MENLO SECURITY

ブラウザセキュリティの現状：

ゼロアワーフィッシング攻撃からブラウザを守る

ミニレポート

今こそブラウザのセキュリティを強化する時です

Menlo Labsの脅威リサーチチームは、ブラウザベースのフィッシング攻撃が過去6ヶ月間で198%増加したことを観測しました（2023年上半期との比較）。特に回避型に分類される攻撃については、206%の増加を観測しています。回避型攻撃とは、従来型のセキュリティ制御を回避するためにさまざまなテクニックを利用する攻撃であり、急速に増加しています。サイバー犯罪者はこれらの手法を使うことで攻撃の成功率が高くなることを知っているのです。回避型の脅威は現在、ブラウザベースのフィッシング攻撃全体の30%を占めています。

多くの企業は業務でブラウザを使用しており、Webベースの脅威から保護するために既存のネットワークベースのセキュリティ制御に依存しています。しかし、回避型のゼロアワーフィッシング攻撃は、そのような制御を回避することができます。企業はもはや、従来の検知ベースのネットワーク制御や継続的なエンドユーザートレーニングによってユーザーの安全を守ることはできません。攻撃者はこのことを認識しており、回避型のフィッシング攻撃とソーシャルエンジニアリングのテクニックを組み合わせて、ブラウザ経由でユーザーを標的にし、ユーザーの認証情報を盗み出そうとしています。

これは、昔ながらのフィッシングとどう違うのでしょうか？

これらの攻撃の本質はフィッシングの進化版ですが、まったく同じものではありません。これらの攻撃は動的で回避的であり、従来のセキュリティツールでは効果的に検知することができないのです。ゼロアワーフィッシング攻撃は、様々なテクニックを併用します：

- スミッシング
- AiTM（Adversary In The Middle）フレームワーク
- 画像ベースのフィッシング
- ブランドへのなりすまし
- 多要素認証（MFA）のバイパス

今、何をなすべきか？3つの重要な洞察

CISOは、脅威の標的が変化した環境において、防御の目標を変更する必要があります。なぜなら、ユーザーの認証情報の侵害は、最終的にランサムウェアの発生や知的財産の盗難につながるサイバー犯罪キャンペーンの最初のステップになることが多いからです。Menlo Security Cloudでは、これらの手法がより頻繁に組み合わされるようになっていることが観測されています。これらの認証情報を盗む試みは、TwilioやCaesarsに対する最近の攻撃、ソフトウェア会社Retoolにおける最近の侵害と一致しています。

サイバーセキュリティ上の懸念という意味では、人間が依然として危険にさらされている点であり、最も弱い部分であることに変わりはありません。このように露出されたブラウザの「パイロット」であるユーザーには、何らかの支援が必要です。このレポートをまとめるために、Menlo Labsの脅威調査チームは、2022年12月から2023年12月までの間の4,000億件を超えるWebセッションを含む、Menlo Security Cloudから収集された脅威データとブラウザテレメトリを調査しました。さらに、チームは2023年第4四半期の30日間を詳しく調査し、サイバー犯罪者の進化する戦術と攻撃パターンに関するより具体的な洞察を得ました。このレポートには、このデータに基づいた3つの洞察が含まれており、変化する環境においてCISOとそのセキュリティチームがより適切な意思決定を行うのに役立ちます。

洞察 1：

フィッシング攻撃は著しく進化しています

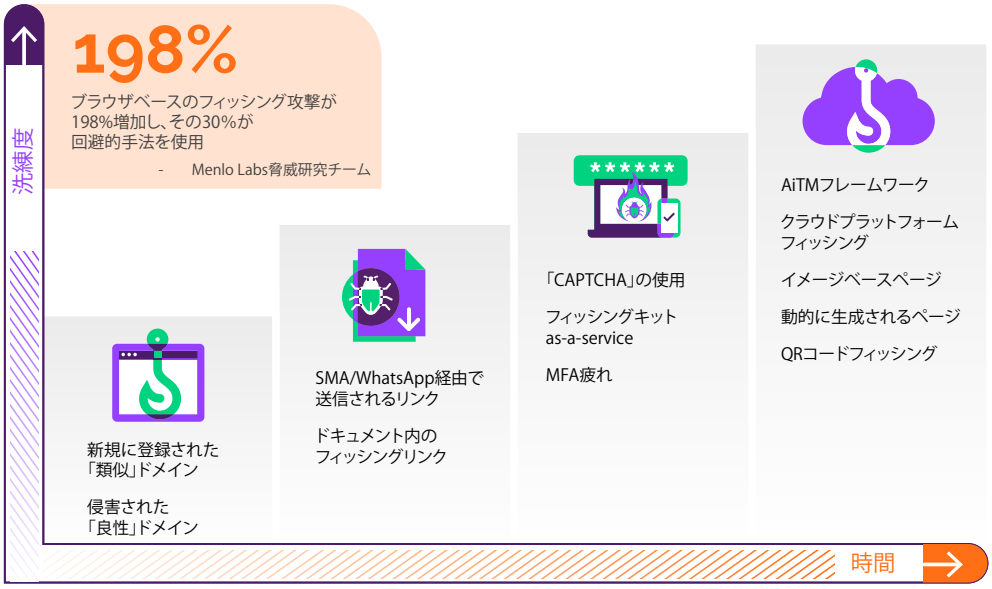

図1：フィッシングの進化

多くのサイバー攻撃は、認証情報を盗み、企業のアプリケーションにアクセスし、アカウントを乗っ取るために、何らかのフィッシング詐欺から始まります。フィッシングが最も一般的な最初の攻撃ベクトルであるのは、それが有効だからです。
世界のデータ侵害の16%はフィッシングから始まっています[1]。しかし回避型のフィッシング手法はより効果的で、従来型のセキュリティツールを回避できるため、増加率は高まっています（206%の増加）。

[1] IBMSecurity. (2023). Cost of a Data Breach Report 2023. IBM. https://www.ibm.com/downloads/cas/E3G5JMBP

攻撃者は、回避的な戦術に加えて、自動化ツールや生成AIツールを使用して攻撃自体の質と脅威活動の量を向上させています。攻撃者は現在、独自の脅威シグネチャを持つ数千ものフィッシング攻撃を行っています。そしてこれらの攻撃で使われる文章では、文法的な間違いが少なくなっており、人間の目で見ても脅威に気づくことが難しくなっています。

最近の30日間で、Menlo Securityの脅威調査チームは次のことを発見しました：

31k

以上の

ブラウザベースの
フィッシング攻撃が
Menloのお客様を
狙いました

Menlo Securityの顧客に対して、31,000件を超えるブラウザベースのフィッシング攻撃が行われました。これらの標的型の企業攻撃は複数の業界と地域にまたがっており、Lazarus、VIPER、Qakbotなどの悪名高い攻撃者によって行われています。[2]

ブラウザベースの攻撃の急増は、既知の悪意のあるサイトや一時的な偽サイトからのものではありません。実際、フィッシングリンクの75%は、既知の、カテゴリ分け済みの、または信頼できるとされたWebサイトでホストされています。

75%

のフィッシングリンク
は、既知の、または
カテゴリ分け済みの、
または信頼できるサイト
でホストされています

500

の異なる企業が

1ヶ月間に
攻撃を受けています

サイバー犯罪者はまた、フィッシング攻撃でより広い範囲の組織を標的にしています。過去の報告では大企業が最も大きな被害を受けていましたが、現在ではあらゆる規模の組織が攻撃対象となっており、1ヶ月間で500もの企業が攻撃を受けています。

（この調査で取り上げた攻撃は、回避的な手法が使用されていたとしても、ブラウザセキュリティによって阻止されました。）

[2] Lazarus - https://www.menlosecurity.com/blog/lazarus-group-browser-exploit-effect
IPER - https://www.menlosecurity.com/blog/vip3r-new-actor-old-story-great-success/
Qakbot - https://www.menlosecurity.com/blog/an-anatomy-of-heat-attacks-used-by-qakbot-campaigns

こうしたフィッシング攻撃は、特定の業界や地域に限ったものではありません。どれだけ教育を施し、Webセキュリティツールを活用しても、フィッシングは引き続き蔓延し、あらゆる業種の企業に影響を及ぼします。このような攻撃の影響を防ぐには、機密情報が盗まれるのを防ぎ、アカウントに疑わしい活動の兆候がないか監視するための予防策と効果的なブラウザセキュリティ制御が必要です。

洞察 2:

回避型のフィッシングは新たな攻撃ツールです

つい最近まで、サイバー犯罪者は企業システムに侵入するために他の手段を使っていました。外部に公開されたシステムのパッチ未適用の脆弱性は格好の標的で、攻撃者はそこに重点を置き、オペレーティングシステム、アプリケーション、従来のセキュリティインフラストラクチャの脆弱性を侵害していました。しかし、最近話題となった情報漏洩事件によってその戦術に注目が集まり、脅威活動も進化しています。

そして、Webブラウザが重要なターゲットになりました。ファイアウォール、セキュアWebゲートウェイ（SWG）、サンドボックス分析、URLレピュテーションチェックなどの現在のセキュリティ対策では、ブラウザを狙った攻撃を阻止することはできません。HTMLスマグリング、AiTM、暗号化ファイルなどの新しい回避的な手法が、急速に認証情報窃取の主要な手段になりつつあります。問題をさらに複雑にしているのは、フィッシングが従来のメールやO365の経路を超えて拡大していることです。攻撃者は、クラウド共有プラットフォームやWebベースのアプリケーションを狙ったフィッシング攻撃を集中的に行っており、組織への新たな侵入経路が生まれています。

最近、Menlo Labsの脅威調査チームは、「indeed.com」でのEvilProxyフィッシングキャンペーンを摘発しました。このキャンペーンは、上級管理職の幹部を積極的にターゲットにし、認証情報の窃取やアカウント侵害の危険にさらしていました。これらの乗っ取られた被害者のセッションクッキーは、正規のMicrosoft Onlineサイトにログインし、被害者になりすまし、フィッシング耐性のないMFAを回避するために使用されました。

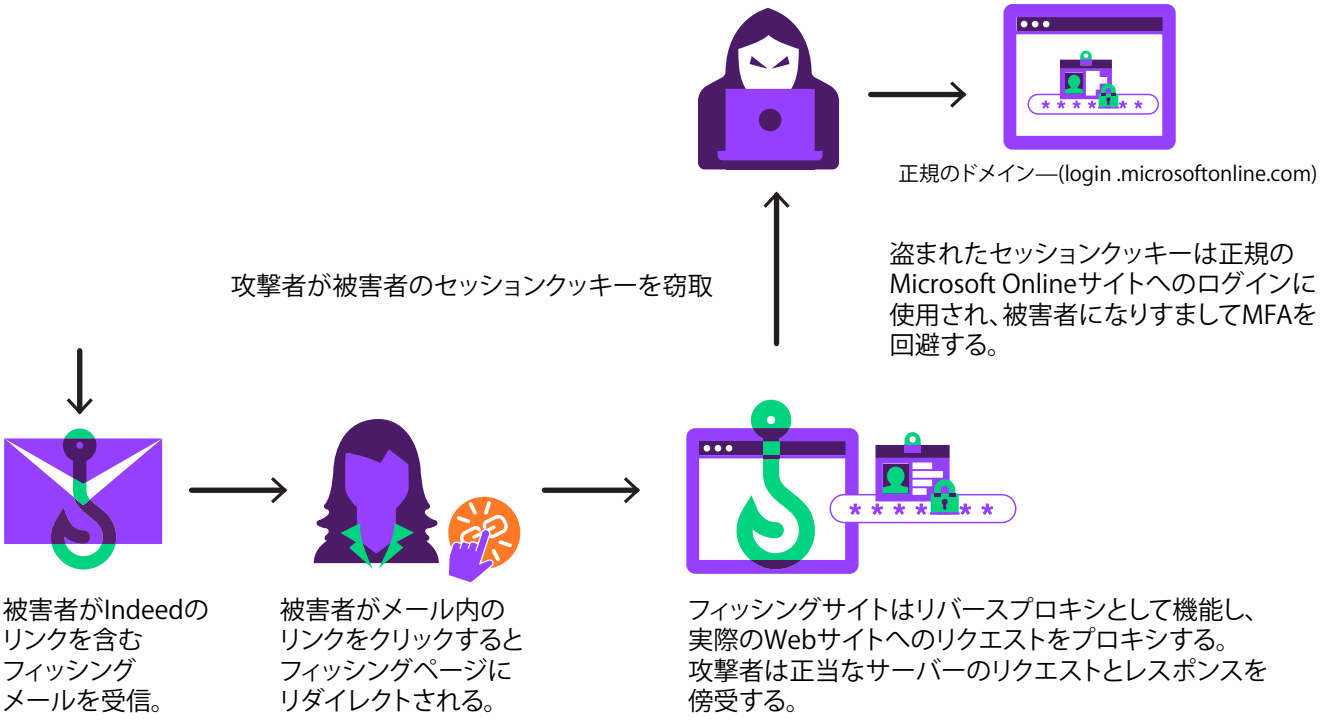

図2：MFA回避攻撃の流れ

攻撃者は、ブラウザを標的とした高品質で大規模な攻撃を仕掛けるためのツールを開発しました。フィッシュキット（PhaaS）やRansomware-as-a-Serviceキット（RaaS）などのサイバー犯罪ツールにより、高度な攻撃を仕掛けるプロセスが簡素化されました。これらのキットは、あらかじめ用意されたテンプレート、スクリプト、およびリソースを攻撃者に提供し、悪意のあるキャンペーンを作成および展開するためのハードルを下げています。また、このようなツールを利用することで、経験の浅い攻撃者でも、狙った被害者から機密情報を盗むために、巧妙な詐欺的Webサイトやメールを簡単に作成できるようになります。

Menlo Labsの脅威調査チームは、**今日のフィッシング攻撃の30%が「回避的」な特徴を示している**ことを観測しました。これらの攻撃の目的は、ランサムウェアの配信と認証情報窃取の2つでした。

Menlo Labsの脅威調査チームは、組織に新たに重大なリスクをもたらすサイバー犯罪キャンペーンを検出しました。この攻撃の多くは、従来型のツールを回避します：

今年、**ブラウザベースのフィッシング攻撃が55万件**
以上検出されました。

これは、2023年の最後の6ヶ月間でほぼ
200%増加したことになります。

レガシーURLレピュテーション回避（LURE）攻撃の
増加が顕著です。Menlo Labsの脅威調査チームは、
2023年のLURE攻撃が2022年と比較して70%増加したこと
を観測しました。

100万件以上のURLを分析した結果、Menlo Labsの
脅威調査チームは**LURE攻撃の73%以上がカテゴリ分け済みの
Webサイトから発信されている**と結論付けました。

レガシーURLレピュテーション回避（LURE）は、最近増えている回避的なフィッシング手法で、特にブラウザを狙い、セキュアWebゲートウェイやURLレピュテーションフィルタのような一般的に導入されているセキュリティツールのWebカテゴリ分けを回避します。攻撃者は信頼できるサイトを乗っ取ったり、新しいサイトを作成してURL/ドメインが信頼されるまで休止状態にしたりすることでフィルタリングを回避します。その後、これらのURLと宛先サイトを使用してフィッシング攻撃を開始します。これは2023年を通して一貫した傾向でした：AWSフィッシングサイトを悪意のあるGoogle広告キャンペーンに忍び込ませるフィッシング攻撃

このような攻撃を受けると、ユーザーはURLを本物だと信じて開いてしまいます。そのURLは安全なカテゴリに分類されているため、SWGやURLフィルタによってブロックされることはありません。その後、ユーザーはマルウェアに感染したり、認証情報を入力させられたりして、侵害されます。

企業のセキュリティに関する課題は、セキュリティツールが依然として従来のネットワークシグナルと従来型のエンドポイントテレメトリのみに依存していることに起因しています。これらのアプローチでは、LUREのような回避的な脅威を特定することはできません。ファイアウォールやSWGはブラウザテレメトリを可視化できず、ネットワークベースのテレメトリでトレーニングされたAIモデルでさえも不十分です。この弱点がこの攻撃ベクトルの拡大に拍車をかけています。ブラウザ固有のテレメトリに対する可視性を改善しない場合、セキュリティチームはゼロアワーフィッシング攻撃にさらされ続けます。企業リーダーは、ネットワーク、エンドポイント、システムのセキュリティに対するアプローチを再評価する必要があります。また、ユーザーがこれらの新しい脅威ベクトルにさらされているかどうか、また脅威を初期段階で特定して防止できるかどうかも考慮する必要があります。

洞察 3：

従来型のツールではブラウザベースの攻撃を見逃してしまいます

従来型のネットワークおよびエンドポイントセキュリティツールを使う限り、企業はゼロアワーフィッシングの脅威にさらされ続けます。これらの攻撃は、一般的に導入されているセキュリティツールを回避するように特別に設計されており、ランサムウェアやデータ流出、サイバースパイ活動の主な手段として機能します。同様に、従来型のツールでは、ブラウザの脆弱性、パッチが適用されていないブラウザ拡張機能、ドライブバイダウンロードなどを防ぐことはできません。

30日間にわたる徹底的なデータ精査により、Menlo Labsの脅威調査チームは、次のことを発見しました：

- 署名やデジタルパンくずが表示されない11,000件以上のゼロアワーフィッシング攻撃について、既存のSWGやエンドポイントツールではこれらの攻撃を検知してブロックすることができませんでした。
- ゼロアワーフィッシング攻撃が最初に発見されてから、従来型のセキュリティツールがそれを検知できるようになるまでに、平均で6日間かかります。

「保護バッファ」：ゼロアワーフィッシングへの対抗

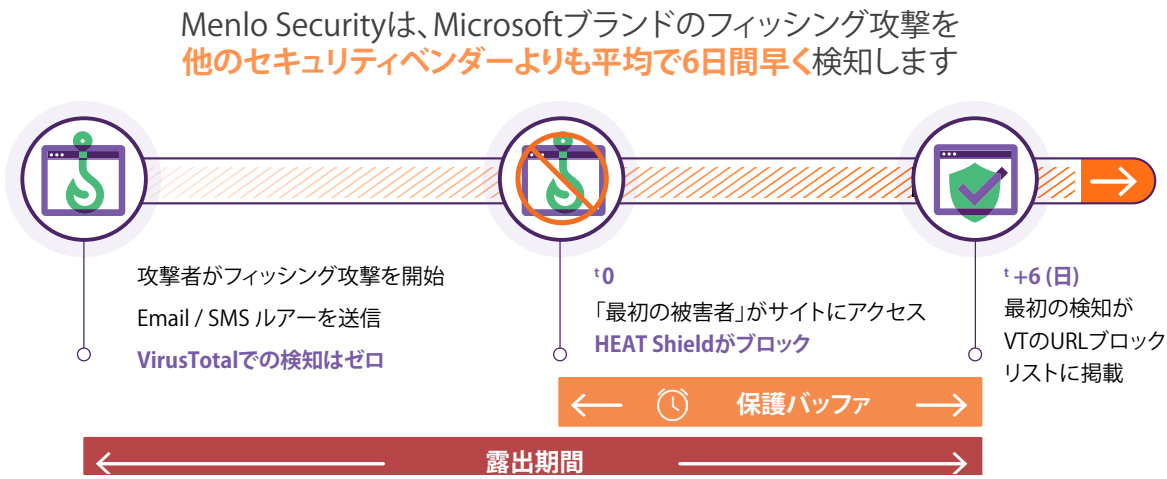

図3:ゼロアワーフィッシング攻撃に対するMenlo Securityの保護バッファ

Webやメール、エンドポイントのセキュリティは、部分的な保護は提供しますが、ブラウザは依然として重大な脅威にさらされたままです。また、エンドユーザーへの適切な教育を最善の努力で実施しているにも関わらず、巧妙なフィッシング攻撃は絶えず進化しており、ブラウザ内での悪意のある動作を無害な動作に偽装することで、今もなお侵入を許しています。これが、フィッシングが強力な脅威である理由です。

検知を回避するために、多くの標的型攻撃は以下のような回避的な手法を組み合わせて行われます：

- 中間者攻撃(AiTM)
- オープンリダイレクトチェーン
- QRコード
- クラウド開発プラットフォーム上でのフィッシングサイトのホスティング
- コンテンツ配信ネットワーク（CDN）上での悪意のあるペイロードのホスト

これらの手法に対抗するためには、ブラウザのセキュリティを強化する必要があり、ネットワークシグナルや静的HTTPSペイロードを越えた検査でのみ検知することができます。これらの攻撃を検知して阻止するためには、Webセッション、ドキュメントオブジェクトモデル（DOM）、HTML、埋め込みメディアオブジェクト（画像など）、JavaScript、CSSから生成される動的要素をリアルタイムに検査する必要があります。

ブラウザセキュリティに注意を払うことで、既存のネットワークセキュリティとエンドポイント技術が補完され、これらの新しい攻撃によって生じるリスクのギャップが解消されます。

結論

Menlo Securityこそが、お客様に必要なブラウザセキュリティです

ブラウザは企業にとってなくてはならないビジネスアプリケーションですが、セキュリティや管理性の面では遅れています。Menlo Securityは、包括的なブラウザセキュリティアプローチを提供するために、ITおよびセキュリティチームが既存のブラウザを適切に管理し、ユーザーを保護し、アプリケーションアクセスと企業データを保護して、ブラウザの攻撃対象を排除します。Menlo Securityのブラウザセキュリティソリューションは、他のどのセキュリティベンダーよりも6日間早く、フィッシング攻撃を正確に識別し、ブロックすることができます。この「保護バッファ」により、ユーザーが悪意のあるサイトに初めてアクセスしてから、VT上の1つまたは複数のベンダーが悪意のあるサイトとしてフラグを立てるまでの時間が大幅に短縮されます。

Menlo Securityのブラウザセキュリティソリューションは、あらゆるデバイス、あらゆるブラウジングで動作し、すべてのブラウザセッションをエンドツーエンドで可視化し、リアルタイムの動的ポリシー制御を提供することで、回避型のマルウェアやゼロアワーフィッシング攻撃がユーザーシステムや企業ネットワークに感染するのを効果的に阻止します。Menlo SecurityのAIを活用したセキュアクラウドブラウザを使用すると、既知のブランドやサービスになりすました、見た目が類似したWebサイトを識別し、あらゆるブラウザでシームレスなユーザーエクスペリエンスを確保しながら、速度と正確さの両方を確保できます。

フィッシングについて、またブラウザセキュリティがどのようにブラウザの攻撃対象をなくすことができるかについて、詳しくはmenlosecurity.comをご覧いただくか、japan@menlosecurity.comまでメールでお問い合わせください。

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

Menlo Securityについて

Menlo Securityは、Menlo Secure Cloud Browserによって高度に回避的な脅威を排除し、生産性を維持します。Menlo Securityは、クラウドベースのセキュリティが目指す、導入展開が容易なゼロトラストアクセスを実現します。Menlo Secure Cloud Browserは、エンドユーザーがオンラインで業務を行う間、ユーザーからは見えない形でサイバー攻撃から防御し、同時にセキュリティチームの運用負担を軽減します。

Menlo Securityは、ユーザーを保護してアプリケーションへのアクセスを確保し、完全なエンタープライズブラウザソリューションを提供します。Menlo Securityなら、ワンクリックでブラウザセキュリティポリシーを導入することができ、SaaSやプライベートアプリケーションへのアクセスを保護して、ラストワンマイルまで企業データを守ります。信頼と実績のあるサイバー防御により、あらゆるブラウザでデジタルトランスフォーメーションを保護します。Menlo Securityと共に、安心してビジネスを前進させましょう。