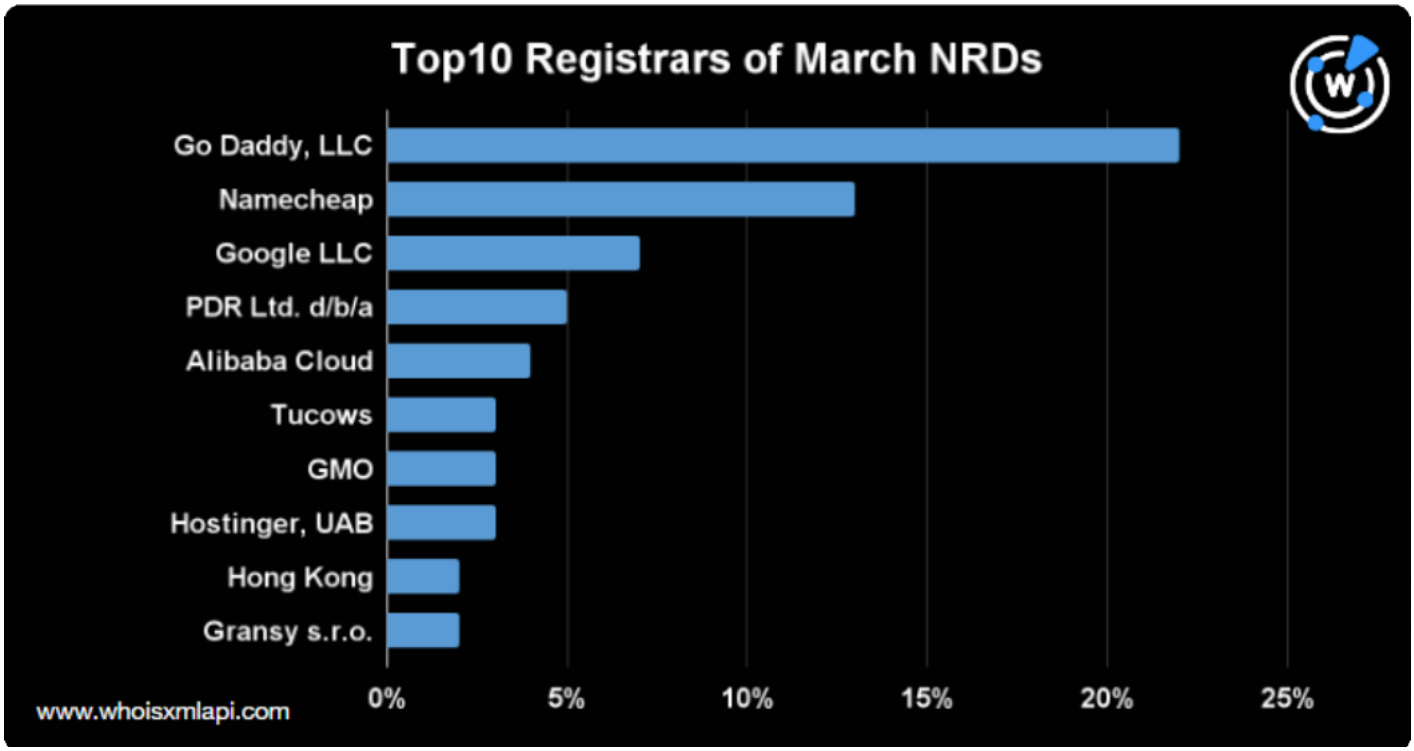


NRDの登録者組織名を見ると、約84%はWHOISレコードを編集しており、そのほとんどがプライバシー保護業者のサービスを利用していました。また、編集のパターンから、WHOISプライバシー保護業者の上位はDomains By Proxy（24%）、Withheld for Privacy EHF（11%）、Contact Privacy, Inc（7%）、Privacy Protect LLC（3%）であることがわかりました。よく使われているプライバシー保護業者のトップ10を以下に示します。



レジストラの分布

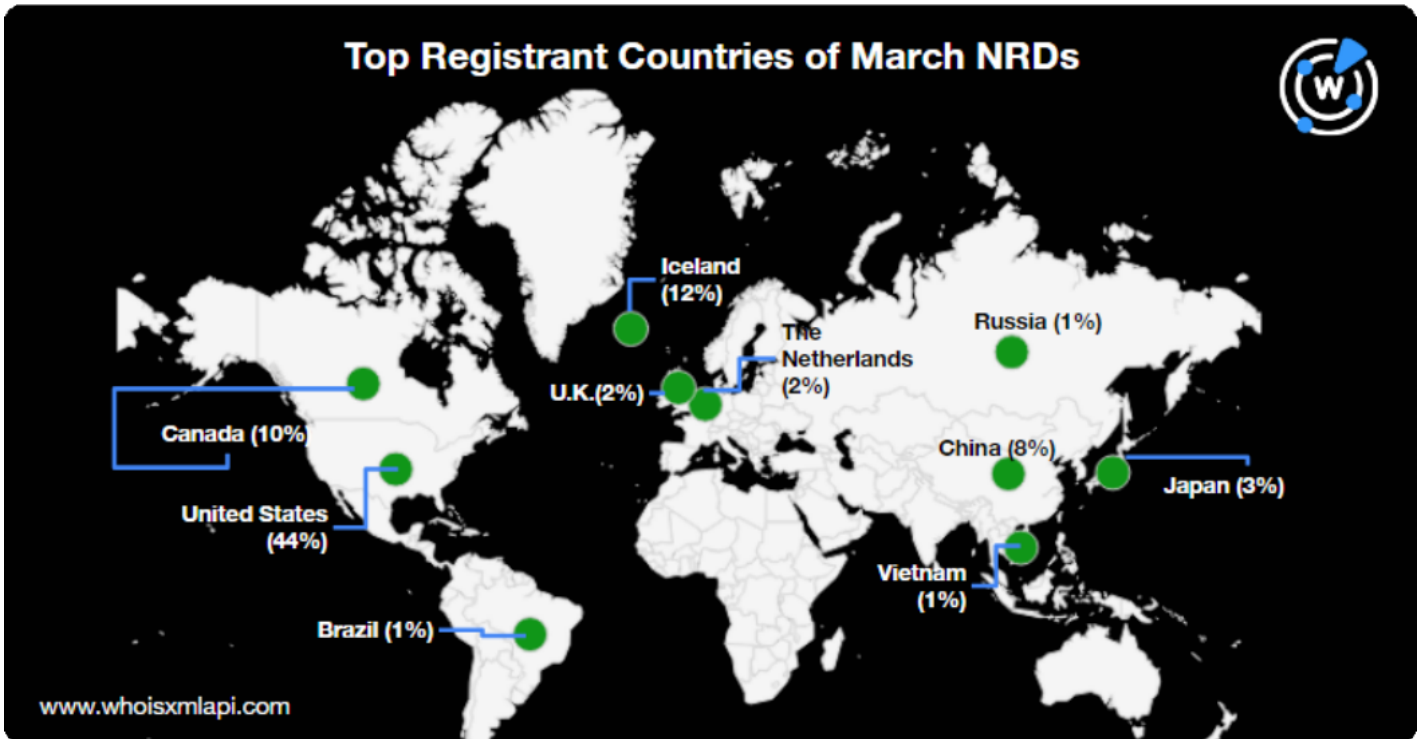
1月および2月と同様に、ドメイン名の登録数が最も多かったレジストラはGoDaddyで、登録数全体の22%を占めました。トップ10も1月、2月とほぼ同じレジストラが占めています。2位はNamecheapで13%のシェアとなり、次いでGoogleとPDR Ltd.がそれぞれ7%と5%を占めました。さらに、Alibaba（4%）、Tucows（3%）、GMO（3%）、Hostinger（3%）、Hong Kong Juming Network Technology Co. (2%)、Gransy S.R.O.（2%）の順となっています。



3月はトップ10のレジストラが総登録数の63%を占めました。残りのドメイン名は、350以上の他のレジストラに分散していました。

登録者数上位の国

3月のNRDのうち約44%が米国で登録され、12%がアイスランド、10%がカナダで登録されたものでした。その他、3月の登録者数上位10カ国には、中国、日本、オランダ、英国、ロシア、ブラジル、ベトナムがランクインしました。



第2レベルドメイン（SLD）に共通して見られる文字列

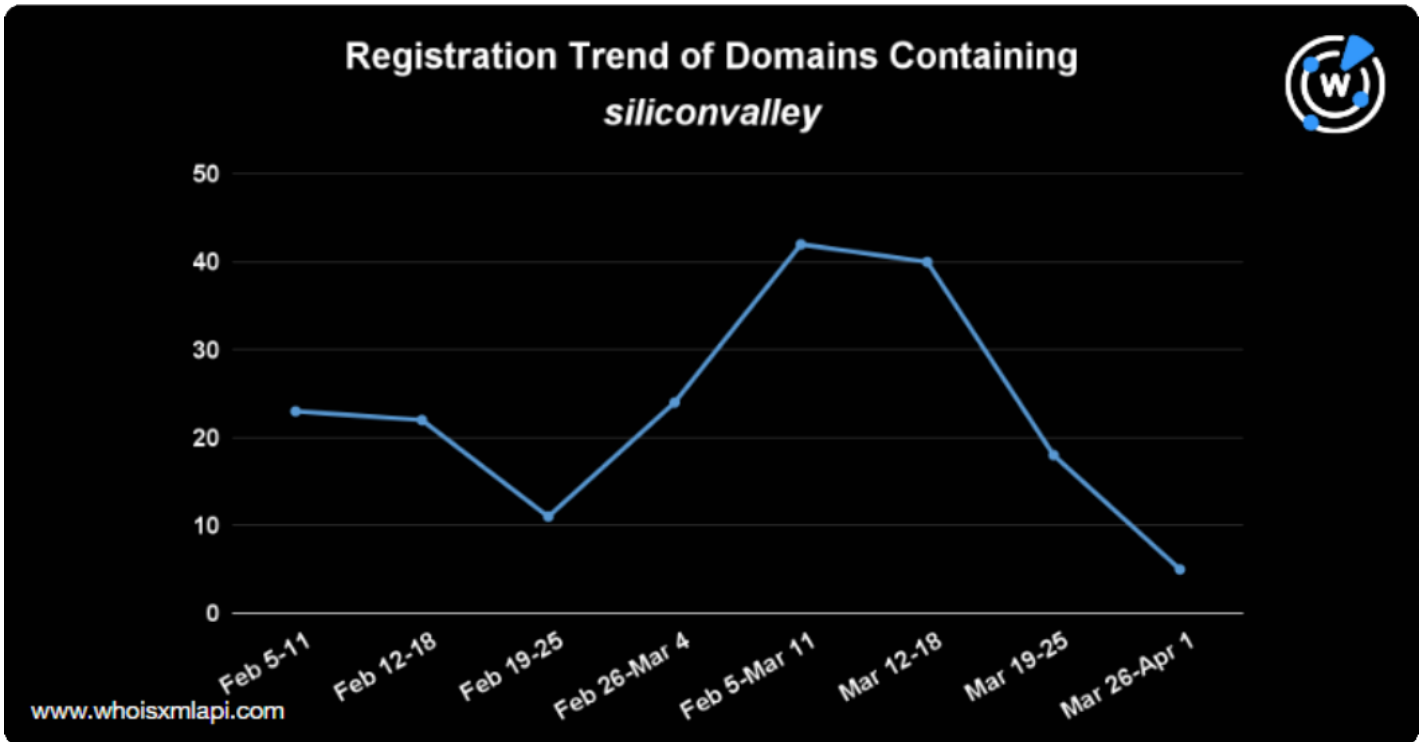
Xnはこの数カ月間最も多く使われている文字列の一つであり、国際化ドメイン名（IDN）の人気が続いていることを物語っています。また、***online***、***home***、***service***といった一般名称もNRDの文字列として引き続き多く使われています。

その他、***ai***、***digital***、***app***、***web***などの技術用語も多く見られました。それらを含む、NRDによく使われていた文字列は下図の通りです。

WhoisXMLAPI

注目を集めたニュース

3月の出来事の中でも、シリコンバレーバンクの破綻をめぐる騒動は特に注目を集めました。下のグラフは、これがDNSにどう反映されたかを示すスナップショットです。シリコンバレーバンクが破綻した週に、***siliconvalley***を含むドメイン名の登録が急増したことがわかります。なお、3月末になるとその登録数は減少しました。



DNSのレンズで見るサイバーセキュリティ

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。

- **DNSの顕微鏡でLorec53のフィッシングを精査**：APTグループ「Lorec53」がフィッシングやマルウェア配布のキャンペーンで使用したとされるセキュリティ侵害インジケーター（IoC）の公開リストをもとに、WhoisXML APIの研究者が調査しました。その結果、1,800超のアーティファクトが追加で検出されました。

- **貴社のイントラネットは大丈夫ですか？DNSにおけるイントラネットのなりすましを調査**：最近のRedditのセキュリティインシデントを受け、DNSにおけるイントラネットのなりすましを調査した結果、人気のイントラネットプロバイダーを標的とする、最近登録された数百のサイバースクワッティングドメインを特定しました。

- **国際的詐欺にWHOISとDNSのスポットライトを当てる**：ネット詐欺に使われるメールアドレスをIoCリスト拡張によって分析した結果、3,000超の関連ドメイン名が判明しました。

- **ヘルスケア関連のIoCをもとにEHRのなりすましを検知**：医療機関を標的とする脅威の1つを当社で調べてみました。CubaランサムウェアのIoCを精査したところ、有名な電子健康記録（EHR）ソフトウェアのベンダーをターゲットにした何千ものアーティファクトとサイバースクワッティングドメインが発見されました。

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支援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。