infoblox

2025年
DNS の脅威の状況レポート

サイバー脅威の霧：

悪意のあるアクターが DNS を使用して欺き、回避する方法

過去 1 年間で、脅威アクターは欺瞞行為を急速に進化させ、活動の規模を拡大し、AI を活用して個人や組織を標的にし、脅威の調査を回避してきました。Infoblox Threat Intel は、消費者、企業、政府機関に同様に影響を及ぼす Domain Name System（DNS）を利用したサイバー攻撃の実行方法が、新たなレベルの専門性とスピードに達していることを観察しました。

効果的に防御するためには、セキュリティチームが直面する脅威を理解することが必要です。防御戦略を強化するためには、攻撃者が利用するな DNS 技術、その背後にいるアクター、そしてそれらがもたらすリスクについての洞察を得ることが不可欠です。

このレポートは、膨大な量のリアルタイムDNSテレメトリ、最先端の分析、数十年にわたる脅威の専門知識を活用して、攻撃者がDNSをどのように悪用するかについての独自の視点を提供します。また、ビジネスへの影響を概説し、現代のサイバー防御の重要なレイヤーとしてDNSベースのインテリジェンスを強調しています。

目次

DNS インテリジェンスの未開拓の可能性 5

セクション 1：DNS 脅威に関する主な観測 6
ドメインの短命な性質 6
使い捨てドメインによる制御を回避 6
悪意のあるドメインと疑わしいドメイン 7
トラフィック分散システムの一部であるドメインを介したクローキング 7
多様な脅威タイプに関連付けられたドメイン 7
ドメインの人気度 8

セクション 2：脅威アクターと調査 9

アクター事例研究：WORDPRESS ハッカーと VEXTRIO VIPER CABAL の連携 12

セクション 3：悪意のある DNS 手法 13

トラフィック分散システムは危険なレベルの回避を提供 14
悪意のあるアドテックは急速に成長し、十分に報告されていない脅威ベクトル 15
大規模なインフラストラクチャを中断させることは困難 15
悪意のあるアドテックが企業のリスクの入り口に 15
TDS の実例： 16
トラフィック分散システムで使用されるドメイン 17

信頼を盗むドメインハイジャック 18
Sitting Ducks 攻撃 18
ダングリング CNAME 18

類似およびタイプスクワットされたドメインがユーザーを欺く 18

脅威アクター、侵入テスター、正規のセキュリティツールが使用する DNS トンネリング 19

セキュリティチームには DNS トンネリングを阻止するためのメスが必要 20

セクション 4：守備側の課題 21

攻撃者が利用するAIが既存のセキュリティ制御をバイパス 21

事例研究：日本語話者を狙った Reckless Rabbit によるディープフェイクの使用 21

AIを活用したチャットボット 22

コードの難読化と回避 23

ブランドと組織の評判の保護 23

セキュリティチームに対するコンプライアンスの圧力と DNS の課題 23

次のステップ 24

使用される用語 25

DNS インテリジェンスの未開拓の可能性

DNS はドメイン名を IP アドレスに変換するため、インターネットの電話帳と呼ばれることがよくあります。すべてのデジタルインタラクションは DNS 要求から始まり、インターネット経由で接続を開始しているデジタル資産に関する詳細な可視性を提供することで、ネットワーク操作のテレメトリの高精度ソースになります。

DNS は、フィッシング、詐欺、検出回避、データ抽出の際に悪意のあるアクターによっても利用されます。したがって、DNS トラフィックとドメインの使用状況を分析することは、セキュリティアナリストにとって基礎となります。DNS データは、攻撃前のテレメトリを総合的に収集し、データを拡充し、ベースラインと比較して分析し、徹底的な脅威ハンティングを実行することで、予測的な脅威インテリジェンスに作り変えることができます。これらの洞察により、防御側は、攻撃者が攻撃する前に、攻撃者が利用するインフラストラクチャ、標的となる犠牲者、戦術を包括的に把握することができます。

「DNS は過去の脅威活動に関する独自の視点を提供し、それが水晶玉のような役割を果たして将来のサイバー脅威の前兆を明らかにします。」

— **Dr. Renée Burton**
Infoblox Threat Intel 責任者

その結果、DNS は単なる名前解決以上の機能を提供し、企業のセキュリティポリシーの施行ポイントとネットワーク上の潜在的な悪意のある活動の指標となっています。米国国立標準技術研究所（NIST）やサイバーセキュリティインフラストラクチャ安全保障庁（CISA）などの組織は、サイバーセキュリティにおけるDNSのこの重要かつ初期の役割を認識し、最近提案された NIST Special Publication (SP) 800-81 Rev. 3 でその予防的なセキュリティの可能性を強調しています。[1]

このレポートでは、次の 4 つの重要な質問に対処します。

過去 12 か月間の主要な DNS 観察結果は何か？

DNS の脅威アクターは誰で、最近どのような活動が発見されましたか？

DNS 技術の背後にある主な悪意のある戦術とは？また、それが危険な理由は？

防御側にとっての主な課題とは？また、DNSベースの脅威インテリジェンスが提供する機会とは？

1 Secure Domain Name System (DNS) Deployment Guide, National Institute of Standards and Technology (NIST), 2025年4月10日

セクション1：DNS 脅威に関する主な観測

100.8
million newly observed domains in one year

25.1%
of newly observed domains are malicious or suspicious

ドメインの短命な性質

2025 年 5 月末の時点で、Infoblox は 13,000 を超える Infoblox 環境から毎日 700 億件の DNS クエリを処理および分析し、あらゆる種類のデバイスの数百万の IP アドレスをカバーしていました。

1,300 社を超える Infoblox Threat Defense™ 顧客から得られる完全に匿名化されたデータは、複数のクライアントタイプ、地域、業種にわたる何百万ものインターネットインタラクションに対するグローバルかつ詳細な可視性を提供します。この DNS テレメトリの量は前年比で 21% 増加しました。

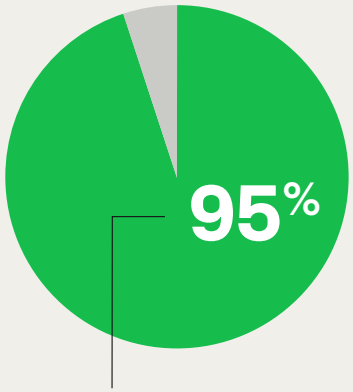
収集されたすべてのデータの中で、Infoblox Threat Intel は**過去12か月間に新たに観測されたドメイン（セカンドレベルドメイン）を 1 億 800 万件**特定しました。この大量の新規ドメインは、急速に変化するインフラストラクチャ、短期的な広告キャンペーン、ブランディングイニシアティブなどに起因することが多いです。

使い捨てドメインによる制御を回避

新たに観測されたドメインの 4 分の 1 以上（2,500 万件以上）は、Infoblox によって悪意のあるドメインまたは疑わしいドメインとして分類されました。脅威アクターは、検出制御を回避するために、膨大な数の新しいドメインを継続的に登録、有効化、導入しています。このような大量のドメインを特定して分類することは難しいため、攻撃者は見えない範囲を飛行し、ブロックメカニズムを迂回し、フォレンジック証拠を最小限に抑えることができます。

特定された脅威関連ドメイン（悪意のあるドメインと疑わしいドメインの両方）の単独使用も重要です。Infoblox Threat Intel は、すべての脅威関連ドメインの 95% が単一のネットワーク環境内で観測されていることを発見しました。

この戦術の背後にある目的は単純です。攻撃者は、自分たちが無限に持っている使い捨てドメインを利用して、「初期感染」データを頼りとする、フォレンジック方式の防御を迂回することです。



of threat-related domains were observed in only one customer environment.

悪意のあるドメインと疑わしいドメイン

- **悪意のあるドメイン**は強力な証拠によって裏付けられた確認された脅威です。これらは時間とともに減少することはないため、1 億を超える新規観測ドメインの 1.6% を占めます。
- **疑わしいドメイン** は、決定的な証拠が不足している潜在的な脅威であり、新たに観測されたすべてのドメインの 23.5% を占めています。確認されない場合、これらの指標は数か月後に期限切れになります。Infoblox Threat Intel のアナリストは、新しい証拠がないかこれらのドメインを継続的にモニターしています。追加のインジケーターが検出されると、スコアが更新され、疑わしいドメインが悪意のあるドメインとして再分類される場合があります。

トラフィック分散システムの一部であるドメインを介したクローキング

アドテック（広告技術の略）とは、デジタル広告の自動化、管理、ターゲティング、配信、分析に使用されるツール、ソフトウェア、プラットフォームを指します。トラフィック分散システム（TDS）は、インターネットトラフィックを事前に定義されたルールに基づいて異なる宛先にリダイレクトするために、合法的または悪意を持って使用されるプラットフォームまたはメカニズムです。脅威アクターもこの技術を採用しており、しばしば**悪意のあるアドテック**と呼ばれます。

82%

of customers queried a domain part of a traffic distribution system.

過去 12 か月間で、**すべての顧客環境の 82% が** TDS の一部であるドメインをクエリしましたが、その多くは、カスタマイズされたフィッシングサイト、スケアウェア、詐欺、インフォスティーラーなどの有害なコンテンツを隠蔽することで知られる悪質なアドテック運営者によって運営されています。

これらの TDS は、多くの場合、数万のドメインで構成されており、検出を回避するために迅速に回転し、脅威の研究者からそのコンテンツを隠蔽しながら、理想的な被害者に標的を絞った悪意のあるコンテンツを配信します。

長年にわたり、Infoblox Threat Intelは、**168社の悪意あるアドテック運営者が TDS インフラ内で 100 万以上のドメインを使用していることを発見しました**。これらの指標は、ハイジャックされたドメイン、類似ドメイン、リダイレクト、アルゴリズムによって事前登録されたドメインセット（登録ドメイン名アルゴリズム、RDGA）など、複数の DNS 手法を網羅しています。TDS、その仕組み、そして危険性については、セクション 3 で詳しく説明します。

多様な脅威タイプに関連付けられたドメイン

新しい脅威関連のドメインが発見されると、Infoblox の脅威研究者は、その背後にいるアクターとその根底にある意図を調査します。次のページの表は、アクターがさまざまな悪意のある目的でドメインをどのように使用しているかを優先順位を付けたリストを示しています。

リスト上位7位：脅威アクターが新しいドメインを利用する方法	
1	**不正な活動や詐欺に従事**（偽の暗号通貨投資サイトなど）します。
2	**違法コンテンツ**（ギャンブル（特に中国のような地域）やアダルトコンテンツなど）をホストします。
3	**フィッシングページを作成**（個人情報やクレジットカード情報を盗むことが目的）します。
4	**マルウェアを導入します。**一般的な例としては、インフォスティーラー（例：Lumma Stealer）、ドライブバイダウンロードによるローダー（例：SocGholish）、ボットネット、ランサムウェア（例：BlackBasta）などがあります。
5	**アクティビティを隠蔽**し、TDS を介してさまざまなペイロードを配信したり、ユーザーをだまして不要なブラウザ通知を許可させたりします。
6	**望ましくない可能性のあるプログラム（PUP）**（スケアウェアや不要なブラウザ拡張機能など）を配布します。
7	**スパムキャンペーンを実施し、悪意のある電子メールを配布します。**

表 1. 新たに観測されたドメインに対するアクターの目的。

ドメインの人気度

Infoblox DNS テレメトリは、ドメインタイプの使用状況に関する洞察を提供し、アプリケーションの人気度や脅威アクターが大量の武器化されたドメインを被害者に押し付ける速度に関する手がかりを提供します。

19 DAYS

Time needed for a TDS domain to become popular

主な観察事項：

- コンテンツ配信ネットワーク（CDN）、テクノロジープロバイダー、セキュリティベンダー、ビジネス生産性ツール、検索エンジン、ストレージ、クラウドサービス、ネット会議などの8つのドメインカテゴリが顧客の DNS クエリ内の全ドメインの大部分（特定の日で約70%）を占めています。
- 2025年5月には、オンラインショッピング、ゲーム、ソーシャルメディア（例：TikTok、Facebook）といった個人的なインターネット利用に関するドメインクエリが、ビジネスコラボレーションプラットフォーム（例：Microsoft Teams、Slack）に関連するクエリとほぼ同数に達しました。これは、**ビジネスと個人的なインターネット**利用の重複が拡大していることを示しています。脅威アクターはこの重複を強く認識しています。
- 攻撃者は、BYOD（個人携帯の業務利用）やモバイルデバイスなどの脆弱な攻撃対象を絶えず探し、ユーザーを欺いて、認証情報などのビジネス関連データを抽出することを目的としたリスクの高い行動を実行させようとします。この傾向は、Verizon の 2025 年データ侵害調査報告書でも強調されています。[2] この報告書は、どのデバイスも制限されていないことを確認し、**盗まれた企業認証情報の 46% が**管理されていないデバイスまたは個人のデバイスから発生したことを指摘しています。

2　2025 Data Breach Investigations Report, Verizon.

- Infoblox Threat Intel は、TDS の一部であるドメインが[3]わずか 19 日間で **2024 年と比較して 2.35 倍、2020 年と比較して 39 倍の速さで普及しつつあることを観察しました。**TDS ドメインが人気を獲得する速度は、`panerabread[.]com` や `draftkings[.]com` のような正規サイトに匹敵する速さです。これは、武装化されたドメインがいかに効果的に拡散され、被害者によってアクセスされているかを示しています。脅威アクターは、ターゲットの前に大量のこれらのドメインを迅速に導入し、キャンペーンの影響を最大化しながら、オープンソースインテリジェンス（OSINT）やフォレンジックベースの分析などの遅いインテリジェンスソースを凌駕しています。

セクション 2：脅威アクターと調査

204K
total identified suspicious domain clusters

662
total identified DNS threat actors

10
new actors publicly disclosed in the past 12 months

過去 1 年間に発見された 1 億件の新しいドメインは、自然発生したものではなく、常に人間の行為によって引き起こされ、特定の目的のために開始されたものです。Infoblox Threat Intel は、収集されたテレメトリを拡充し、共通のパターンを相関させることで、脅威関連ドメインの背後にいるアクターを継続的に分析および調査します。

Infoblox Threat Intel は調査開始以来、共通の脅威要素を共有する合計 204,000 の疑わしいドメインクラスターを発見し、662 の固有の脅威アクターを特定しました。過去 12 か月だけでも、Infoblox の研究者は、さまざまな調査レポートやブログ投稿を通じて 10 の新しいアクターを公開しました。

3 ドメインは、特定の期間における顧客トラフィックの大部分を占めるドメインのサブセットに属する場合、人気のあるドメインと見なされます。1 日あたりのドメイン数は 6,000 から 10,000 までさまざまです。詳細については、https://blogs.infoblox.com/wp-content/uploads/infoblox-whitelists-that-work.pdfをご覧ください。

次のリストは、2024 年 7 月 1 日から 2025 年 7 月 1 日の間に Infoblox Threat Intel によって特定され、公開された主要な脅威アクターを示しています。

RDGAパターンの例	説明
	このアクターは、主に侵害された WordPress サイトからの正当なウェブトラフィックを乗っ取り、詐欺、マルウェア、フィッシングコンテンツにリダイレクトする悪意のある TDS を運用しています。 VexTrio は、脅威の状況において最も蔓延し、回避能力に優れたアクターの1つと考えられています。過去 12 か月間、このアクターはアフィリエイトハッカーとの関係についていくつかのレポートで名前が挙がり、攻撃インフラストラクチャを提供するためにドメインをハイジャックすることで知られています。 **最近公開されたレポート：** • 厄介で悪質な存在：WordPress ハッカーとアドテックカルテルの不気味な関係 • ウサギの穴に押し込まれて
	この高度な DNS 脅威アクターグループは、誤構成された、または忘れられた DNS レコード、特に未解決の正規名（CNAME）エントリを悪用して、Amazon S3 バケットや Azure エンドポイントなどの放棄されたクラウドリソースを乗っ取ることに特化しています。 Hazy Hawk がこれらのサブドメインの制御権を獲得すると、正当なドメインの固有の信頼性を利用して悪意のあるコンテンツをホストします。その操作には、多くの場合、TDS を介してユーザーをリダイレクトし、詐欺、マルウェア、欺瞞的なプッシュ通知を配信することが含まれます。 **最近公開されたレポート：** • 曇り時々DNSレコードのハイジャック — 詐欺行為を可能にするリスク
	この金銭的動機のある脅威アクターは、2023 年 2 月以来、ハイジャックされたドメインを投資詐欺に使用しています。これらのドメインを、複数の大陸で短期間表示される Facebook 広告に埋め込み、英語、イタリア語、ポーランド語、トルコ語、スペイン語など 30 以上の言語で被害者を標的にしています。 このアクターは「Sitting Ducks」攻撃ベクトルを利用して評判の良いドメインを乗っ取り、セキュリティ研究者から詐欺サイトを保護するために使用します。2024 年 10 月現在、Infoblox はこのアクターに関連する約 5,000 件のハイジャックされたドメインを特定しています。 **最近公開されたレポート：** • 投資詐欺におけるアクターの TTP パターンと DNS の役割の解明 • DNS プレデターはドメインを乗っ取り、攻撃インフラを供給します

Reckless Rabbit は、悪質な Facebook 広告を通じて被害者を誘い込む投資詐欺アクターです。辞書ベースの RDGA を採用し、オーストリア、ベルギー、デンマーク、フランス、ポーランド、スウェーデン、英国など複数の国の個人を狙っています。アクターは RDGA と偽の推薦を使用しています。

最近公開されたレポート：

- 投資詐欺におけるアクターの TTP パターンと DNS の役割の解明

このフィッシング攻撃者は、辞書ベースの RDGA を活用し、人気のあるサービスを偽装する投資詐欺キャンペーンを実施しています。アクターは独自のドメインクローキングサービスを運営してユーザーの検証チェックを行い、ルーマニア、ロシア、ポーランドなどの東欧諸国をターゲットにしています。

最近公開されたレポート：

- 投資詐欺におけるアクターの TTP パターンと DNS の役割の解明

この攻撃者は、放棄されたクラウドリソースを特定し、さまざまな悪意のあるアクティビティに再利用します。Hasty Hawk は、Google 広告を通じて配信される慈善活動や DHL をテーマにしたキャンペーンで使用されるドメインをハイジャックすることで知られています。Hasty Hawk は主に、Proton66 などの「防弾」ホスティングネットワークと TDS を使用して、ユーザーをコンテンツに誘導します。

最近公開されたレポート：

- DNS プレデターはドメインを乗っ取り、攻撃インフラを供給します

Vacant Viper は 404TDS を運用し、それを使用してマルウェアやその他の悪意のあるコンテンツを配信します。Vacant Viper は、誤設定された DNS ネームサーバーにより脆弱性が残されたドメインを乗っ取り、Infoblox の研究者によって「Sitting Ducks」と名付けられたこの欠陥を利用して、それらを悪意のある TDS インフラストラクチャに組み込みます。

最近公開されたレポート：

- 意外にも、ドメインの乗っ取りはとても簡単

この悪意のあるアドテックアクターは、WordPress の脆弱性を利用して、マルウェア、フィッシングページ、偽アプリ、不要なコンテンツを配信します。プッシュ通知、ポップアップ、リダイレクトをブラウザに組み込んだ広範な TDS を実行し、ユーザーが最初のページを離れても広告を配信します。

最近公開されたレポート：

- 厄介で悪質な存在：WordPress ハッカーとアドテックカルテルの不気味な関係

Morphing Meerkat は、高度なフィッシング・アズ・ア・サービス（PhaaS）プラットフォームの背後にいる世界的なスパムアクターです。このアクターは、DNS MX レコードを使用して被害者のメールサービスプロバイダーを特定し、偽のログインページを動的に提供します。Morphing Meerkat は、侵害された WordPress サイトおよびアドテックサーバーのオープンリダイレクトの脆弱性を悪用します。

最近公開されたレポート：

- ある DOH と DNS MX の悪用によるフィッシングの物語

アクター事例研究：WORDPRESS ハッカーと VEXTRIO VIPER CABAL の連携

Infoblox は最近 **、WordPress ハッカーと悪意のあるアドテック企業ネットワーク**（特に VexTrio の TDS）との複雑な連携関係を明らかにしました。

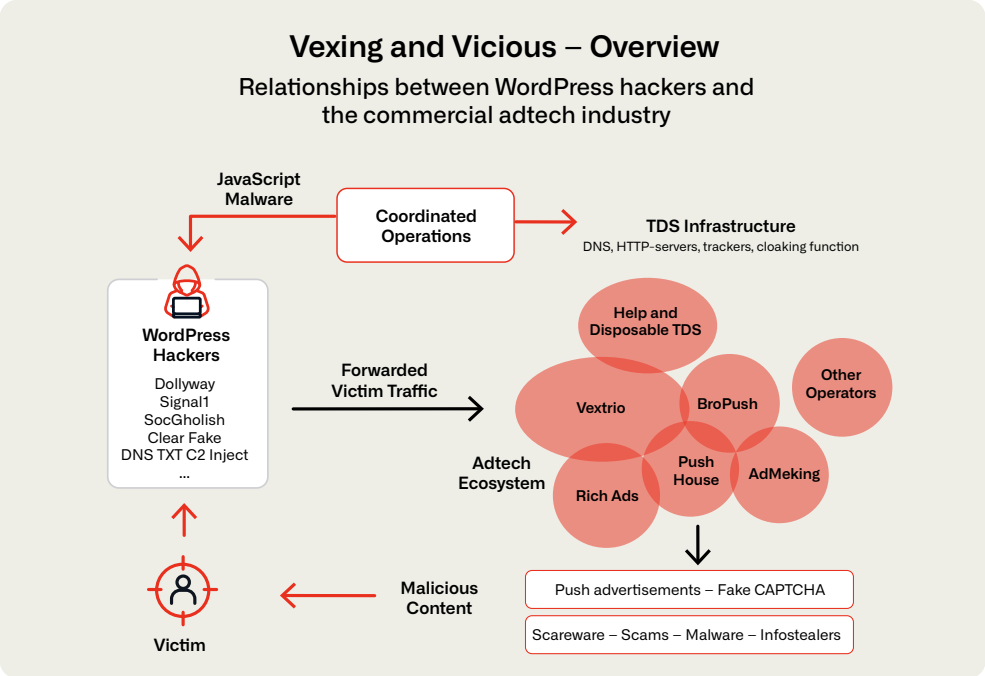


図 1. WordPress ハッカーと商用アドテック業界の関係

発生した事象

- **迅速な移行：**2024 年秋に VexTrio の TDS が中断されたとき、複数のマルウェアアクターが同時に「Help TDS」という名前の一見新しい TDS に移行しました。さらなる分析により、Help TDS は独立しているわけではなく、VexTrio と密接に連携しており、インフラストラクチャとソフトウェアコンポーネントを共有していることが明らかになりました。
- **協調作戦：**Infoblox は 6 か月間にわたり、侵害されたウェブサイトからの 450 万件の DNS TXT レコード応答を分析しました。その結果、ロシアと関連するインフラ上にホストされた 2 つの異なるコマンドアンドコントロール（C2）サーバーが明らかになり、WordPress ハッカーと VexTrio グループの協調作戦を示唆しています。

- **商業アドテック企業の関与：**Los Pollos、Partners House、BroPush、RichAds を含むいくつかのアドテック企業が VexTrio の事業と絡み合っていることが判明しました。これらの企業は、スマートリンクやプッシュ通知を介して悪意のあるコンテンツの配布を促進しました。

この調査では、侵害された WordPress サイトや商用アドテックインフラストラクチャを活用するサイバー犯罪者ネットワークの高度かつ適応性の高い性質が浮き彫りになっています。これは、そのような脅威を発見し軽減するための DNS テレメトリと協力的な取り組みの重要性を強調しています。

セクション 3：悪意のある DNS 手法

セクション 2 で説明した脅威アクターは、特定の目的を念頭に置いて、さまざまな方法で DNS を使用します。Infoblox が脅威関連のドメインを検出すると、分析プロセスと専門家のレビューによって、既知の悪意のある手法がドメインに割り当てられます。以下の表は、Infoblox Threat Intel によって脅威関連ドメインに割り当てられた最も一般的な DNS 手法の概要を示しています。

DNS 技術と脅威関連ドメイン 期間：2025 年 1 月～2025 年 6 月	
機械アルゴリズムによって生成されたドメイン（RDGA、DDGA、DGA）	54.7%
トラフィックをリダイレクトするために使用されるドメイン	11%
CNAME またはエイリアスドメイン	5.8%
類似ドメイン	5.1%
ハイジャックされたドメイン	5.1%
悪意のある SMS で使用されているドメイン	4.2%
TDS の一部として作成されたドメイン	1.8%
C2 と流出に使用されるドメイン	< 0.4%

表 2. 脅威関連ドメインに割り当てられたDNS技術

これらの手法の多くは、脅威キャンペーン中に重複し、目的を達成するためのより大規模なアクターの戦術の一部になります。このレポートでは、4つの一般的な DNS 技術、使用方法、そしてそれらが危険な理由について詳しく掘り下げます。

- TDS 内でのドメインの使用
- 信頼を盗むためのドメインハイジャック
- 被害者を欺くための類似ドメイン
- C2 とデータ流出のための DNS トンネリング

トラフィック分散システムは危険なレベルの回避を提供

DNS は、地理位置情報、デバイスの種類、セキュリティ体制などのさまざまな属性に基づいて、多くの場合はユーザーに知られることなく、複数の中間層を介してユーザーを密かにリダイレクトすることで、TDS において中心的な役割を果たします。DNS は、ネットワークトラフィックがどのように、どこにルーティングされるかを決定する上で基本的な役割を果たします。TDS の正規の運営者は、主にデジタル広告やアドテック業界に存在します。アドテック（広告技術の略）という名前は、デジタル広告キャンペーンの管理、配信、分析に使用されるツール、プラットフォーム、ソフトウェアを指します。

よく知られている合法的な広告技術（例：Google AdSense）と同様に、悪意のあるアドテックは、キャンペーンの効果を高めるために、適切なコンテンツを適切なオーディエンスに適切なタイミングで配信します。この種のサイバー脅威は、多くの関連会社と豊富な資金を持つ専門組織によって実行されます。

接続共有別の上位 TDS 運営者	
アクター名	**接続共有**
Vextrio Viper	72.8%
VANE VIPER	68.4%
Venal Viper	72.5%
非公開のアクター	64.8%
Vero Viper	60.5%
Tiano Gambling	50.9%

表 3：TDS 運営者と受信した顧客接続試行の割合

これらの活動の中心には、被害者をプロファイリングし、悪意のある広告主に誘導すると同時に、脅威研究者を偽のサイトに誘導する TDS があります。

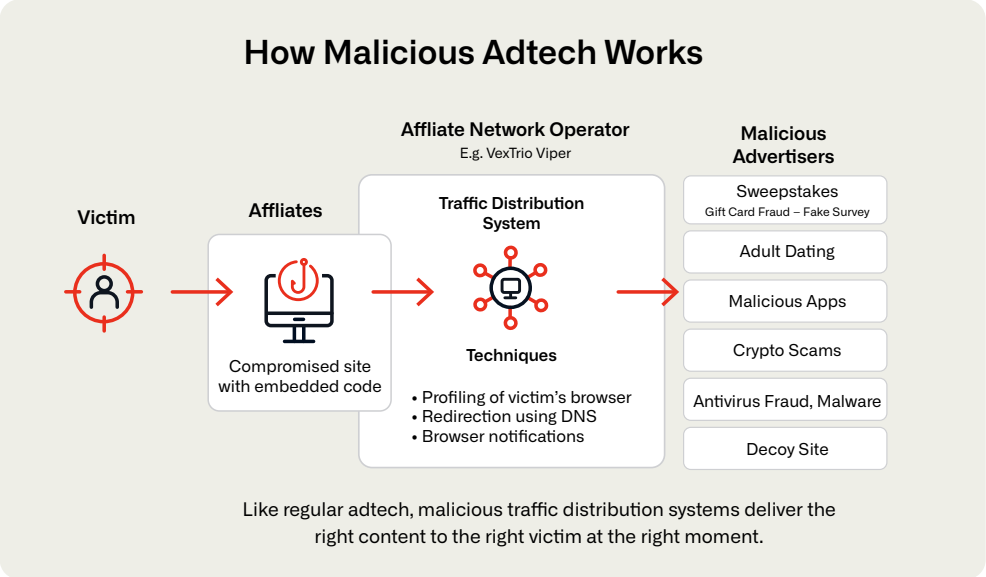


図 2：悪意のあるアドテックに関わる 3 つのプレーヤー（アフィリエイト、運営者、悪意のある広告主）

悪意のあるアドテックが有害であり、企業のセキュリティチームにとって重要な重点分野であるべき理由は複数あります。

悪意のあるアドテックは急速に成長し、十分に報告されていない脅威ベクトル

攻撃者は、マルウェアやその他の悪意のあるコンテンツを配信するための低コストサービスとして、悪意のある広告ネットワークをますます活用しています。これらの広告は、ドライブバイダウンロード攻撃、フィッシングサイト、認証情報窃取ツール、エクスプロイトキットなど、さまざまな種類の攻撃につながる可能性があります（表4：TDS運営者と配信される悪意のあるコンテンツを参照）。

セキュリティ業界のほとんどは、ゼロデイ攻撃アプローチ（攻撃中（例：サンドボックス化）または攻撃後（例：フォレンジックベースのインテリジェンス）にテレメトリを収集）に依存しているため、結果として得られる対策は、その最初の侵害ポイントから発見されたアーティファクトに限定されます。この制限により、TDS は検出を回避するための効果的なツールとなり、攻撃者は配信する悪意のあるコンテンツを継続的に変更し、脅威研究者をおとりサイトにリダイレクトします。結果として、TDS はサイバーセキュリティ業界で最も報告が少ない脅威の 1 つとなっています。

大規模なインフラストラクチャを中断させることは困難

悪意のあるアドテックを運用している組織は、ユーザーをリダイレクトしてブラウザのプッシュ通知を受け入れるように誘導するように設計され、急速に変化する何万ものドメインを含む、かなりの規模でインフラストラクチャを構築することがよくあります。これらの活動は、法的調査を回避しながらサイバー犯罪を実行するために、複数の組織に細分化されることがよくあります。VexTrio Viper などの一部の運営者は何年も存続し、大きな利益を上げており、その活動は止まる気配がありません。

悪意のあるアドテックが企業のリスクの入り口に

悪意のあるアドテックは、人気ブランドを模倣したり、アクセスしたいコンテンツを提供したりして被害者を欺き、警戒を緩めてリスクの高いやりとりをするように促します。これらの脅威は通常、消費者向けサイトから発生しますが、企業環境にも簡単に侵入し、従業員の個人用デバイスを武器化されたコンテンツにさらす可能性があります。これにより、脅威アクターは偵察を行ったり、企業からの通知になりすましたりして、組織ネットワークへのリスクを高めます。

DNS 運営者	マルウェア	詐欺	フィッシング	乗っ取られたドメイン
Vacant Viper	X	X		X
VANE VIPER	X	X	X	
Vextrio Viper	X	X	X	X
ヘイスティホーク			X	X
Sophisticated Chickens			X	X
Black TDS	X		X	
Parrot TDS	X			
R0bl0ch0n TDS		X		

表 4. TDS オペレーターと配信された悪意のあるコンテンツ

TDS の実例：

被害者がモバイルデバイスまたはエンドポイントから侵害されたサイトにアクセスすると、運営者は偽の CAPTCHA を表示して、悪意のある広告主からのブラウザプッシュ通知を被害者に許可させることがあります。その後、これらの通知により、未検証のソフトウェアのダウンロード、個人情報の共有、組織の資格情報の入力を求めるプロンプトなど、さらに不正なコンテンツが配信されることがあります。

TDS は侵入してくる被害者をプロファイリングするため、一般的なセキュリティツールを使用している SOC アナリストや脅威研究者はこれらの通知や悪意のあるコンテンツを検出できない可能性があり、代わりに正当なコンテンツを表示するおとりサイトにリダイレクトされる可能性があります。

業務でのインターネット利用と個人的なインターネット利用が重複しているため、悪意のある広告テクノロジーは、特にモバイルデバイス、タブレット、BYOD、保護されていない資産に対するサイバー犯罪の大きな要因となっています。

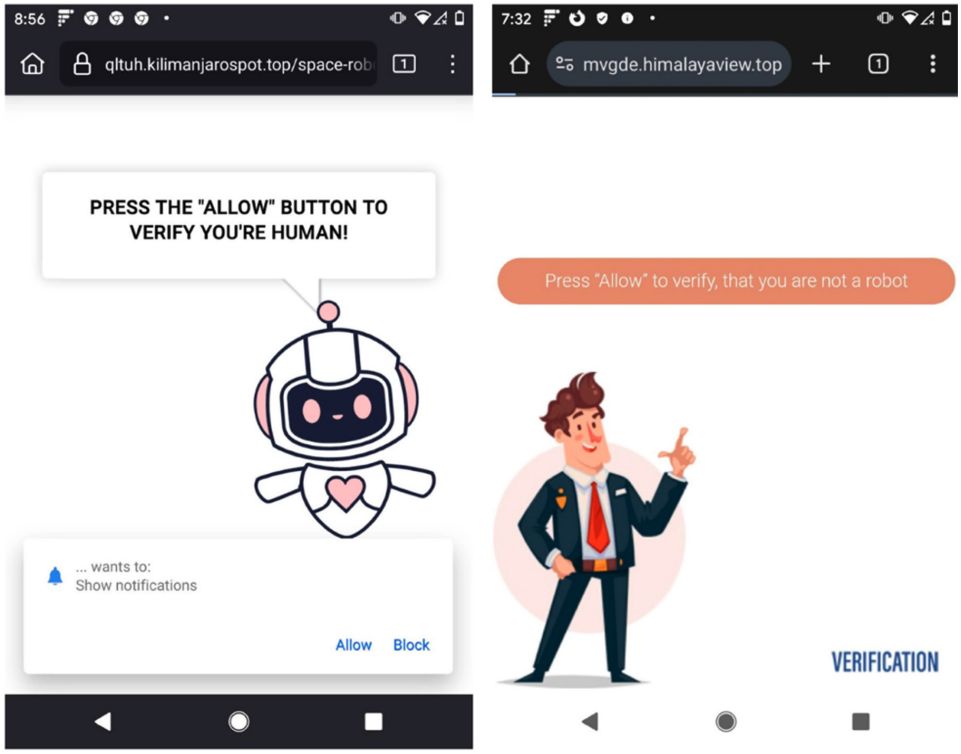


図 3：VexTrio Viper のランディングページの例。このランディングページは、ユーザーをデバイスでプッシュ通知を受け入れるように誘導します。どちらも `germannautica[.]com` を閲覧しているときに確認されました。

トラフィック分散システムで使用されるドメイン

過去 12 か月間で、Infoblox Threat Intel は、168 の悪意のあるアドテック運営者が TDS 内で使用した 100 万を超える指標を発見しました。これらのインジケーターは、RDGA、リダイレクト、乗っ取られたドメイン、類似サイトなど、複数の手法にわたります。

悪意のあるアドテック運営者が使用する TDS は非常に大規模となる可能性があります。多くは 10,000 以上のドメインを含み、中には 100,000 を超えるものもあります。しかし、TDS のサイズはその蔓延度や脅威レベルと必ずしも相関するわけではありません。Vigorish Viper は 170,000 のアクティブなドメインからなる広大で成長中のネットワークを運営していますが、主に中国、香港、マカオの被害者を標的にしています。Venal Viper は、サイズではトップ5に入っていませんが、顧客ネットワークで最も頻繁にクエリされるものの 1 つです。過去 12 か月間で、Infoblox 全顧客の 65% が Venal Viper ドメインをクエリしています。

TDS の破壊

TDS を使用する有害なアドテックは、正当な広告を装い、被害者を欺き、シミュレーションや最初の被害者のデータを通じて既知の悪意のある動作を識別するセキュリティツールによる検出を回避するため、繁栄しています。対照的に、DNS レコードは、新しい悪意のあるインフラストラクチャがいつ、どのように構成されたかを明らかにすることができます。

リアルタイムおよび過去の DNS データを革新的なデータサイエンスと組み合わせて活用する研究者は、ペイロードが配信される前に、悪意のあるアドテックで使用されているドメインを含め、疑わしいドメインや悪意のあるドメインを特定できます。

DNS から得られるインテリジェンスは、TDS の動作やトラフィックのリダイレクト方法など、脅威の背後にあるインフラストラクチャを明らかにします。他のセキュリティ手法とは異なり、DNS ベースのセキュリティ実装は、悪意のあるアドテックを積極的に検出し、インターネットに接続されたエンドポイントがそれと対話するのを防ぐことができます。

簡単に言えば、DNS ベースの保護は、攻撃者のインフラストラクチャに焦点を当てることで、悪意のある広告主と被害者の間のサプライチェーンを断ち切り、最新のペイロードに単に反応するのではなく、長期的な保護を提供します。

信頼を盗むドメインハイジャック

脅威アクターは、主に正規のドメインに関連する信頼性と信用を悪用するために、既存のドメインをハイジャックします。攻撃者の支配下に置かれると、ハイジャックされたドメインは、説得力のあるフィッシングサイトを作成したり、検索エンジンに優先順位を付けられたり、スパムフィルターを迂回したり、詐欺を実行したりするために利用されます。

Infoblox Threat Intel は、攻撃者がドメインを乗っ取る複数の方法と、ユーザーを欺くために使用するツールを発見しました。

Sitting Ducks 攻撃

Sitting Ducks 攻撃は過去数年間で蔓延してきました。2024年、Infoblox Threat Intel は、この攻撃に対して脆弱なドメインが**100 万を超えると推定しました**。2024 年下半期の詳細な調査では、**脆弱な 80 万ドメインのうち 7 万ドメインが乗っ取られていることが発見されました**。これは、問題の規模と堅固なセキュリティ対策の必要性を浮き彫りにしています。

複数の脅威アクターがこれらの手法を体系的に使用しています。こうした攻撃は実行が容易である一方、セキュリティチームが攻撃を検出するのが難しいため、特に危険です。

この攻撃を悪用していることが知られているアクターには、VexTrio Viper、Vigorish Viper、Horrid Hawk、Hasty Hawk などがあります。これらのグループは Sitting Ducks 攻撃の有効性を実証しており、これらの脅威に対抗するためには警戒を強化し、セキュリティ対策を改善する必要性を強調しています。

ダングリング CNAME

2025 年初頭、脅威アクターは `cdc[.]gov` や米国の複数の大学といった高評価ドメインのリダイレクト構成を悪用しました。これは、組織がサードパーティプロバイダー（Microsoft Azure など）がホストするクラウドアプリケーション（CDN など）を廃止した一方で、DNS エイリアス（CNAME レコード）を有効なままにしていたために可能になったものです。

Hazy Hawk のような悪意のあるアクターは、同じ CDN 上に新しいコンテンツを作成することで、DNS 衛生のこの欠陥を悪用しました。動機は単純で、元のドメインエイリアスの評判を利用して、Google やその他の検索エンジンをだまして悪意のあるコンテンツをインデックスに登録し、検索結果に含めることができました。

類似およびタイプスクワットされたドメインがユーザーを欺く

類似ドメインは、ユーザーを欺くために登録された、わずかに変更されたドメイン名です。多くの場合、正規のブランド、従業員のコミュニケーション、サプライチェーン、またはその他の信頼できるパートナーを偽装し、重大な問題を引き起こします。

攻撃者は、SMS メッセージ、電話、ソーシャルメディア上のダイレクトメッセージ、電子メール、QR コードで類似ドメインを使用しました。最近では、ゲーマーからデジタル通貨市場まで、あらゆる分野で採用が進んでいる多要素認証（MFA）が標的となっています。その他の例としては、企業の MFA をバイパスしたり、一般的な ID アクセスプラットフォームのドメイン名を悪用したりすることが挙げられます。

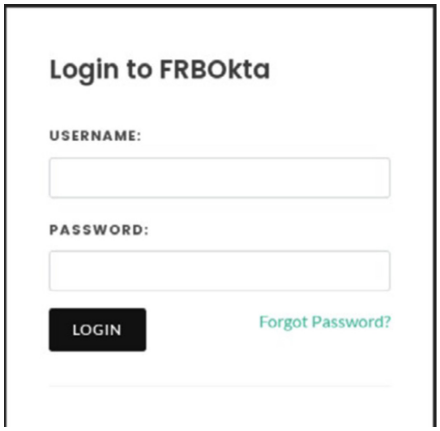


図 4. 類似ドメインからの MFA メッセージ

類似ドメインは、1,500 を超えるトップレベルドメインがあるため、はるかに大きな問題になっています**ほとんどの組織では、すべてのバリエーションをモニターするためのコストが高くなっています。**

さらに、組織にはドメインを登録している複数のグループがあり、誰が何をしているのかを把握できない場合があります。セキュリティチームは、ヘルプデスクチームやクラウドアプリケーションチームが似たようなドメインを作成したと思うかもしれませんが、実際にはその新しいドメインは、顧客をフィッシングするアクターによって設定された可能性があります。

セキュリティチーム内の専門知識の欠如は、マネージドサービスを通じて迅速な解決策を求める傾向を生み出すことがよくあります。残念ながら、類似ドメインは簡単に解決できる問題ではありません。成熟したセキュリティチームでさえ、このような問題に遭遇し続けており、効果的な監視には多大な注意が必要です。

Infoblox：特定された類似手法	
	**同形異義語（ホモグラフ）は、**キリル文字やギリシャ語など、異なる文字セットから視覚的に類似した文字を使用します（「o」を「0」に置き換えるなど）。挿入された文字が必ずしも明確に区別できるとは限らないため、この手法は効果的です。
	**タイポスクワット**には、人気のあるウェブサイトに酷似したドメインを登録する（「amazon[.] com 」を「amazonn[.] com 」に置き換えるなど）ことで、ユーザーを詐欺ウェブサイトに誘導する卑劣な入力ミスが含まれます。
	**コンボスクワット**は有名なブランド名や会社名を「mail」、「security」、「support」などの他のキーワードと組み合わせます。コンボスクワッティングはタイポスクワッティングよりも約 100 倍普及しています。
	**サウンドスクワット**は、口に出すと似たように聞こえる類似ドメイン名を使用する脅威の最新形態です（例：「hsbsee[.]com」ではなく「hsbc[.]com」）。Google Home、Siri、Alexa などのスマートデバイスを使用するユーザーを欺きます。

脅威アクター、侵入テスター、正規のセキュリティツールが使用する DNS トンネリング

DNS トンネリングは、DNS クエリとレスポンス内のデータをエンコードし、C2 操作やデータ漏えいにしばしば利用される秘密の通信を可能にします。

Infoblox は、一部の月に 480 を超える固有の DNS トンネリングドメインを観察しましたが、2024 年 6 月から 2025 年 6 月の間には、平均して毎月 100 を超える DNS トンネリング関連の固有のドメインが検出されました。DNS トンネリングは、サイバー犯罪の使用に加えて、正規の侵入テストやセキュリティツールにも採用されています。次のリストは、C2 機能を備えた一般的な DNS トンネリングツールの概要を示しています。

+100

unique DNS tunneling domains found monthly—benign and malicious

- **Cobalt Strike** は、DNS C2 モジュールを備えた広く使用されている侵入テストツールです。レッドチームや脅威アクターによって利用され、ヘックスでエンコードされたクエリと「post」、「api」、「dx」などのオプションのカスタマイズ可能なプレフィックスを使用します。
- **Dnscat2** は、暗号化された DNS トンネルを作成するために使用されるツールです。オープンソースの侵入テストツールである METASPLOIT に含まれています。
- **DNS Exfiltrator** は、データを DNS クエリにエンコードして抽出するツールで、DNS の潜在的な悪用を実際のシナリオで示します。TXT レコードを使用し、一方向の通信のみを許可し、コマンドラインから起動されます。Infoblox は脅威アクターによる使用を確認しておらず、一方向のメカニズムのため実用的ではないと考えています。
- **Sliver** は、DNS トンネリング機能を備えたクロスプラットフォームの C2 フレームワークであり、敵対者のシミュレーションや悪意のあるキャンペーンで頻繁に利用されます。
- **Weasel** は、Facebook のレッドチームによって開発された、あまり文書化されていない DNS トンネリングツールです。ステルスデータ流出と C2 をサポートし、通常はニッチなレッドチーム演習で使用されます。通信では A レコードと AAAA レコードを使用します。
- **Pupy** は、DNS トンネル機能を備えたオープンソースのマルチプラットフォームリモートアクセスツールで、政府機関や企業を標的としたスパイ活動で歴史的に利用されてきました。通信には A レコードを使用します。
- **Iodine** は、IPv4 トラフィックを DNS 経由でトンネリングするためのよく知られたツールで、侵入テストに使用され、C2 を目的とした国家主体による攻撃などで悪用されることもあります。Iodine は A、TXT、CNAME、MX レコードを使って通信します。
- **Cymulate や AttackIQ といったベンダーから、最近いくつかの自動侵入テストツールが登場しています。**Infoblox は、顧客ネットワーク内にこれらのベンダーに関連するドメインを発見しました。
- **ウイルス対策ツールやスパム対策ツール**も、ドメインまたはファイルハッシュが悪意のある可能性があるかどうかを調べるメカニズムとして DNS を使用します。クエリは「<domain>.<guid>.<avdomain>」または「<file hash>.<guid>.<avdomain>」という形式になり、ドメインまたはファイルハッシュが既知のマルウェアまたはスパムリストにない場合は NXDOMAIN、リストに含まれる場合は 127.0.0.X が返されます。

セキュリティチームには DNS トンネリングを阻止するためのメスが必要

DNS トンネリングを理解して軽減することは、企業をサイバー脅威から保護し、ペイメントカード業界データセキュリティ基準（PCI DSS）、医療保険の相互運用性と説明責任に関する法律（HIPAA）、一般データ保護規則（GDPR）などの規制要件への準拠を確保するために不可欠です。DNS トンネリングツールは広く使用されているため、多くのセキュリティチームは DNS トラフィックを効果的に監視および制御するのに苦労しています。

Infobloxは、次世代ファイアウォールやセキュアアクセスサービスエッジ（SASE）タイプの技術を備えたネットワークでも、DNS トンネリングを頻繁に検出します。これらの技術は DNS トンネリングの検出において改善されましたが、いくつかの複雑な点が残っています。CDN、新しい類似ドメインの使用、正規の DNS C2 ツールの拡張により、すべての C2 アクティビティの検出とブロックが複雑になっています。

そのため、セキュリティチームには、広範で一般的な対策ではなく、正確でターゲットを絞ったツールが必要になります。この課題に対処するには、積極的な脅威アクター追跡と継続的に更新される機械学習技術を活用したプロテクティブ DNS ソリューションが不可欠です。

セクション 4：守備側の課題

TDS、ドメインハイジャック、類似ドメイン、DNS トンネリングなどの従来の攻撃者が利用する DNS 手法に加えて、防御側（SOC アナリスト、リスクマネージャー、CISO）は、ますます多くの課題に直面しています。

このセクションでは、攻撃者が利用するAIの使用、ブランド保護、新しいコンプライアンス義務による圧力の高まりなど、主要な傾向の概要を説明します。最も重要なのは、DNS から導き出された脅威インテリジェンスがこれらの課題に対処するために提供する機会に焦点を当てていることです。

88%

of AI-generated malware evades detections[4]

攻撃者が利用するAIが既存のセキュリティ制御をバイパス

生成AI（GenAI）、特に大規模言語モデル（LLM）は、サイバーセキュリティの変革を推進しています。敵対者は、欺瞞的で説得力のあるコンテンツの作成の障壁を低くする生成 AI にますます魅力を感じており、ソーシャルエンジニアリングや検出回避などの侵入手法の有効性を高めるためにこれを使用します。

これらの新しい AI の課題を補うために、セキュリティチームには、AI によって変更または難読化されず、保管チェーンに十分な透明性を提供する、DNS ベースのテレメトリなどの新しいレベルの真実が必要です。

悪意のある AI の最近の例：

ディープフェイク詐欺

2024 年末、FBI は犯罪者が 生成 AI を使用して大規模な詐欺を実行し、その計画の信憑性を高めていると警告しました。[5]音声クローンなどの生成 AI ツールは、一見信頼できる音声メッセージでターゲットを欺くのに必要な時間と労力を大幅に削減します。特に懸念されるのは、サイバー犯罪者がこれらのツールに簡単にアクセスできることと、セキュリティ保護手段が欠如していることです。音声クローニングは、暗号通貨詐欺用の大規模なディープフェイク動画や、標的を絞った通話中の音声の模倣など、さまざまなシナリオで使用されています。

事例研究：日本語話者を狙った Reckless Rabbit によるディープフェイクの使用

Infoblox Threat Intel は 2024 年 9 月、イーロン・マスクのディープフェイク動画を仮想通貨詐欺に利用した YouTube アカウント乗っ取りキャンペーンについて報告しました。現在、追跡中の **Reckless Rabbit** と呼ばれるアクターも同様の手法を用いており、ディープフェイク動画を詐欺ウェブサイトに直接埋め込んでいます。

Reckless Rabbit は最近、**日本語話者のユーザーに**焦点を移し、AI が生成したニュース記事を通じて偽の投資スキームを宣伝しています。これらのサイトには、**イーロンマスク**や**孫正義**などの著名人のディープフェイクビデオと、信頼性を高めるために捏造された肯定的なレビューが掲載されています。

---

4 Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud. FBI Alert Number: I-120324-PSA, 2024年12月3日

5 AI Could Geneate 10,000 Malware Variants, Evading Detection in 88% of Case, Lakshmanan, Ravie, The Hacker News, 2024年12月23日

以前、このアクターは、**東欧のユーザーをターゲットに、RDGA ベースのドメインと Facebook 広告を使用して**単純なテキストと画像で構成された偽のニュースコンテンツに被害者を誘い込んでいました。

図 5. 最近発見されたディープフェイクページ

Reckless Rabbit は、読売新聞などの大手メディアを装い、**日本語字幕付きのディープフェイク動画**を使った偽記事を拡散しています。これらの記事には**「Finance Legend」**という偽の投資プラットフォームの宣伝があり、登録ボタンをクリックすると問い合わせフォームにリダイレクトされます。Reckless Rabbit は、被害者に高額の利回りを約束して入金を促していると考えられます。

AIを活用したチャットボット

アクターはしばしば被害者の興味に関する情報を収集し、慎重に選んで高度にパーソナライズされた詐欺を仕掛けます。最初の偵察の後、被害者をチャットボットによる会話に誘導するスミッシングメッセージを作成します。これらの会話は数週間にわたって続き、YouTube で「いいね！」を求めたり、ソーシャルメディアで再投稿を求めたりといった、被害者の影響されやすさを評価するための戦術を含む、異常な行動が伴う場合もあります。肯定的なやり取りごとに、アクターは偽の「口座残高」を増加させるように操作します。被害者が現金化しようとすると、アクターは仮想通貨アカウントへのアクセスを要求し、時間をかけて築かれた信頼を悪用して被害者の資金を盗みます。AI 搭載のチャットボットにより、アクターはこれらの会話を自動化し、業務を効率的に拡大することができます。

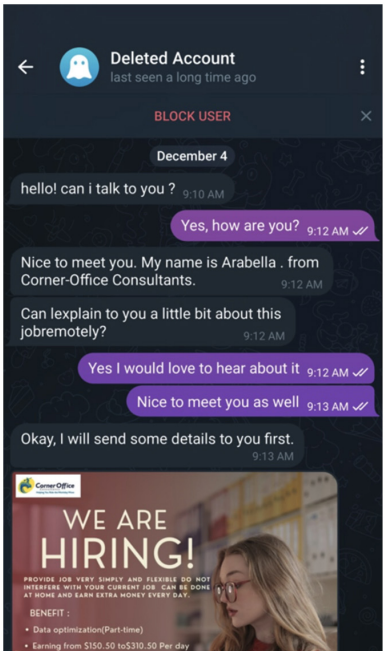


図6. AI/LLM と半自動チャットボットインタラクションを組み合わせて使用する攻撃者が利用するチャットメッセージングの例

コードの難読化と回避

脅威アクターは、生成 AI を使用してマルウェアを難読化、再利用、新しい方法で組み立て、検出を回避することが増えています。このアプローチにより、脅威キャンペーンの作成が加速され、効果的な感染チェーンを構築するために必要な技術的スキルが軽減されます。HP Wolf Security の調査によると、電子メールベースの脅威回避は約 11% 増加しています。[6] 一方、著名なセキュリティベンダーは最近、貪欲な LLM アルゴリズムが自身のマルウェア分類モデルの判定を **88%** のケースで悪意のあるものから無害なものに反転させたと報告しました[7]これは、攻撃者が利用するAIが現在の検出モデルをどれだけ効果的に悪用できるかを示す重要な指標です。

ブランドと組織の評判の保護

ブランドと組織の評判は戦略的資産です。強力な評判は顧客の信頼を築き、市場の信頼性を高め、パートナーや投資家を引きつけ、長期的なブランド価値をサポートします。Forbes によると、「企業のリーダーたちは、常に評判を最も価値のある資産として位置づけています。」[8]ただし、DNS 内でブランドを保護するには、いくつかの課題があります。

- **境界を超えた可視性の限界：**ドメインを監視するには、自社ドメインだけでなく、数千もの類似ドメインやなりすましドメインの可能性も追跡する必要があります。例えば、Infoblox は 2025 年 5 月に 28,331 件の類似ドメインを検出しました。
- **人間が作成した類似ドメインは検出が依然として困難：**類似ドメインは人間によって慎重に選択され、模倣されるため、自動システムの検出能力を超えることがよくあります。
- **手動ドメイン監視はリソースを圧迫：**セキュリティチームには、アラートをモニターし、効果的に対応するためのリソースが不足していることがよくあります。自動化がなければ、ドメイン監視は手間がかかり効率の悪い作業になります。
- **管轄権の障壁が執行を阻害：**発見された高リスクドメインの 87% は米国または欧州連合（EU）の法律が適用されない外国資産管理局（OFAC）によって制裁を受ける事業体に登録されています。その結果、ドメインやウェブサイトの削除は効果がないことがよくあります。

28,331
lookalike domains detected by Infoblox in May 2025

これらの障害を克服するには、セキュリティチームとマーケティングチームは、グローバル DNS の使用状況を詳細に把握し、DNS ベースのインテリジェンスを活用できる DNS エキスパートと連携する必要があります。この連携により、組織の評判やブランドを反映するデジタル資産への脅威をモニター、検出、修復できるようになります。

セキュリティチームに対するコンプライアンスの圧力と DNS の課題

ネットワークおよびセキュリティチームは、進化するベストプラクティスや、セクター全体に適用され、より広範な監視（DNSインフラストラクチャを含む）を必要とする新しい規制（**EU NIS2**や**NIST SP 800-81 Rev. 3**など）により、ますます増大するプレッシャーに直面しています。

6 Hackers Use Image-Based Malware and GenAI to Evade Email Security, Coker, James, Infosecurity Magazine, 2024年1月16日

7 AI Could Generate 10,000 Malware Variants, Evading Detection in 88% of Case, Lakshmanan, Ravie, The Hacker News, 2024年12月23日

8 The Importance Of Brand Reputation: 20 Years To Build, Five Minutes To Ruin, Blanchard, Paul, Forbes, 2019年12月27日

これらのフレームワークには、いくつかの課題があります。

- **運用上の複雑さ：**NIS2 は、リスク評価、24 時間のインシデント報告、継続的なモニタリングを義務付けています。これらの要件は、集中的な可視性や自動化を欠くチームにとっては困難です。NIST SP 800-81 Rev. 3 では、さらに専用の DNS サーバーの導入と内部および外部の DNS トラフィックの暗号化が要求されています。
- **断片化されたツール：**既存のツールはオンプレミス、クラウド、リモート環境に分散していることが多く、ポリシーの不一致や可視性のギャップが生じています。中断を回避するには、DNSポリシー（レスポンスポリシーゾーン（RPZ）など）を一貫して適用する必要があります。
- **限られたリソース：**SOC チームはアラートの量に圧倒され、コンテキストに応じた洞察が不足しています。NIS2 は早期発見と迅速な対応に重点を置いているため、すでに過密な状況にあるチーム、特に DNS レイヤーの可視性が欠けているチームにさらなる負担がかかります。
- **予算の制約：**コンプライアンスには、ツール、トレーニング、DNS ログへの投資が必要です。しかし、DNS ロギングはフォレンジックやインシデント対応に不可欠であるにもかかわらず、組織は予算が厳しい中でこれらのコストを正当化する必要があります。

セキュリティチームには、新しいコンプライアンス要件を満たすためのシンプルなアプローチが必要です。予測的な脅威インテリジェンスを有効にし、DNS レベルで制御を実装することは、NIST SP 800-81 Rev.3 および NIS2 への準拠を簡素化するだけでなく、NIST サイバーセキュリティフレームワーク（CSF）やゼロトラストなどのより広範なセキュリティフレームワークとも整合します。最も重要なのは、グローバルな脅威の防止、可視化、セキュリティ運用の負担軽減を強化することです。

次のステップ

Infoblox は、セキュリティ担当者に、専門家が作成した脅威インテリジェンスを調査し、予測インテリジェンスで環境を保護するための複数のオプションを提供します。

脅威研究者向け：

- Infoblox Threat Intel の調査の詳細については、https://www.infoblox.com/jp/threat-intel/をご覧ください。
- Mastodon で infobloxthreatintel@infosec.exchange にご相談ください。
- 当社の調査と指標には GitHub の https://github.com/infobloxopen/threat-intelligence/ からアクセスできます。

セキュリティチーム向け：

- DNS セキュリティワークショップを https://info.infoblox.com/sec-ensecurityworkshop-20240901-registration.html でリクエストしてください。
- Infoblox Threat Defense の詳細については https://www.infoblox.com/jp/products/threat-defense/ をご覧ください。

使用される用語

アドテック：**広告技術**の略称で、ブランド、広告代理店、パブリッシャー、プラットフォームが**デジタル広告キャンペーン**の企画、実行、管理、分析に使用するソフトウェア、ツール、プラットフォームを指します。オンライン広告エコシステムの基盤です。

BYOD：個人携帯の業務利用

C2：コマンド & コントロール

CDN：コンテンツ配信ネットワークは、**地理的に分散されたサーバーのネットワークであり**、これらのサーバーが連携して、ユーザーの所在地に基づいてデジタルコンテンツ（ウェブサイト、ビデオ、画像、スクリプトなど）を**迅速かつ信頼性が高く安全に**配信します。

CNAME：正規名レコードは、**DNS（Domain Name System）**レコードの一種で、**あるドメイン名（エイリアス）を別のドメイン名（正規名）にマッピングします。**これは、IP アドレスを直接指すのではなく、あるドメインまたはサブドメインを別のドメインに指すために使用します。

DDGA: 辞書ドメイン生成アルゴリズム

DDI：**DNS、DHCP、IP アドレス管理（IPAM）は、**3 つの重要なネットワークサービスであり、**企業ネットワーク全体のIPアドレス空間と名前解決の自動化および中央管理を提供します。**

DGA: ドメイン生成アルゴリズム

DNS：Domain Name System（ドメインネームシステム）

DNS クエリ：**DNS クエリ**（Domain Name System クエリ）は、デバイス（通常はコンピューターや携帯電話）が**人間が読めるドメイン名**（例：www.google.com）を**機械が読める IP アドレス**（例：142.250.190.68）に変換する要求で、これによりインターネット上の正しいサーバーに接続できます。

GDPR: 一般データ保護規則

HIPAA：Health Insurance Portability and Accountability Act（医療保険の相互運用性と説明責任に関する法律）

LLM：大規模言語モデル

MFA: 多要素認証

MXの悪用：これは、MX（メール交換）レコードを悪用または誤用する悪意のある活動を含みます。

NIST：National Institute of Standards and Technology（米国国立標準技術研究所）

NOD：新たに観測されたドメイン

OFAC：**外国資産管理局。米国財務省の一部門で、経済制裁および貿易制裁**を米国の外交政策および国家安全保障目標に基づいて管理・執行します。

OSINT: オープンソースインテリジェンス

PCI DSS：Payment Card Industry Data Security Standard（ペイメントカード業界データセキュリティ基準）

PhaaS：フィッシング・アズ・ア・サービス

RDGA：登録ドメイン生成アルゴリズム

SASE: セキュアアクセスサービスエッジ

TDS：トラフィック分散システム

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

© 2025 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：20250730