ドメイン名、IP、DNSデータに関する24のトレンドとサイバーセキュリティ統計：2022-2023年

2023年3月20日

ドメイン名とDNSの集約データは、セキュリティ研究者、企業および各種のソリューションに役立つ豊富なインテリジェンスの源であり、脅威の検知と対応、アタックサーフェス管理（ASM）、サードパーティー・リスク管理、ブランド保護、IDおよびアクセス管理（IAM）を含むさまざまな業務やサイバーセキュリティのプロセスにおける文脈情報を提供します。

WhoisXML APIは長年にわたってさまざまなサイバー調査を実施してきましたが、このたび、最新の調査から注目に値する事実と統計データをピックアップして以下にまとめました。

脅威、悪意あるキャンペーンおよびマルウェアファミリーに関する統計

当社では、さまざまな悪意ある行為に関与したセキュリティ侵害インジケーター（IoC）のリストを継続的に精査し、拡充しています。そうした当社の調査を通じて見えてきた脅威アクターに関する重要な傾向を以下に示します。

- IoCと特定され、米国以外の国/地域を拠点とする脅威アクターに使用されたIPアドレスの60%は、地理的に米国内に位置。
- IoCと特定され、米国以外の脅威アクターが使用したIPアドレスの所在国としては、米国のほかオランダ、日本、タイが上位に挙がった。
- IoCと特定され、米国以外の脅威アクターが使用したドメインとURLの69%は、その登録者の国として米国を指していた。

- IoCと特定され、米国以外の脅威アクターが使用したドメイン名やURLの上位登録国として、米国に加えてロシア、中国、オランダが挙がった。

注：上記の統計は、シリア電子軍、Hiveランサムウェアのキャンペーン、BlackEnergyを利用したDDoS攻撃およびDucktailの背後にある脅威と脅威アクターの分析をもとにしています。これらの分析は、2022年10月から2023年2月にかけて当社が行ったものです。

なりすましまたはサイバースクワッティングに関する統計

新規登録ドメイン名（NRD）は、フォーチュン500企業を狙ったブランドなりすましやフィッシング攻撃によく使われています。サイバースクワッティングやドメインなりすましの傾向を業界横断的に調べた結果、以下のことがわかりました。

- 大手金融機関のブランド名を含むNRDの99.04%は、そのブランドの正規ドメイン名とWHOISレコードが一致しなかった。
- 主要なチャットアプリのブランド名を含むNRDの97.81%は、そのブランドの正規ドメイン名とWHOISレコードが一致しなかった。
- 電子健康記録（EHR）ソフトウェアの主要開発会社の名称を含むNRDの99.41%は、それらの会社の正規ドメイン名とWHOISレコードが一致しなかった。
- フォーチュン500企業になりすますために登録されたと思われるドメイン名とサブドメインのうち、12%は悪意あるものと判明。残りの88%は悪用されていない可能性があるものの、悪意ありと判断されたドメイン名に見られる不審なパターンを共有している。
- フォーチュン500企業になりすました悪意あるドメイン名の79%は、緊急性の高い文字列（***auth***、***login***、***pay***、***register***、***update***など）を使用。残りの21%はマーケティング、サポート、財務、セキュリティなどの企業部門を偽装していた。
- CEOやフォーチュン500企業を標的としたサイバースクワッティングドメインのIPホストを管理する上位10社のうち4社が、スパムやボットネット感染の点で最悪のISPに該当。

注：上記の統計は、Gigabud RAT、サプライチェーン攻撃、ヘルスケア関連のサイバー攻撃、Google広告によるマルウェア配布、および企業のなりすましについて当社が行った分析をもとにしています。これらの調査は、2022年7月から2023年2月にかけて実施しました。

テーマ・イベント別の統計

また、世界的な事件やニュースがDNS、特にドメイン名登録に与える影響についても追跡調査しました。当社が注目した主なテーマおよびイベント関連の統計は以下の通りです。

- 2022年第2四半期に新規登録された納税申告シーズン関連ドメイン名のうち13%が悪意あるドメイン名。
- 祝日関連のドメイン名登録は、各祝日の日の2〜3週間前に集中。
- ***Russia***または***Ukraine***を含むNRDの数は、2022年のロシアによるウクライナ侵攻開始から1週間で150％増加。
- ***Russia***または***Ukraine***を含むドメイン名の登録は侵攻開始から1カ月後には数千件単位で減少したが、それでも侵攻前の水準を上回っていた。
- 祝日をテーマにしたドメイン名の56%は米国で登録されたが、それらの祝日は複数の国で祝われている。
- 祝日関連のドメイン名の登録者が所在する国として、米国のほか、アイスランド、カナダ、中国が上位を占めていた。
- 祝日関連ドメイン名が名前解決したIPアドレスの80.5%は、米国内に位置していた。

注：上記の統計は、当社のDomain Registration Trends Report—Q2 2022およびAugust 2022: DNS Highlightsをもとにしています。これらの分析は、2022年8月から9月にかけて実施しました。

よく悪用されるTLDに関する統計

2023年初頭、Spamhausが公表した最も疑わしいTLDを使用しているドメイン名数千個の特徴を当社で分析し、ホワイトペーパー「DNS Abuse Trends」にまとめました。以下は主な分析結果です。

- 最も悪用されたTLDのドメイン名のうち約64%はWHOISレコードが編集されており、悪意あるキャンペーンに使用された場合、攻撃主体の帰属特定が困難となることが判明。
- 最も悪用されているTLDの下で登録されたNRDが名前解決したIPアドレスの67%は、地理的に米国に位置。
- 最も悪用されているTLDのNRDが名前解決するIPアドレスのジオロケーションとして多かった国は、米国以外では中国、シンガポールおよびドイツ。
- 最も悪用されているTLDのNRDの28%は、登録者が米国に所在していた。
- 最も悪用されているTLDのNRDの登録者が多い国は、米国のほか中国、アイスランド、英国が上位を占めていた。

不審なドメイン名大量登録に関する統計

複数の脅威アクターが、レジストラの提供する一括大量ドメイン名登録機能を悪用しています。そこで、大量登録されたドメイン名の背後にある不審なパターンを当社で調査し、以下を見出しました。

- 当社のtyposquatting data feed filesを使用した分析によれば、ある日に登録された見た目の似ているドメインの24%超が、同一のレジストラに帰属している可能性がある。
- 脅威アクターが持つドメイン名ポートフォリオの全体は、彼らがある1日に大量登録するドメイン名数の140倍に相当する可能性がある。

—

当社は今後もサイバー脅威の情報源を活用し、脅威や悪意あるインフラの調査およびドメイン名登録トレンドの追跡を続けていきます。

組織のサイバーセキュリティプロセスやソリューションにご活用いただけるWhoisXML API のサービスにご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。