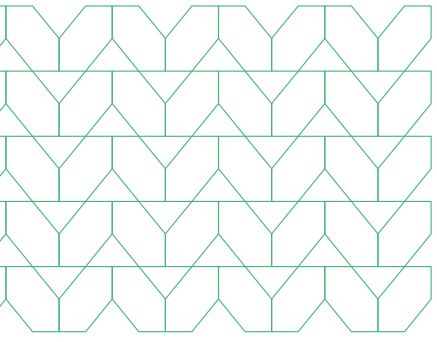
MENLO SECURITY

攻撃者が既存のエンタープライズセキュリティを回避した結果、検知回避型脅威が急増

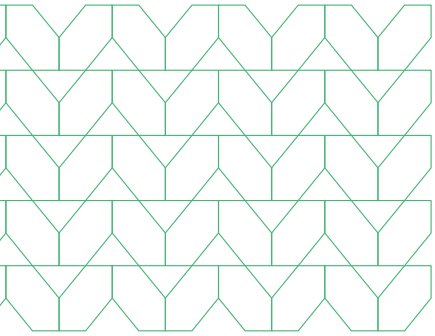
悪意のある攻撃者は常に、最も侵害しやすい経路を探し求めています。ネットワークセキュリティとエンドポイント保護はますます強固になっていますが、ブラウザーは最も普及しているエンタープライズアプリケーションの1つでありながら、最も防御されていないアプリケーションの1つでもあるのです。ハッカーはフィッシングやランサムウェアのための足場を築くために、早くから斬新で回避的な手法を使ってブラウザーを侵害してきました。

サイバーセキュリティへの投資は毎年継続的に行われていますが、脅威は相変わらず侵入に成功しており、ユーザーは毎日のように影響を受けています。セキュリティ意識向上トレーニングは、最もわかりやすい攻撃をユーザーが認識するのに役立っていますが、そのようなアプローチでは脅威を100%捕捉することはできません。一般的に導入されているセキュリティソリューションに対して、単純な攻撃が今でも有効なのは、それが理由です。



ブラウザーを使った業務が増加したため、それに関連する攻撃とデバイスの侵害が急増しています。回避的な脅威の50%は信頼できると分類されたWebサイトからのもので、ブラウザー内で起きています。

Webブラウザーは、企業内で最も多く導入されているアプリケーションでありながら、同時に最も守られていないという不名誉な立場に置かれています。ほとんどの企業ユーザーは、Webやエンタープライズクラウド、SaaSアプリケーション、そしてメールにアクセスするために、様々なデバイス上で複数のブラウザーを使用しています。そのため、ブラウザーはフィッシングやマルウェア攻撃において最も狙われる標的の1つとなっているのです。残念ながら、セキュアWebゲートウェイ（SWG）やEndpoint Detection and Response（EDR）、ファイアウォールなどの既存のセキュリティ制御では、これらの攻撃を阻止することができません。攻撃者はこれら従来型のセキュリティソリューションがどのように機能するかを理解しており、それらを回避するために高度に回避的で適応型の手法を進化させています。企業がセキュリティスタックへの投資を増やしているにも関わらず、ユーザーはこれまで以上に危険に晒されているのです。



ユーザーは勤務時間の75%をブラウザー経由の業務に充てており、生産性や効率性を上げ、コラボレーションするために重要なクラウドやSaaSベースのアプリケーション、その他のWebベースのツールにアクセスしています。

攻撃者は現代のエンタープライズセキュリティスタックに「鎧の隙間」を発見しました。この隙間は、新しい種類の強力で効果的な脅威であれば、すり抜けることができます。このような脅威は検知回避型脅威（HEAT：Highly Evasive and Adaptive Threat）と呼ばれ、ダイナミックに行動し、ファイルレス攻撃や遅延実行などの高度な技術を駆使して検知を免れ、従来型のセキュリティ対策を回避します。これらの脅威はファイアウォールやSWG、EDRソリューションの死角を攻撃するように設計されているため、セキュリティの専門家でもそれらを特定して軽減するのは困難な場合があります。検知回避型脅威は、特に脆弱なWebブラウザーを狙ってマルウェアを配信し、ユーザーシステムを侵害し、機密データを盗み出します。

検知回避型脅威の増加と高度化

企業はファイアウォールやSWG、EDR、サンドボックス分析、URLレピュテーションエンジン、そしてフィッシング検知などを導入し、「従来型の」攻撃ベクトルに対抗するための防御を構築してきました。Webブラウザーは通常適切な保護機能を備えていないため、ITチームとセキュリティチームは検知ベースのアプローチに頼らざるを得ませんが、シグネチャを使うアプローチでは既知の脅威しか識別できず、特にブラウザーを標的にした回避型の脅威を効果的に阻止することはできません。そのため、ブラウザー内の可視性および制御性、そして脅威からの保護の必要性がますます明らかになりつつあります。企業がブラウザーセキュリティを完全に導入しない限り、最近の攻撃に見られるように、攻撃者は検知回避型脅威を使用して企業ネットワークへの侵入を続けるでしょう。

検知回避型脅威の例：1

Oktaハッカーが、多要素認証（MFA）バイパスの手法により130以上の組織を攻撃

この攻撃者は最近TwilioとCloudflareに対する攻撃を行い、136の組織を対象としたさらに大規模なフィッシングキャンペーン（MFAバイパス攻撃により9,931のアカウントが侵害された）にも関与しています。この攻撃は標的となった組織の従業員からOkta IDの認証情報と2要素認証（2FA）コードを取得しようとするもので、被害組織のほとんどは、米国、インド、カナダ、フランス、スウェーデン、オーストラリアに拠点を置いていました。使用されたフィッシングキットは、それ以前には公開されていなかったものです。このキャンペーンの背後にある動機は不明のままですが、スパイ行為と金銭的利益を目的としており、攻撃者が機密データ、知的財産、企業のメールボックス、資金にアクセスできるようにするためのものと考えられています。

検知回避型脅威の例：2

ロシアが支援する攻撃者が、ウクライナを支援する国々の外交機関への侵入を継続

ロシアの諜報機関（特にハッカーグループのNobelium/APT29）は、海外の外交機関、NATO加盟国の外交官、欧州連合とアフリカのその他の組織を標的としたスパイ活動に関与しています。この攻撃はカナダのインフラへの攻撃と同時に行われており、これも同様にロシアと関係があると考えられています。

SolarWindsへのサプライチェーン攻撃で知られるNobelium/APT29は、悪意のあるサイトに誘導する巧妙に作成されたスピアフィッシングメールを使って攻撃を開始しました。このメールは、検知を回避して悪意のあるペイロードを配信するために、HTMLスマグリングという高度な回避技術を採用しています。現時点で重大な被害は報告されていませんが、カナダ当局は重要なシステムを保護し、緩和策を適用することの重要性を強調しています。

検知回避型脅威の例：3

データを収集し、遠隔操作を可能にするための、医療機関を標的にした積極的なマルウェアキャンペーン

積極的な攻撃者が、高度に回避的なマルウェアの亜種とSEOポイズニング（従来のセキュリティ対策を回避し、検索エンジンの結果を操作するためのレガシーURLレピュテーション回避（LURE）として分類される、広く知られたURL回避手法）を使用して金融および医療分野を狙っています。

この積極的なキャンペーンには、複数レイヤーでの難読化、特権の昇格、データ収集が含まれます。感染が成功すると、攻撃者は被害者のデバイスの遠隔操作が可能になり、その状態を維持して機密情報を収集します。攻撃の深刻さと現在進行中であるという状況を考慮すると、組織、特に医療分野の組織には厳重な警戒を怠らず、システムを保護するための適切な措置を講じることが推奨されます。

マルウェアの42%は、アーカイブ形式で配信されています。攻撃者が境界型のセキュリティ制御を回避するため、今ではアーカイブがマルウェアを配布するための最も一般的なファイルタイプになりました。

検知回避型脅威の例：4

攻撃者がGoogleのオープンソースのGC2ツールを使用して、大手メディアを標的としたデータの流出とアカウント侵害を実行

中国が支援するグループであるAPT41（Barium）は、Googleのオープンソースのコマンド&コントロール（GC2）ツールとLUREによる回避手法を使い、Googleドライブでホストされている悪意のあるパスワードで保護されたファイルを利用して台湾の大手メディアを標的にしました。この標的型キャンペーンは、2つの重要なトレンドを浮き彫りにしました。1つは、中国の脅威グループがGC2などの公開ツールを使用することが増えていること、もう1つは攻撃者が検知を避けるために正規のクラウドサービスを使用していることです。信頼できるクラウドサービスへのリンクは、アラームを鳴らさないのです。

Googleは、サイバー犯罪者や国家が支援する攻撃者がマルウェアのホスティングやコマンド&コントロール（C2）運用のインフラを考える際に、クラウドサービスが有効な選択肢になっていると主張しています。フィッシングキャンペーンでは、さまざまなマルウェアがZIPアーカイブファイルとしてGoogleドライブに保存されていることがわかっています。攻撃ベクトルとしてクラウドサービスが持続的に使用されていることは、アカウントを認証情報の漏洩から保護するために堅牢なセキュリティ対策が必要であることを示しています。

検知回避型脅威の例：5

Microsoft 365を狙ったフィッシング攻撃を簡素化する新しいPhishing-as-a-Serviceキット

Phishing-as-a-Service（PhaaS）プラットフォームの「Greatness」では、米国、カナダ、英国、オーストラリア、南アフリカでMicrosoft 365を使用する組織を標的とした活動が急増しています。このプラットフォームは、犯罪者がMicrosoft 365のページを模倣してユーザーの認証情報やセッションクッキーを盗もうとする際に必要になるインフラや難読化されたJavaScript、画像など、フィッシングキャンペーンを成功させるためのツールをすべて提供します。

攻撃者がセッションクッキーを取得すると、被害者のメール、ファイル、Microsoft 365サービスのデータにアクセスできるようになります。盗まれた認証情報は多くの場合、企業ネットワークの侵害に使用され、ランサムウェアの展開など、さらに危険な攻撃につながります。

有名ブランドを模倣した新たなフィッシングサイトが、毎分のように生まれています。

企業はどのようにすれば、高度に回避的なブラウザーベースの脅威から自らを守ることができるのでしょうか?

検知回避型脅威から企業を守るためには、新しい種類のソリューションが必要です。既存のオンプレミスおよびクラウドベースのネットワークセキュリティは、既知の脅威のシグネチャやネットワークベースのテレメトリで訓練されたAIに依存しているため、未知のフィッシング脅威や回避手法を検知できません。組織には、すべてのWebトラフィックを完全に可視化し、動的なポリシーの適用を可能にする防御的なブラウザーセキュリティソリューションを必要です。そうして初めて、ITチームとセキュリティチームはユーザーを標的にした高度に回避的な脅威を特定し、未然に防ぐことができるのです。

攻撃者が回避型の脅威を使用する傾向が強まっていることから、Menlo Securityはブラウザーを標的とした検知回避型脅威を検知してブロックするための一連の防御機能を導入しました。HEAT Visibilityはインラインで分析を行い、すべてのブラウザーセッションにエンドツーエンドの可視性を提供します。この可視性により、高度に回避的なブラウザーベースの脅威に関する豊富なコンテキストを持つ実用的なインテリジェンスが提供され、迅速なインシデント対応が可能になります。このようなデータセットは、他のソリューションでは見ることができません。

また、Menlo SecurityのHEAT Shieldは、コンピュータービジョンやURLリスクスコアリング、Webページの要素の分析など、複数のAIベースの技術を活用して、開かれているリンクがユーザーの認証情報を盗むように設計されたフィッシングサイトかどうかをリアルタイムで正確に判断します。HEAT Shieldにより、検知回避型脅威やゼロアワーフィッシング攻撃に関するアクション指向の脅威インテリジェンスを表示するブラウザーにリアルタイムの保護を提供し、エンドユーザーにシームレスなブラウジング体験を提供しながら、組織のセキュリティを強化するために必要な情報を提供できます。

お問い合わせ：
www.menlosecurity.jp
japan@menlosecurity.com

Menlo Securityについて

Menlo Securityは、他に類を見ないアイソレーションを活用したクラウドセキュリティプラットフォームにより、企業が脅威を排除し、生産性を完全に維持することを可能にします。Menlo Securityは、悪意のある攻撃を防ぐために最も安全なゼロトラストアプローチを提供し、エンドユーザーはセキュリティの存在を気にせずにオンラインで仕事をすることができ、さらにセキュリティチームの運用負担を軽減することで、クラウドセキュリティの目標を実現できる唯一のソリューションとなっています。これにより企業は安全なオンライン体験を提供することができ、ユーザーは安心して業務を行いビジネスを進めることができます。