ソリューションノート

類似ドメイン監視は、ネットワーク、顧客、ブランドを保護します

企業への侵害、顧客への危害、または貴重なブランドへの損害を目的とした高度な標的型攻撃において、類似ドメインを使用するソーシャルエンジニアリングの脅威を事前対応的に阻止します。

増大する類似ドメインの脅威

大規模で広範囲にわたる消費者レベルの攻撃から、標的型スピアフィッシング、ビジネスメール詐欺（BEC）、その他の企業脅威に至るまで、類似ドメインは、攻撃者が人的および技術的防御を突破するための重要な要素となっています。攻撃者はブランド、従業員、サプライチェーン、または他の信頼できるパートナーになりすますことができ、壊滅的な結果をもたらす可能性があります。

最初に使用されてからほぼ 20 年が経ちますが、脅威アクターは新しいタイプの攻撃に類似ドメインを適用する新たな方法を生み出し続けています。敵対的中間者（AitM）手法を使って、認証の際に従業員を騙して会社の実際のネットワークとやりとりしているかのように見せかけようとするケースが増えています。

今日、攻撃者はSMSメッセージ、電話、ソーシャルメディアのダイレクトメッセージ、メール、QRコードなどで類似ドメインを利用しています。最近では、ゲーマーからデジタル通貨のマーケットプレイス、ウォレット、取引所まで、あらゆる場所で導入が進んでいる多要素認証（MFA）が、2023年初頭に Coinbase への攻撃で見られたように攻撃者の標的となっており、類似ドメインは、あらゆる主要なサイバー脅威において不可欠な要素となっています。

増大する類似ドメインの脅威

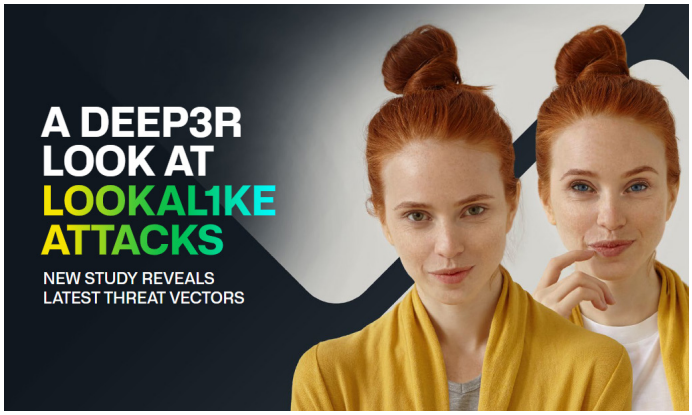

図 1：Infoblox Threat Intelligence が共有した、類似ドメインのリスクの増大に関する驚くべき調査データ。

事実と数字

その他の BloxOne Threat Defense Advanced のセキュリティ機能により、次のことが可能になります。

- 1 年余りで 30 万個以上の類似ドメインを検出
- コンボスクワッティング・ドメインがタイポスクワッティングよりも 100 倍一般的に
- 毎日 20 万の新しいドメインが作成されている
- 2023 年には 1,600 を超えるドメインが公式の MFA サービスを模倣するために使用された
- 60% のコンボスクワッティング・ドメインは 1,000 日以上アクティブである
- .comを使用するだけでなく、今日、攻撃者は他に 1,588 種類の TLDを悪用できる
- DNS はサイバー攻撃の 92% で利用されている

ブランドと顧客を保護

企業の類似ドメインの脅威に対して防御するには、消費者グレードのマスマーケット攻撃とは異なるアプローチが必要です。Infoblox Lookalike Domain Monitoring を使用すると、お客様は、自社や従業員、自社の顧客に対して使用される可能性があるドメインのカスタムリストを独自に管理できます。Infoblox Threat Intelligence は、グローバルレジストラ、ISP、実際の DNS アクティビティなどをモニターし、お客様の監視リストに照らして潜在的に高リスクの類似ドメインを特定し、初期評価と監視を開始します。Lookalike Domain Monitoring のインターフェースは、特定された高リスクの類似ドメインとリスクプロファイルデータを可視化します。これにより、組織は情報に基づいた意思決定を行い、潜在的なネットワーク侵害、顧客への危害、または組織の評判やブランドへの損害を事前対応的に回避できます。

Lookalike Domain Monitoring は個別に利用可能で、Infoblox の業界をリードする DNS Detection and Response（DNSDR）ソリューションである BloxOne Threat Defense Advanced のサブスクリプションに含まれています。これらのソリューションは、高リスクの類似ドメインを監視するためのカスタムドメインの初期セットを特定するライセンスをお客様に提供します。これらのリスクについてより多くのドメインを監視したいお客様は、100 ドメイン単位で追加ライセンスを購入できます。

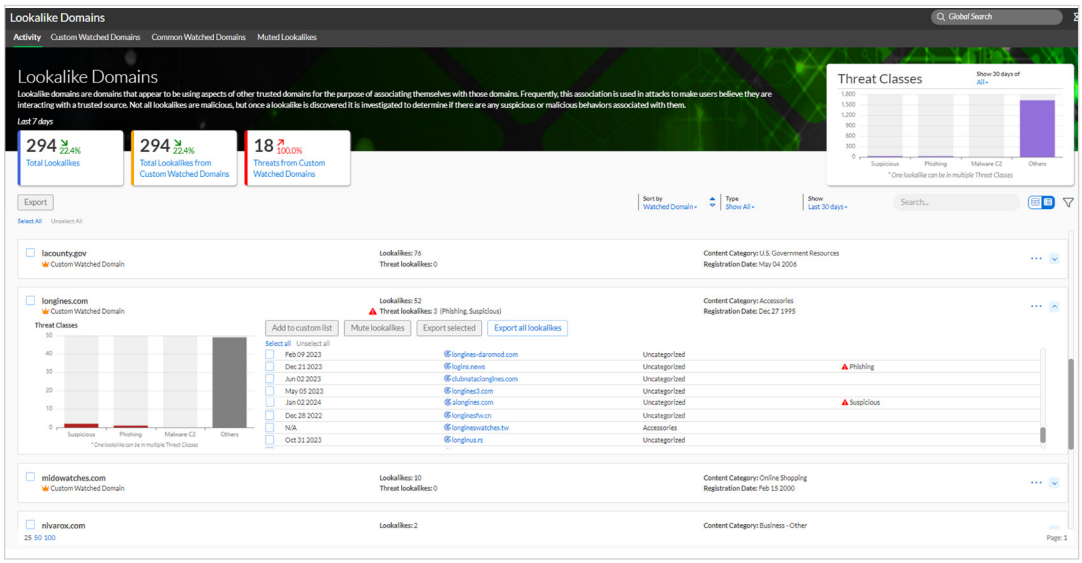

図 2：高リスクの類似ドメインを簡単に確認し、それらがもたらすリスクのレベルを理解する

インターネット詐欺における類似ドメインの悪用を防ぐ

Infoblox は、組織や顧客にリスクをもたらすドメインをお客様が迅速に削除できるように支援する「Domain Mitigation Services」を提供しています。Infoblox は、独自の調査スキル、自動化技術、業界との関係を組み合わせ、データ盗難、サイトのなりすまし、その他のサイバーインシデントなど、業界をリードする時間単位で測定される SLA に伴う問題を迅速かつ慎重に解決します。

Infoblox Domain Mitigation Services の詳細については、こちらをご覧ください
https://insights.infoblox.com/jp-resources/jpr/infoblox-datasheet-infoblox-domain-mitigation-services-jp

Infobloxはネットワークとセキュリティを統合して、これまでにないパフォーマンスと保護を提供します。Fortune 100企業や新興企業から高く信頼され、ネットワークが誰に、そして何に接続されているのかをリアルタイムで可視化し制御することで、組織は迅速に稼働でき、脅威を早期に検知・対処できます。

Infoblox株式会社
〒107-0062 東京都港区南青山
2-26-37
VORT外苑前I
3F

03-5772-7211
www.infoblox.com/jp

© 2024 Infoblox, Inc.All rights reserved.Infoblox ロゴ、およびここに表示されているその他のマークは、Infoblox, Inc. の所有物です。
他のすべてのマークは、それぞれの所有者に帰属します。

バージョン：20240125v3