infoblox

Threat Intel

ソリューション ノート

脅威の兆候を検知する：DNSベースのセキュリティ監視と対策

数字から見る DNSベースのセキュリティ対策の必要性

- DNS の範囲は膨大です。現在、1,589 のトップレベルドメインがあり、毎日 20 万個の新しいドメインが誕生しています。
- 2023 年サイバーセキュリティグローバル調査によると、過去 12 か月間にフィッシング攻撃を 1 回以上受けた組織の割合は 81% にのぼります。
- 2024 年の Proofpoint フィッシングレポートによると、75% の組織がスミッシング（SMSフィッシング）攻撃に遭っています。
- 類似ドメインは、フィッシング攻撃やスピアフィッシング攻撃で頻繁に利用されています。Hacker News によれば、中国のハッカーは 2022 年に大規模なフィッシング攻撃キャンペーンで 4 万 2,000 個の偽ドメインを使用しました。
- 攻撃者は、類似ドメインだけでなく、幅広い攻撃で使用するために数か月前からドメインを登録するケースが多数あります。その 1 例である Decoy Dog ツールキット は、Infoblox Threat Intel によって最初に発見されました。Decoy Dog が使用するロシアの C2 ドメインの多くは、事前にセットアップされ、2022 年秋に Infoblox によって検出されました。
- Infoblox は毎週約 2万5,000 個の新しい類似ドメインを発見し、ブロックしています。
- **結論：**今後、攻撃で使用される恐れのある新興ドメインを事前に発見する脅威インテリジェンスが不可欠となっています。

課題

攻撃者がフィッシングを好む理由はコストの低さにあり、たった 1 人のユーザーが誤ってリンクをクリックするだけで十分だからです。スミッシング（SMS フィッシング攻撃）は最近、発生頻度が増しており、攻撃者は持続的なスミッシング活動を大規模に展開しています。類似ドメインはフィッシングやスピアフィッシング攻撃で多用され、2022 年には中国のハッカーが 4 万 2,000 個の偽装ドメインを用いて大規模なフィッシング攻撃を繰り広げました。

フィッシングや類似ドメインといった問題が増大する一方で、攻撃で使用される数か月前に、ドメインが登録される事例も発生しています。最近発見された一例が C2 インフラとの通信に DNS を悪用するビーコンツールである Decoy Dog ツールキットです。このツールキットは、過去に国家レベルの攻撃者と関連付けられることが多かった Pupy RAT を使用しています。Decoy Dog に関連するドメインの多くは 2022 年 4 月から活動しており、持続的で目立たないため、従来のセキュリティツールでは発見が困難でした。

攻撃開始のかなり前にドメインがセットアップされるタイプの攻撃を検出するには、手法を変える必要があります。

DNS ベースの脅威ハンティング

DNSベースの脅威ハンティングは、大規模なDNSと分析を活用して、実際の攻撃が始まる前に敵のインフラストラクチャを追跡します。具体的には、次のことができます。

- レジストラ、TLD ドメイン、SSL 証明書、ネームサーバー、登録行動などのメタデータを使用して、お客様にとって新規であるドメインを検出し、それらを新規/新興、または不審なドメインに分類します。
- 例えば CISA アドバイザリのような公開されたサードパーティのアドバイザリを取得し、それを拡張して、DNS メタデータを使用してより多くの指標を見つけます。たとえば、最近の CISA の発表で、Infoblox は、DNS メタデータを活用する能力に基づいて、勧告に含まれていなかった 13 のドメインを追加で発見しました。これは潜在的な脅威ベクトルを大幅に削減するのに役立ちました。

DNS ベースの脅威ハンティングは、不審なドメインが悪意のあるものであり、攻撃に使用されたことが確認される数週間から数か月前の時点に、こうしたドメインから保護します。

BLOXONE THREAT DEFENSE を使用して早期保護を実現

BloxOne Threat Defense は、クエリパス内での Infoblox の独自の立ち位置を利用して、通信の意図を目撃、分析、ブロックし、早期保護を実現します。DNS 市場の最大手としての豊富な専門知識を活かして、敵のインフラを追跡し、DNS ログを精査して、脅威ライフサイクルの早い段階（「侵害」意図を持つアクターが実際に攻撃を開始する前に）で不審な活動を検知します。これにより、Infoblox Threat Intel は、悪用を目的とした新しいドメインと類似ドメインを武器化フェーズで特定でき、他のセキュリティ組織やベンダーが悪質ドメインとして検出が可能になる数週間から数か月も前の時点に、不審ドメインとして分類します。Infoblox が他のソリューションよりこれほど早く不審ドメインと分類できる主な理由は、他のセキュリティソリューションがこれらドメインに関連するトラフィックの挙動やコンテンツという、通常、脅威活動が活発化した後にのみ、関連性が現れる側面を評価対象とすることにあります。

高リスクドメイン

Infoblox は「不審」と判断した特定ドメインを、BloxOne Threat Defense で利用可能な、「Infoblox High Risk（Infoblox 高リスク）」というフィードに追加して、お客様が新しく台頭中の脅威から事前に身を守れるようにします。これらのフィードには不審度の高いドメインの指標が付いています。具体的には、悪質な活動との関連性はまだ確認されていないドメインのうち、武器化段階で脅威アクターによって取得された可能性があり、将来、悪用するために有効化される可能性があるものを指します。これらフィードは次の 3 つの区分に分類されます。

- **不審な類似ドメイン** - 正規ドメインに類似し、将来、フィッシング活動に利用される可能性があるタイプです。
- **不審な NOED** -（「Newly Observed Emergent Domains」新たに観測された新興ドメイン） - 顧客トラフィック内で最近観測されたばかりの（すなわち「Emergent」（新興））、高リスクなタイプの不審なドメインです。
- **不審なドメイン** - 疑わしく見えるドメインのうち、類似と NOED のいずれのプロファイルにも適合しないタイプのドメインです。

Infoblox は、2022 年 11 月初旬に不審な新興ドメインに関するデータの収集を開始しました。2023 年には、不審な兆しを示すアクティブなドメインを 1,940 万個検出、分類しました。アクティブなドメインのうち不審なものの数は、増加の一途をたどっています。数の膨大さ以外のもう 1 つの重要な基準として、不審という分類の質が上げられます。不審と分類された数百万のドメインのうち、誤検知とフラグされたのはわずか 0.0002% です。

「不審なドメインをブロックする」というコンセプトを掲げたことにより、Infoblox のお客様は Decoy Dog や Oktapus などの MFA 攻撃をはじめとする一部の脅威アクターを早期にブロックしやすくなりました。Decoy Dog ツールキットに関連するドメインの多くは、2022 年の秋には既に発見済みで、BloxOne Threat Defense の不審なドメインフィードに含まれていました。そのため BloxOne Threat Defense Advanced の利用中で不審なドメインフィードをブロックするというポリシーを設定済みのお客様は、それ以降、C2 ドメインの多くから保護されています。

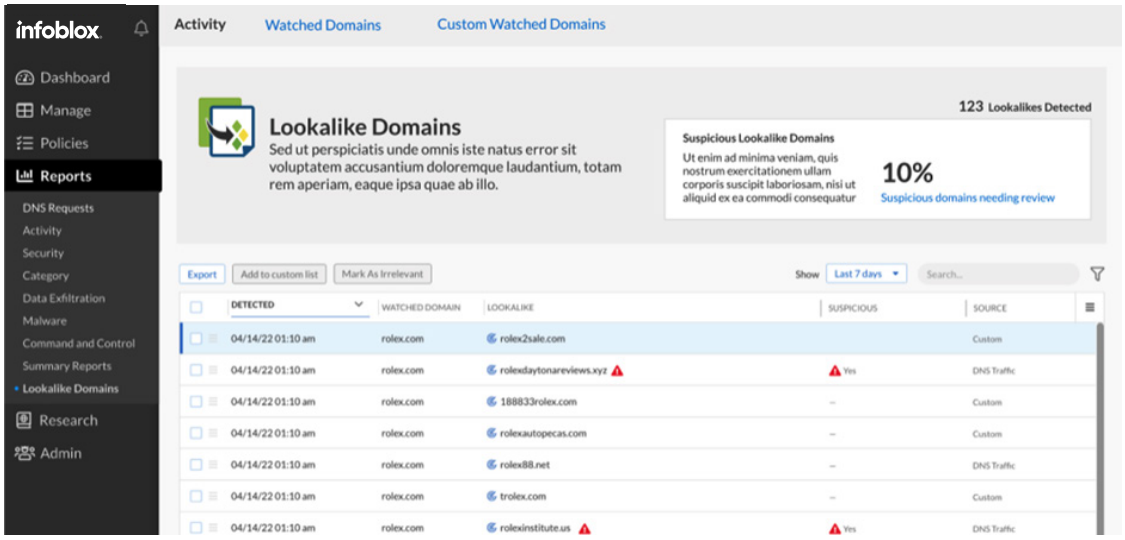
Infoblox は 2023 年に不審なドメインフィードに 1,940 万個のドメインを追加し、将来攻撃を受けるリスクを大幅に軽減しました。

類似ドメイン

Infoblox のお客様は不審なドメインフィードに加え、BloxOne Threat Defense に組み込まれている類似ドメインセキュリティ機能も利用可能です。その結果、企業への侵入、顧客への侵害、貴重なブランドの毀損を目的とする、標的を絞った高度な攻撃で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早期に特定し、阻止することができます。

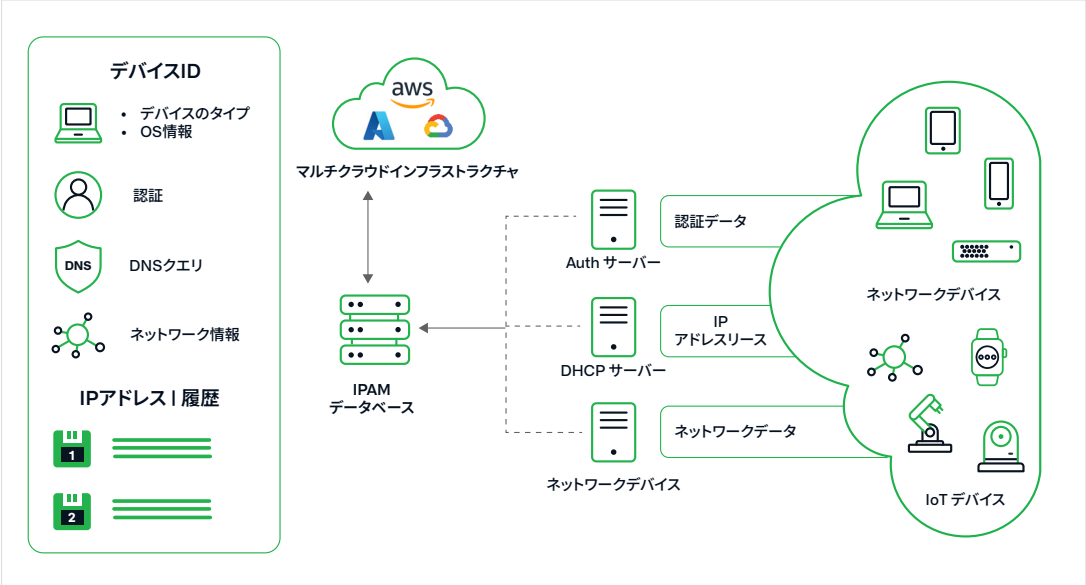
お客様は組織内やサプライチェーンパートナーが利用するドメイン、またはサイバー攻撃中にユーザー、パートナー、お客様を騙すために模倣された可能性のある他のドメインを送信できます。ドメインの送信を受け、Infoblox は潜在的な類似ドメインの継続的な監視プロセスを開始し、それぞれの登録、活動、履歴などを分析してリスクレベルを評価します。評価結果は、お客様が次のステップに関して情報に基づき決断をすばやく下すのに役立つように、インタラクティブなダッシュボードに提示されます。この情報は、新しい類似ドメインや現在特定されている類似ドメインに関連するアクティビティが反映されるように、継続的に更新されます。

Infoblox ではお客様との深い信頼関係とグローバル IT 環境における独自の立場を活用した「テイクダウン（フィッシングサイトの閉鎖）」サービスを別途提供しています。このサービスは、脅威にさらされている企業が財務やブランドに関するデータ漏洩を限定するのに役立ちます。Infoblox ドメイン脅威軽減サービスには、インシデントが実際に発生したことを確認する検証サービス、主要な ISP や規制当局との協調による軽減、脅威状況に対する理解を深め、セキュリティを強化するためのレポートによる監視が含まれています。評判どおりの熱心な調査と優れた品質により、一部地域では平均除去時間が最短 24 時間となることもあるなど、お客様が多数の脅威を事前に排除し、迅速に通常業務に復帰するのに貢献しています。



ユーザーとデバイスの属性認識が簡単に

これらのドメインへの通信をブロックすることが最初のステップですが、それらの通信に関与するデバイスや資産を迅速に可視化することも同様に重要です。IPAM メタデータを DNS と同期することで、ネットワーク内で悪意のあるクエリが発生した場所を特定するために必要な可視性を提供します。IPAM データを使用することで、異常な DNS アクティビティがファイアウォール、ユーザーデバイス、またはその他のネットワーク接続資産などのネットワークデバイスから発生しているかどうかを容易に判断できます。Infoblox を使用すれば、IPAM メタデータに基づいてセキュリティポリシーを簡単に定義することも可能です。



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

バージョン: 20240411v1