Press Release

2025 年 8 月 5 日（火）

Infoblox 株式会社

Infoblox が 2025 年の DNS 脅威状況レポートを発表
AI による脅威と悪意ある広告技術の急増を明らかに

- 新たに観測された 1 億 800 万のドメインのうち、25.1%が悪意あるいは疑わしいと分類
- 顧客環境の 82%が悪意ある広告技術ドメインに接触

2025 年 8 月 5 日（火） – クラウドネットワークおよびセキュリティサービスのリーダーである Infoblox は本日、2025 年の DNS 脅威状況レポートを発表しました。本レポートは、DNS を基盤としたサイバー脅威の劇的な増加と、AI 対応のディープフェイク、悪意ある広告技術、回避的なドメイン戦術を駆使する攻撃者の高度化を明らかにしています。

数千の顧客環境からの事前攻撃テレメトリとリアルタイムの DNS クエリ分析（1 日あたり 700 億以上の DNS クエリ）に基づき、本レポートは脅威アクターが DNS を利用してユーザーを欺き、検知を回避し、信頼を乗っ取る手法を包括的に示しています。

「今年の調査結果は、脅威アクターが大量のドメイン名を登録するだけでなく、DNS の誤設定を利用して既存ドメインを乗っ取り、大手ブランドを偽装するなど、多様な方法で DNS を悪用していることを浮き彫りにしています」と Infoblox Threat Intel 責任者の Renée Burton（レネー・バートン）博士は述べています。「本レポートは、これらの犯罪を隠すためにトラフィック分散システム（TDS）が広く使われていることを明らかにしており、セキュリティチームが攻撃者に先んじるために注視すべき他のトレンドも示しています。」

Infoblox Threat Intel は設立以来、660 以上のユニークな脅威アクターと 20 万 4,000 以上の疑わしいドメインクラスター（同一のアクターによって登録されたと考えられるドメインのグループ）を特定してきました。過去 12 か月間で、Infoblox の研究者は 10 の新しいアクターに関する研究を発表しました。Infoblox Threat Intel は、TDS を通じてユーザーから脅威を隠す悪質な広告技術の広がりと深さを明らかにし、この分野で業界のリーダーシップを牽引しています。

本レポートは過去 12 ヶ月の調査結果をまとめ、攻撃トレンドを明らかにし、セキュリティチームが悪意ある攻撃者に対抗するための重要な知識を提供します。特に、広告技術がこれらの攻撃に果たす役割に焦点を当てています。

主な調査結果

- 過去 1 年間に新たに観測された 1 億 800 万のドメインのうち、25.1%が悪意あるまたは疑わしいと分類
- 脅威関連ドメインの 95%は 1 つの顧客環境でのみ観測されており、セキュリティ業界が脅威を検出し阻止する難しさを証明
- 顧客環境の 82%が悪意ある広告技術（adtech）に関連するドメインを照会しており、これらは多数のドメインを回転させてセキュリティツールを回避し、悪意あるコンテンツを配信
- 過去 12 か月間に Infoblox ネットワーク内で約 50 万のトラフィック分配システム（TDS）ドメインを確認
- DNS トンネリング、データ流出、コマンド＆コントロール（Cobalt Strike、Sliver、カスタムツールを含む）の検出が日々行われており、これらの検出には機械学習アルゴリズムが求められる

新規観測ドメインの増加

Infoblox Threat Intel は、新たに観測されたドメインが 1 億 800 万件にのぼり、そのうち 25%以上が悪意あるものまたは疑わしいものと分類されていることを明らかにしました。年間を通じて、脅威アクターは自動登録プロセスを通じて非常に大量のドメインを継続的に登録、活性化、展開しています。ドメイン数を増やすことで、脅威アクターは「患者ゼロ（patient zero）」アプローチに基づく従来のフォレンジック防御を回避できます。この受動的な手法は、脅威が世界のどこかで既に使用された後に検出・分析することに依存しているため、攻撃者が新たなインフラを増やすにつれて効果を失い、組織は脆弱な状態に置かれてしまいます。

先制的なセキュリティ対策の必要性

これらの調査結果は、AI を装備した攻撃者に対して組織が積極的に対応する必要性を強調しています。先制的なセキュリティ対策への投資が脅威アクターを阻止する決定的な要因となり得ます。Infoblox の先制型の DNS 脅威インテリジェンスを用いたプロテクティブ DNS ソリューションは、初期の影響前に 82%の脅威関連への DNS クエリをブロックしました。

先制的な防御と新たな脅威への継続的な監視がセキュリティチームに有利に働き、攻撃者に先んじて無限のドメイン供給を断ち切ることを可能にします。

レポート全文のダウンロードとその他最新情報

Infoblox が発表した 2025 年の DNS 脅威状況レポート全文（英語）

脅威研究者向け

- Infoblox Threat Intel の研究内容
- Mastodon での情報配信（英語）
- GitHub で研究成果と指標（英語）

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のご依頼
- Infoblox Threat Defense の詳細

Infoblox について

Infoblox は、ネットワーク、セキュリティ、クラウドを統合し、回復力と俊敏性を兼ね備えた運用プラットフォームを構築します。フォーチュン 100 社の 92 社を含む 13,000 社以上のお客様に信頼されており、重要なネットワークサービスをシームレスに統合、保護、自動化することで、企業は妥協することなく迅速に行動できます。infoblox.com にアクセスするか、LinkedIn でフォローしてください。

【本プレスリリースに関するお問合せ】
Infoblox 株式会社
〒107-0062 東京都港区南青山 2-26-37 VORT 外苑前Ⅰ 3 階
Email：SalesJapan@infoblox.com
https://www.infoblox.com/jp