ソリューションノート

DOT と DOH の想定外の課題を解決

まとめ

かつてないほど重要性を増す DNS インフラストラクチャのセキュリティ確保：マルウェア関連インシデントの 90% 以上、ランサムウェアおよびデータ盗難攻撃の半数超が DNS ベクトルに依存。

まずは良いニュースから始めましょう。DNS プライバシーを向上させるために設計された、新しく進化を続ける 2 つのテクノロジーが、著しい発展を遂げています。

一方、悪いニュースもあります。これらのテクノロジーは、サーバーとアプリケーションを外部の DNS リゾルバに誘導し、サブスクリプション加入者のデバイスが、従来の DNS メカニズムを回避して、制御外の DNS サービスにアクセスすることで、企業を潜在的なセキュリティリスクにさらします。そして、これらの変化は今まさに起こっているのです。

Infoblox は、これらの DNS プライバシーの課題を解決するソリューションを組織に提供します。外部の DNS リゾルバへのアクセスをブロックし、内部で暗号化された DNS 解決を提供する機能を通じて、組織は DNS を管理できます。

改善の余地

オープン性の概念は、インターネットの誕生以来、その基盤的な特徴となっています。ユーザーは、安全な HTTPS プロトコルを使用して、Web ブラウザと Web サイト間でクレジットカード番号、電子メール、パスワードなどの機密情報を送信しますが、インターネットアドレスの最初の要求と、それに続く Web サイトの場所の応答はプレーンテキストで送信されます。その結果、DNS は従来、いわゆる「ラストマイル」のセキュリティ問題に悩まされてきました。DNS クライアントとそのローカル DNS サーバー間の通信はほぼ常時暗号化されておらず、そのため、なりすまし、傍受、ハイジャックなどの問題にさらされる可能性があります。過去にエンドツーエンドのセキュリティを強化するための改善が行われてきましたが、Web ブラウザへの通信の最終段階は依然としてスプーフィングに対して脆弱でした。

DOT および DOH の紹介

インターネット技術特別調査委員会（IETF）に所属する業界団体は、これらの問題に対処するにあたり 2 つのメカニズムを提案しています。これらは、オペレーティングシステムのスタブリゾルバまたはローカルアプリケーションと、再帰 DNS リゾルバ間の DNS 通信を暗号化することで機能します。1 つは DNS over TLS（トランスポート層セキュリティ）または DoT、そしてもう 1 つは DNS over HTTPS または DoH です。DoT と DoH は DNS のプライバシー問題に対処するために設計されましたが、ブラウザやアプリケーションの動作に対して、重大な DNS 動作の変更をもたらします。これらの変更は、複雑さを増大させ、ネットワークセキュリティに予期せぬ影響をもたらし、企業におけるセキュリティおよびコンテンツフィルタリングサービスの提供に直接影響を与えます。DoT と DoH は、サーバーとアプリケーションを外部の DNS リゾルバに誘導できるため、クライアントデバイスは従来の DNS メカニズムを回避して、管理外の DNS サービスにアクセスし、企業を潜在的なセキュリティリスクにさらす可能性があります。一例として、米国国家安全保障局（NSA）は最近、組織が独自の DoH リゾルバをホストし、内部 DNS トラフィックを外部のサードパーティリゾルバに送信しないようにするためのガイダンスを公開しました。

DNS OVER TLS（DOT）

DoT は、DNS クライアントと DNS サーバー間の TLS 暗号化および認証を階層化するための接続プロトコルとして、一般的な伝送制御プロトコル（TCP）を使用する IETF 標準です。多くの場合、オペレーティングシステムレベルで機能し、TCP ポート 853 を介して通信します。この広く知られたポートはすべての暗号化された DNS トラフィックに使用されており、ネットワーク管理者にとっては慣れ親しんだポートです。DoT トラフィックは暗号化されていますが、よく理解されているポートを使用することで、ネットワーク管理者は、暗号化された DNS が表示された際にモニターおよび制御しやすくなります。DoT は、DNS 業界の伝統的なプレーヤーによって支持されている成熟した標準でもあります。

DNS OVER HTTPS（DOH）

Apple、Microsoft、Mozilla Foundation、Chromium Projects の支援を受けた DoH は、DNS クライアントと DNS サーバーの通信セキュリティに対処するもう 1 つの IETF セキュリティプロトコルです。DoH は、DNS クライアントとサーバー間の暗号化と認証を提供するセキュリティプロトコル拡張 HTTPS を活用します。

DoH の潜在的な問題は、すべての HTTPS トラフィックが使用するのと同じ TCP ポート（443）を使用することです。DoH ベースの DNS リクエストと通常の HTTPS リクエストを区別できないため、DoH 関連の DNS 問題のトラブルシューティングが難しくなる可能性があります。たとえば、ネットワーク管理者が DNS 監視を使用して既知の悪意のあるドメインへの DNS リクエストをブロックしている場合、それらのリクエストは HTTPS では表示されません。したがって、その悪意のあるトラフィックは検出されないでしょう。

さらに、DoH はオペレーティングシステムではなくアプリケーション層で実装されることが多く、これによりブラウザトラフィックが企業の DNS 制御をバイパスする可能性があります。DNS 制御の回避は、企業が DNS に求めるネットワークパフォーマンス、セキュリティ、スケール、信頼性のレベルを維持するためのサポートチームの能力を妨げる可能性があります。

企業が DOT と DOH において抱える課題

ネットワークおよびセキュリティ管理者は、高速なアプリケーションアクセスを確保し、マルウェアやその他のインターネット由来の脅威からユーザーを保護するために、ネットワーク制御プレーンの重要な要素として DNS を利用しています。新しい DoT および DoH 標準により、ネットワークおよびセキュリティチームが直面する可能性のある注目すべき課題は次のとおりです。

- **集中型 DNS：**DNS の外部制御により、クライアントは IT 部門が提供しない第三者によって管理される集中型 DNS リゾルバを使用することができるため、これはリスクをもたらし、ネットワークリソースの効果的な管理とセキュリティの確保を困難にする可能性があります。
- **企業制御のバイパス：**DoH は、独自の DoH 設定を持つ数百のアプリケーションやウェブサイトが DNS 制御をバイパスする可能性をもたらします。DNS ハイジャックなどの DNS エクスプロイトの監視を複雑にするだけでなく、DoH はアダルトコンテンツ、ゲーム、ストリーミング、マルウェアサイトなどの企業コンテンツフィルターをバイパスする可能性もあります。
- **データ持ち出しとマルウェア拡散への露出：**DoH が制御されていない場合、保護されたネットワークへのバックドアを開く可能性があるため、データ持ち出しとマルウェア拡散への露出が増大する可能性があります。サイバー犯罪者は、DNS をバックドアとして利用し、機密情報を取得・持ち出ししたり、デバイスとのコマンドアンドコントロール（C&C）通信を通じてマルウェアを拡散したりします。DoH の DNS リクエストは暗号化されているため、第三者（例えば、既知の悪意のあるドメインへのリクエストをブロックするためにパッシブ DNS 監視を利用するサイバーセキュリティソフトウェアなど）には見えません。通常、セキュリティチームは、社内 DNS インフラストラクチャの脅威インテリジェンスと、人工知能および機械学習に基づく分析を組み合わせることで、これらの攻撃を効果的に阻止できます。DoH はこれらの DNS セキュリティ対策を回避するため、企業がこれらの DNS ベースのフィルターやその他の DNS ベースのフィルターに晒される可能性が新たに生じます。

  例えば、PsiXBot マルウェアの最新バージョンは DoH を使用して悪意のある通信を暗号化し、通常の HTTPS トラフィックに紛れ込んで、データを窃取したり、被害者をボットネットに追加したりするマルウェアをインストールします。

- **DNS サーバーのオーバーヘッドの増加／ DNS サーバーのパフォーマンスの低下：**DoT および DoH は、各 DNS クエリが DNS サーバーに与える負荷を増大させ、ユーザーの体験品質に影響を与える可能性があります。従来の DNS はユーザーデータグラムプロトコル（UDP）に基づいており、オーバーヘッドは最小限に抑えられています。一方、DoT および DoH は、DNS サーバーにとってよりリソース集約型な TCP 上で動作します。さらに、DoT と DoH のどちらにおいても、DNS サーバーがクエリを復号化し、応答を暗号化する必要があり、これにより DNS サーバーのオーバーヘッドがさらに増加します。DNS サーバーの管理者は、従来の DNS クエリと比較して、DoH および DoT ベースのクエリレートを処理できるサーバーの容量が大幅に減少することを想定する必要があります。

異なるブラウザとオペレーティングシステム

展開計画

Google DNS、Cloudflare、Quad9 などの多くのパブリック再帰 DNS プロバイダーは、サービスの一部として DoT および DoH を提供しています。多くのオペレーティングシステムのクライアントは DoT を選択する必要がありますが、多くの Android クライアントはデフォルトで DoT を使用するように設定されています。しかし、DoH を使用する場合、Chromium や Mozilla などのウェブブラウザは、それぞれクライアントが接続するための独自の方法を必要とします。

Chromium

DoH の Chromium 実装は、Google Chrome、Microsoft Edge、Opera など、Chromium プロジェクトに基づくすべてのブラウザに影響を与えます。Chromium はデフォルトで自動モードに設定され、サポートされているオペレーティングシステムで構成されたリゾルバのリストを調べて DoH の可用性を確認し、使用可能な場合にのみ構成されたリゾルバを DoH に使用します。また、Android の DoT OS クライアント設定を監視し、制御可能で予測可能な方法で動作する予定です。ほとんどの Infoblox 顧客にとって、Chromium の変更によりリゾルバまたはネットワークを変更する義務は生じないかもしれません。

Mozilla

Mozilla は、DoH を使用するデフォルトの信頼できる再帰的リゾルバとして Cloudflare を提供しています。Mozilla は、必要と判断した場合に DoH の使用を検出して無効化します。残念ながら、従来の DNS 解決にスムーズにフォールバックするための方法は、まだ実証されておらず、すべての状況に適しているとは限りません。一部の企業は、組織内にインストールされているブラウザを完全には制御できない場合があります。例えば、

BYOD、在宅勤務、その他のモバイルシナリオにおいて、ブラウザ設定に関する会社の推奨を確実に遵守することは難しいかもしれません。同様に、多様なエンドユーザを抱える通信サービスプロバイダーは、ネットワークデバイス上のブラウザ設定に対する影響力がさらに低下します。

Apple

Apple が最近リリースした iOS と macOS のバージョンは、DoT および DoH プロトコルの両方をサポートしています。これらの設定は、オペレーティングシステム全体から MDM プロファイルやネットワーク拡張機能、個々のアプリケーション、またはアプリケーションの特定のネットワーク要求に至るまで、選択的に適用することができます。

Apple によると、暗号化された DNS を有効にする方法は 3 つあります。あるオプションでは、システム全体に暗号化された DNS 設定を適用できます。ユーザーまたは管理者は、オペレーティングシステム上のすべてのアプリケーションのデフォルトリゾルバとして、1 つの暗号化された DNS サーバーを選択できます。開発者は、そのサーバーを使用するように OS を構成するネットワーク拡張アプリケーションを作成したり、暗号化された DNS 設定を構成するクライアントに MDM プロファイルをプッシュしたりできます。このオプションを使用しない場合、他の 2 つのオプションが自動的に有効になり、デバイス所有者はそれらを直接無効にすることはできません。

2 番目のオプションは、ドメイン所有者向けです。ドメインに対して暗号化されたリゾルバの存在に関するメッセージ設定をドメインレベルで構成できます。リゾ r これらの設定が検出・検証されると、そのドメインの DNS トラフィックはドメインが提供する暗号化されたリゾルバに再ルーティングされます。

最終的な選択肢は、アプリケーション層で暗号化された DNS を使用することです。ここで、開発者は、個々のアプリケーションから DoT と DoH を直接使用できるアプリケーションを作成できます。このオプションは、OS が構成されていない場合に、開発者がアプリケーション接続の一部またはすべてに対して特定のサーバーを選択できることを意味します。

Apple は、特定のネットワークがポリシーによってネットワーク上の暗号化された DNS 通信をブロックした場合に、特定のメッセージでユーザーに警告する予定です。特定のネットワークにはプライバシー警告が視覚的に表示され、特定の DoH リゾルバを使用するように設定されたアプリケーションは正しく通信しません。

Microsoft

Microsoft は 2019 年に DoH をサポートする意向を発表し、Windows DNS クライアントに DoH を採用しました。また、将来のバージョンでは DoT をサポートするオプションも用意しています。Microsoft は、従来の DNS プロトコルへのフォールバックを許可することでネットワーク管理者が制御を維持できるようにする一方で、ユーザーが DoH を使用するために専門知識を必要とすべきではないという前提で、このアプローチを考案しました。

設定されると、DNS クライアントは「オポチュニスティック・モード」で動作し、従来の DNS の代わりに DoH プロトコルを使用しようとします。ただし、DoH プロトコルが利用できないか応答しない場合、従来の DNS にフォールバックするようにクライアントを構成できます。初期の信頼できる DoH リゾルバは、Cloudflare、Google、Quad9 で構成されます。

INFOBLOX は DOT と DOH の課題を解決します

安全なクラウド管理ネットワークサービスの業界リーダーである Infoblox は、既存の内部 DNS インフラストラクチャを迂回すると、運用の複雑さが増すと主張しています。これらの新しい DNS プライバシーオプションは、まだ展開し始めたばかりです。組織は、これらのテクノロジーがもたらすリスクを軽減するため、今すぐ対策を講じる必要があります。最低限、開始点として有効となるのは、内部 IP アドレスとインターネット上の DNS サーバー間の直接の DNS トラフィック（DoT および DoH を含む）をブロックすることです（図 1）。このステップにより、エンドユーザは自社の内部 DNS インフラストラクチャを使用し、IT 組織が DNS 解決ポリシーを包括的に適用し、問題をトラブルシューティングできるようにします。Infoblox は、これらの DNS プライバシーの課題を解決するソリューションを組織に提供します。外部の DNS リゾルバへのアクセスをブロックし、内部で暗号化された DNS 解決を提供する機能を通じて、組織は DNS を管理できます。

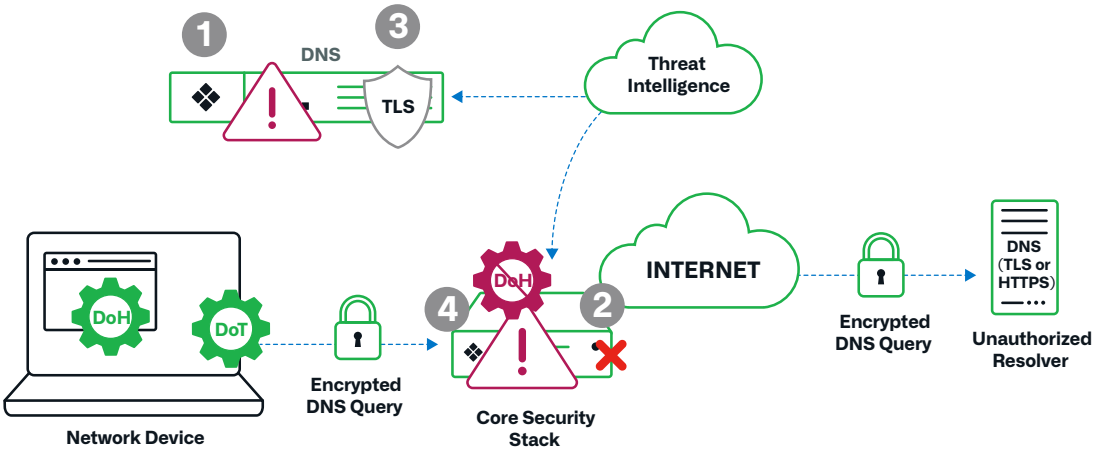

図 1：DoT/DoH のベストプラクティスにより、ユーザーとデバイスを保護します

DoH ドメインへの解決をブロック

BloxOne® Threat Defense、は、DNS を最初の防衛線として使用します。DoH ドメインへの解決をブロックし、既存の内部 DNS へのスムーズなフォールバックを促進します。これらの機能により、DoH の悪用を防止し、リスクを軽減します。

BloxOne Threat Defense には、DoH の管理を支援するいくつかの機能が含まれています。

- DoH サプライネットワーク管理者に対するポリシー脅威インテリジェンスフィードは、DoH ベースのセキュリティポリシーを無効にすることで、脅威を検出・軽減するために使用される DNS アクセス方法を制御する能力を提供します。ブラウザは、ユーザーのアクティビティを中断することなく、組織が管理する DNS にスムーズにフォールバックします。
- 既知の DoH IP と DoH ドメインのための DoH ポリシーフィードが、Infoblox の脅威インテリジェンス集約および配信プラットフォームである Threat Intelligence Data Exchange に追加されました。NGFW などの他のセキュリティツールは、このデータフィードと関連するインテリジェンスを使用して、外部サーバーへの DoH トラフィックをブロックすることができます。
- ユーザーは、Infoblox の脅威調査ツールである Dossier 内で、DoH 関連のドメインと IP を確認できます。

これらの機能は、BloxOne Threat Defense のすべてのサブスクリプションレベルで利用可能です。

Infoblox の暗号化された DNS

Infoblox Network Identity Operating System（NIOS）は、Infoblox のコアネットワークサービスを支える OS であり、ネットワークインフラストラクチャの継続的な運用を保証します。

Infoblox Encrypted DNS は、Infoblox によるクラス最高の DNS サービスを提供しつつ、効率的な暗号化を提供する NIOS の機能です。起動機能には、DOH と DoT のサポートが含まれます。

Infoblox Encrypted DNS は、DNS トラフィックを暗号化するための独自のアプローチを提供します。ロードバランサーやオーバープロビジョニングに依存する方法とは異なり、Infoblox Encrypted DNS は、すべての DNS ニーズに対応する単一のサービスとして機能します。標準機能には、高度な DNS 保護や DNS キャッシュアクセラレーションが含まれており、すべて同じ高いスケーラビリティを持つ DNS サービスからご利用いただけます。

結論

Infoblox は、現代の企業ネットワークが求めるネットワークパフォーマンス、セキュリティ、スケーラビリティ、信頼性をお客様が維持できるよう支援することに尽力しています。これらの変化は、最近のブラウザの更新や OS のリリースによって、現在のネットワークに導入されることで行われています。「ラストマイル」問題の解決は重要で価値のある取り組みですが、企業は DNS トラフィックの可視性と制御を維持する必要があることも当社は認識しています。NSA を含む著名なセキュリティ機関は、これらの技術がもたらすリスクを軽減するための対策を組織に推奨しています。お客様は Infoblox ソリューションを活用することで、DNS の制御を維持し、新たな DNS プライバシーイニシアティブに伴う予期せぬ下流の問題を軽減できます。これらの進化する技術と Infoblox ソリューションの詳細については、Infoblox Community をご覧ください。

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 : 20230919v1