infoblox

Threat Intel

ソリューション ノート

Infoblox Threat Intel

三度の飯より DNS 分析

マルウェア中心の脅威インテリジェンスの限界

ほとんどのセキュリティソリューションは、脅威情報に対してマルウェア中心のアプローチを採用しており、悪意のあるドメインとしてフラグを立てるには、侵害が発生することを前提としています。このような事後的なアプローチは、モグラたたきをするように、悪意のある Web サイトが現れたら追跡し、それらを脅威情報フィードに追加してブロックしていることを意味します。

その結果、セキュリティ業界が最善を尽くしても、MFA 攻撃や類似ドメイン攻撃、標的型フィッシング攻撃は依然として組織に影響を及ぼし、データ漏えいやブランドの評判低下につながり続けています。セキュリティについては、犯罪者が攻撃を仕掛けるインフラストラクチャを構築する際に、能動的に企業を保護できるような、異なるアプローチを取る必要があります。

INFOBLOX THREAT INTEL でサイバー犯罪を根底から阻止

Infoblox Threat Intel は、市場をリードする DNS の専門知識と最先端のデータ サイエンスを組み合わせて、脅威アクターがインフラストラクチャを使用して高リスクのドメインとの通信を妨害する前に、そのインフラストラクチャを特定します。Infoblox Threat Intel は、DNS 脅威アクターとそのインターネット上での活動を追跡することに重点を置いた最初で唯一のソリューションであり、スミッシング、類似ドメイン、高リスクドメイン、ランサムウェア、マルウェア C&C などの新たな攻撃から顧客を能動的に保護します。Infoblox Threat Defense は Infoblox Threat Intel を使用して、他のセキュリティシステムよりも数か月前に、重大な脅威を検出・阻止します。Infoblox Threat Intel は DNS に特化しているため、DNS の専門性が必須ではなくなり、パフォーマンスをリスクにさらすことなくネットワークを保護できます。

主な統計：

2024年第1四半期において以下の事象が確認されました。

- 60% の脅威が、最初の DNS クエリ前に検出されました
- 82% の脅威が、最初の DNS クエリの後に検出されました
- 89% の脅威が、最初の 48 時間以内に検出されました

事実と数字

- MFA 攻撃は、従業員（WFH/リモートも含む）の脆弱性と類似ドメインの利用を組み合わせた、2023年に最も目につき、脅威となった攻撃
- 75% の組織がスミッシング攻撃を経験（Proofpoint 2024 State of Phish レポート）
- 多くの攻撃において、脅威アクターはドメインが登録されてから非常に長期間、場合によっては数ヶ月間、ドメインのエイジングを行う

設定不要な INFOBLOX THREAT INTEL の可用性

Infoblox の DNS Detection and Response 製品である Threat Defense は、次の 4 つのパッケージで提供されています。

1. Threat Defense Essentials
2. Threat Defense Business On-Premises
3. Threat Defense Business Cloud
4. Threat Defense Advanced

各パッケージでは、「RPZ フィード」を介してさまざまな Infoblox Threat Intel のデータにアクセスできます。Advanced パッケージには、TIDE（Threat Intelligence Data Exchange）というカスタム脅威フィードの取り込み/配信ツールや、このデータを活用する Dossier という脅威調査ポータルなども含まれています。

各 Threat Defense パッケージで利用可能な脅威フィードは次のとおりです。

フィード	Essential	Business OnPrem	Business Cloud	Advanced
Infoblox Base	x	x	x	x
Infoblox Base IP		x	x	x
Infoblox High Risk				x
Infoblox Medium Risk				x
Infoblox Low Risk				x
Infoblox Informational		x	x	x
DoH Public Hostnames	x	x	x	x
DOH Public IPs	x	x	x	x
Bogon	x	x	x	x
DHS_AIS_Domain	x	x	x	x
DHS_AIS_IP	x	x	x	x
EECN IPS		x	x	x
US OFAC Sanctions IPs				x
US OFAC Sanctions High IPs		x	x	x
US OFAC Sanctions Med IPs		x	x	x
Cryptocurrency hostnames and domains		x	x	x
TOR Exit Node IPs		x	x	x

フィードの概要

Infoblox Base：Infoblox Base のフィードにより、既知の悪意のあるドメインや侵害されたドメインに対する保護が可能になります。これには、既知のマルウェア、ランサムウェア、APT、エクスプロイトキット、悪意のあるネームサーバー、シンクホールなどが含まれます。すべてのユーザーに対してこれらをブロックすることをお勧めします。

Infoblox Base IP： Infoblox Base IP のフィードにより、既知の悪意のある IP アドレスや侵害された IP アドレスに対する保護が可能になります。これらの IP は、C&C マルウェアのダウンロードやアクティブなフィッシングサイトを通じて、システムに働きかけたりシステムを制御したりする脅威をホストする既知のインフラストラクチャです。すべてのユーザーに対してこれらをブロックすることをお勧めします。

Infoblox High Risk：Infoblox High Risk フィードには、いまだに確認されていないものの非常に疑わしいドメインが含まれています。ある時点で悪意のある行為に使用される可能性が非常に高いです。これらのドメインは、確認されていないものの、脅威と信頼性が高いため、ほとんどのユーザーに対してブロックすることを推奨します。脅威と信頼性のレベルの合計スコアが高い、疑わしいドメイン、疑わしい類似ドメイン、疑わしい NOED（Newly Observed Emergent Domains：新たに観測された新興ドメイン）が含まれます。

Infoblox Medium Risk：Infoblox Medium Risk フィードには、いまだに確認されていないものの、中程度のリスクがあるドメインが含まれます。これらは、脅威と信頼度レベルの合計スコアが、 High Risk フィードより低いものの、Low Risk フィードより高い疑わしいドメインです。悪意のある行為に使用される可能性は依然として高いため、ほとんどのユーザーに対してブロックすることを推奨します。これには、脅威と信頼度レベルの合計スコアが中程度の疑わしいドメイン、疑わしい類似ドメイン、疑わしい NOED が含まれます。

Infoblox Low Risk：Infoblox Low Risk フィードには、いまだに確認されていないものの、依然として疑わしいドメインが含まれます。悪意のある行為に使用される可能性があります。これらのドメインは、脅威レベルと信頼度レベルの合計スコアが低くなります。ほとんどのユーザーは、Allow-WithLog オプションを使用して監視し、機密性の高い環境ではブロックモードにすることを推奨します。これには、脅威と信頼度レベルの合計スコアが低い、疑わしいドメイン、疑わしい類似ドメイン、疑わしい NOED（新たに観測された新興ドメイン）が含まれます。

Infoblox Informational： Infoblox Informational フィードには、脅威と信頼度レベルが低いドメインが含まれています。これらは、ポリシーと環境の機密性に従って情報提供を目的としています。このフィードは、NOED を送ります。ほとんどのユーザーに対しては Allow-WithLog オプションを使用して監視し、機密性の高い環境ではブロックモードにすることを推奨します（新しいドメインはほとんどの場合ミッション・クリティカルではなく、存続時間が長くなるときに有効にするのが最善であるため）。

Bogon：Bogons の IP は、DDoS 攻撃の発信元アドレスであることがよくあります。「Bogon」とは、予約されているものの、Internet Assigned Numbers Authority（IANA）または委任された Regional Internet Registry（RIR）によってまだ割り当てられていない IP アドレス空間の領域からのものであると主張する公共のインターネット上の IP パケットの非公式な名称です。未割り当てのアドレス空間の領域は、「ボゴン空間」と呼ばれます。多くの ISP やエンドユーザー・ファイアウォールでは、bogon には合理的な使い道がなく、通常は偶発的または悪意のある設定ミスの結果であるため、bogon をフィルタリングしてブロックします。

DHS AIS IP および DHS AIS Domain（2 つのフィード）：国土安全保障省（DHS）の自動インジケーター共有（AIS）プログラムは、連邦政府と民間セクター間のサイバー脅威インジケーターの共有を可能にします。AIS は、企業または連邦政府機関が侵害の試みを観察 するとすぐに、そのインジケーターが Infoblox を含む AIS プログラム・パートナーと共有されるエコシステムを構築する、DHS の取り組みの一部です。このフィードに含まれる IP インジケーターは、速度と量を重視しているため、DHS によって検証されていません。Infoblox はインジケーターを変更または検証しません。ただし、AIS プログラムのインジケーターは、消費しやすいように Infoblox によって分類および正規化されます。

これらの AIS IP および AIS ホスト名フィードに含まれるデータには、米国 DHS 自動インジケーター共有利用規約（ww w.us-cert.gov/ais）の対象となる AIS データが含まれており、本データは、当該利用規約に従って処理する必要があります。AIS データを新たに配信する前に、当該利用規約（www.us-cert.gov/ais）に署名して提出する必要がある場合があります。詳細については、ncciccustomerservice@hq.dhs.gov まで電子メールでお問い合わせください。

DoH Public Hostnames と DOH Public IPs（2 フィード）このポリシーベースのフィードには、サードパーティの DoH（DNS over HTTPS）サービスのドメイン名と IP が含まれています。DNS を通じてセキュリティポリシーを施行したい組織は、サードパーティの DoH サーバーを使用した DNS セキュリティポリシーのバイパスを防ぎたい場合があります。

Tor Exit Node IPs：Tor 出口ノードは、暗号化された Tor トラフィックがインターネットに到達するためのゲートウェイです。これは、出口ノードが（オニオンネットワークを離れた後）Tor トラフィックを監視できることを意味します。Tor ネットワークは、トラフィックソースの特定を困難にするように設計されています。

Cryptocurrency Hostnames：このフィードでは、悪意のあるアクターが違法および/または詐欺行為を行うことを可能にする脅威、サイト所有者が通常の広告の代わりに暗号通貨マイニングソフトウェアをウェブページに埋め込むことを可能にする Coinhive（コインハイブ）、サイト所有者が所有者の同意なしに暗号通貨をマイニングできるクリプトジャッキング、および暗号通貨マイニングプールが取り上げられています。

EECN IP：このポリシーに基づくフィードには、知的財産やその他の機密データを求めている、およびクレジットカードや財務情報の盗難しようとしているサイバー攻撃のソースとなることが多い、東ヨーロッパの非 EU 諸国と中国の IP が含まれています。

US OFAC Sanctions IPs：このポリシーベースのフィードには、米国財務省外国資産管理局（OFAC）によってリストされた米国による制裁対象国の IP が含まれています。OFAC は、米国が諸外国に対して課している経済制裁を管理および執行しています。詳細については、「Sanctions Programs and CountryInformation（制裁プログラムおよび国情報）」ページ（www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx）を参照してください。

US OFAC Sanctions IPs（High Risk）：このフィードには、制裁対象国に関する高リスク指標がすべて含まれています。フィードには、ベラルーシ、カンボジア、中央アフリカ共和国、中国、キューバ、コンゴ民主共和国、イラン、イラク、リビア、マカオ、ミャンマー、北朝鮮、ロシア、シリア、ベネズエラ、イエメンの指標が含まれています。

US OFAC Sanctions IPs（Medium Risk）：このフィードには、制裁対象国の中程度のリスク指標がすべて含まれています。フィードには、ベラルーシ、カンボジア、中央アフリカ共和国、中国、キューバ、コンゴ民主共和国、イラン、イラク、リビア、マカオ、ミャンマー、北朝鮮、ロシア、ソマリア、南スーダン、スーダン、シリア、ベネズエラ、イエメン、ジンバブエの指標が含まれます。

INFOBLOX THREAT INTEL の使用をさらに最適化する機会

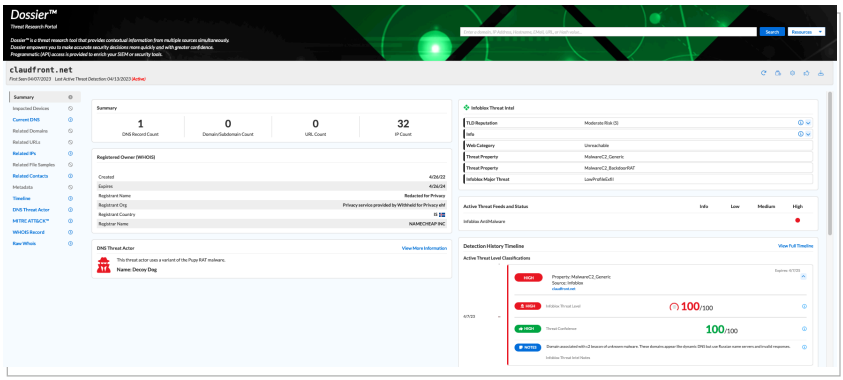
Threat Defense Advanced は、脅威の調査を迅速化し、インシデント対応を加速し、脅威ハンティングを容易にし、その他多数の SecOps アクティビティを強化する 2 つの独自の機能を提供します。

TIDE（脅威インテリジェンスデータ交換）

TIDE は、Infoblox Threat Intel の取り込み、管理、配信を自動化できるプラットフォームであり、政府/業界、オープンソース、サードパーティの脅威インテリジェンス（TI）ベンダー、一般のセキュリティ ベンダー、さらには貴社独自の内部脅威インテリジェンスからの追加フィードの使用までサポートします。

DOSSIER

Dossier は、アナリストに、自社のネットワーク内での影響と指標の完全な判定履歴を含む、DNS 中心の脅威インテリジェンスのビューを提供します。関連する指標と脅威アクターの情報が強調表示されるため、持続的な脅威を簡単に評価できます。Enrichment には、Infoblox の評判スコア、登録情報、コンテンツの分類、公開リンク、その他の現在の DNS 情報が含まれます。API は、SIEM 製品と統合するためのプログラムによるアクセスを提供します。



INFOBLOX THREAT DEFENSE ADVANCED で利用可能なサードパーティの脅威フィード

Threat Defense Advanced は、サードパーティ・ソースからの追加の脅威データを使用して、Infoblox が持つ多くの脅威インテリジェンス機能を補完するオプションをお客様に提供します。Threat Defense の TIDE 機能は脅威インテリジェンスの取り込みと共有を自動化できますが、一部のパートナーは迅速かつ簡単な BYOL (Bring Your Own License) 統合機能のサポートを提供しています。以下のパートナーから適切なライセンスを購入した後、お客様は Threat Defense Advance の BYOL ページにライセンスを入力するだけで、設定不要の統合機能を有効化し、すぐに使用できます。一部のパートナーは Infoblox と連携して、お客様のオンボーディングプロセスを簡素化しています。以下のパートナーは、設定不要のサポートを提供しています：

FireEye iSIGHT Threat Intelligence：IP およびホスト名のサイバー脅威インテリジェンスにより、企業は世界規模の専門家チームから得られる戦略的、運用的、戦術的な分析を活用できます。ThreatScape のサブスクリプションは、セキュリティ・プログラムをビジネス・リスク管理の目標に整合させ、新しいサイバー脅威や出現しつつあるサイバー脅威に対して能動的に防御するために必要なインテリジェンスを提供します。顧客は iSight フィードを FireEye から直接購入する必要がありますが、Infoblox では、TIDE プラットフォームでフィードを簡単に「オン」にできます。

Farsight Security の新しく観測されたドメイン（NOD）フィード：DomainTools からのこのフィードは、新しく開始されたドメインで発生または終了するマルウェアの持ち出し、ブランドの悪用、およびスパムベースの攻撃に対抗するための、防御の増分レイヤーを提供します。

VirusTotal は、地球上で最も贅沢かつ実用的なクラウドソーシング脅威インテリジェンス・プラットフォームです。包括的なコンテキストを提供することで、セキュリティチームが攻撃の意味を理解しようとして、未知のファイル/URL/ドメイン/IP アドレスに頻繁に遭遇する場合にサポートします。VirusTotal 脅威インテリジェンスを Threat Defense に統合すると、セキュリティアナリストは、デバイス、イベント、脅威インテリジェンスのデータを軸に、インシデントの状況を迅速に把握しながら、この独自のコンテキストを簡単に活用できるようになります。

注意: これは、*Threat Defense* 製品の脅威インテリジェンス機能のマーケティング概要です。本概要は定期的に更新されますが、SaaS 製品であるため、実際の製品機能はこのドキュメントに記載されているものと異なる場合があります。

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

バージョン: 20251902v2