MENLO SECURITY

ブラウザセキュリティの現状:

AIの力で進化する フィッシングおよびランサムウェア配信

REPORT

目次

ブラウザセキュリティの現状:

AIの力で進化するフィッシングおよびランサムウェア配信

本レポートでは、ブラウザセキュリティを取り巻く脅威の現状を調査し、世界中の組織やユーザーに影響を及ぼしている最新の攻撃ベクトル、脆弱性およびトレンドについて評価します。サイバー犯罪者が侵入の足掛かりを得るためにブラウザを侵害するケースが増えており、企業はこうした新たなリスクに対処する必要に迫られています。高度なフィッシングやゼロデイエクスプロイト、ブラウザベースのチャネルを介したデータ流出が増加しており、新たな脅威として不正な生成AIサイトも急増しています。本レポートでは、ブラウザベースの攻撃の進化を分析し、ブラウザアイソレーションやAIを活用した脅威検知などの保護テクノロジーを検証します。この調査は、ブラウザセキュリティによりゼロトラストアクセスを可能にし、生成AIの利用を管理して防御を強化するための実用的な洞察を提供します。Menlo Securityの目的は、セキュリティの専門家にブラウザが直面している最新の脅威についての理解を深めて頂くこと、そしてそれらに対する回復力のある防御を構築するために必要なツールを提供することです。

ブラウザセキュリティの現状:
AIの力で進化する フィッシングおよびランサムウェア配信

マクロ環境: 進化する脅威ランドスケープ

AIを活用した攻撃、Phising-as-a-Service（PhaaS）、ゼロデイ攻撃など、エンタープライズブラウザを狙う攻撃が増加しており、ブラウザセキュリティに対する新たなアプローチの必要性が改めて注目されています。最新の脅威は従来型の防御をすり抜けるため、従来型のネットワークおよびエンドポイントのセキュリティツールだけでは、もはや十分とは言えません。クラウドブラウジングを安全に行えるようにすることは、最新の業務環境で活動する企業にとって極めて重要です。安全なクラウドブラウジングとは、ユーザーのブラウジング活動をネットワークから物理的に分離（アイソレーション）し、ユーザーエクスペリエンスを変えることなく、ブラウザベースの脅威から保護することです。

過去12ヶ月間で、Menlo Threat Intelligenceは800社を越える企業において、ブラウザベースのフィッシング攻撃を752,000件以上確認しました。生成AIによって生み出された脅威が急増しており、偽のWebサイトが正規の生成AIプラットフォームを装ってユーザーを欺いています。Menlo Securityは過去1年間で、偽のフィッシングサイトが生成AIの名の元に無防備な被害者を騙して悪用や侵害を行おうとするインシデントを数百件阻止しました。ユーザーの行動が変化したことで、ブラウザはビジネスや個人の活動の中心として定着しましたが、同時にサイバー犯罪者や国家が支援する攻撃者の注目を集めることにもなりました。

現代において、ブラウザは単なるWebブラウジングや企業アプリケーションへのアクセスツールではありません。高度なサイバー攻撃においては最初のアクセスポイントとなっており、攻撃者は脆弱性を悪用して従来型のセキュリティ制御を掻い潜り、機密データを盗みます。

巨額のセキュリティ投資にもかかわらず、ブラウザベースの脅威は減っていない

高度な攻撃者は、もはや単純なエクスプロイトには頼りません。その代わりにゼロデイ攻撃やソーシャルエンジニアリング、高度なフィッシングテクニックなどを組み合わせ、システムに侵入して貴重なデータを盗みます。ガートナーによると、攻撃の98%以上はインターネット由来であり、そのうち80%はエンドユーザーのローカルブラウザを標的にしています。よく見られる攻撃ベクトルは以下の通りです：

- 悪意のある広告：マルバタイジングキャンペーンは、人気のWebサイトや広告ネットワークを悪用し、マルウェアを配布して認証情報を盗みます。
- ブラウザベースのフィッシング：ブラウザベースのフィッシング攻撃（特に、回避的なフィッシングテクニックや、SlackやTeamsなどのビジネスコラボレーションツールを利用したもの）は、より説得力が増し、検知するのが難しくなっています。ブランドのなりすましは、サイトの正当性についてユーザーを欺くフィッシング攻撃で急速に利用されるようになっています。

- ブラウザ脆弱性のエクスプロイト：Chrome、Firefox、Edgeなどの主要なブラウザのゼロデイ脆弱性を悪用することは、依然として深刻な脅威です。この問題に対処するために代替のHeavyweight Browserが登場しましたが、結果的には最小限の業務環境しか提供できず、むしろブラウザの管理性やセキュアなアプリケーションアクセスの面で新たな課題を生みました。また、アップデートや技術革新においても、主要なブラウザに大きく遅れをとっています。

2024年後半までに、サイバー犯罪者は毎月100万個近くのフィッシングサイトを生成するようになるでしょう：これは、2020年と比べ700%近い増加です

2024年、ブラウザセキュリティは歴史上最も高度なサイバー脅威のいくつかにさらされました。企業がSaaSプラットフォームやクラウドベースのアプリケーション、ハイブリッドな業務環境、BYOD方針などのリモートワーク環境に移行したため、攻撃者はブラウザに注目し、脆弱性を執拗に悪用するために回避的なテクニックを活用するようになりました。2024年には注目を集めるブラウザベースの攻撃が多数発生し、脅威ランドスケープが進化していることが明らかになり、組織がブラウザセキュリティに対して積極的なアプローチを採る必要性が注目されました。これらの脅威には、次のようなものがあります：

***「0.0.0.0 Day」脆弱性：OligoSecurityのチーム**が2024年の「0.0.0.0 Day: Exploiting Localhost APIs From the Browser」について解説しています。研究者らは、主要なブラウザのすべてに最新の脆弱性があることを明らかにしました。この脆弱性により、外部のWebサイトがMacOSおよびLinux上でローカルに実行されているソフトウェアと通信し、そのソフトウェアを悪用する可能性があります。この「0.0.0.0 Day」脆弱性は、ブラウザがネットワークリクエストを処理する方法における根本的な欠陥を狙ったものであり、攻撃者に機密サービスへのアクセスを許可してしまう可能性がありるという、ローカルのエンドポイントブラウザのリスクを浮き彫りにしました。*

***2024年には、ChromeブラウザとEdgeブラウザに影響を与えるゼロデイ脆弱性が顕著に増加しました。**これは、パッチが適用されていないシステムを狙う攻撃者の巧妙さが増していることを示すものです。Chromeでは、リモートでのコード実行を可能にするCVE-2024-7971を含む、深刻度の高い複数の脆弱性が見つかりました。この脆弱性により、攻撃者はセキュリティパッチが適用される前に企業ネットワークや機密データにアクセスすることが可能になります。影響を受けた組織では、ダウンタイム、データ侵害、高コストな復旧作業が発生しています。*

***Google DrawingsとWhatsAppの短縮URLフィッシング攻撃：**2024年に起きたもう一つの注目すべき攻撃は、Google DrawingsとWhatsAppのURLリダイレクトを使った攻撃です。これは、Google Drawingsでホストされている偽装したAmazonアカウント確認リンクを使用して、ユーザーを欺いてログインのための認証情報を共有させるものです。この攻撃が特に狡猾なのは、ログイン用の認証情報を収集するために、確立されたサービスに対するブラウザの本質的な信頼につけ込んでいることです。このフィッシング攻撃は、Google独自のツールの一部であるかのように見せかけており、ユーザーが正規のページと詐欺的なページを区別することを困難にしていました。*

***2024年にCloudflareドメインのフィッシング悪用が104%増加：**FortraのSEAチームによって、Cloudflare Workersプラットフォームがフィッシングに悪用されたインシデントが5,000件弱検出されました。これは104%の増加で、1か月あたり500件を超える攻撃が発生しています。Fortraは、Cloudflareのpages.devおよびworkers.devドメインがフィッシング攻撃に悪用されるケースが増加していると警告しています。これらのプラットフォームは無償でホスティングを提供しており、正規の外観を持ち、セキュリティフィルタを回避できるため、サイバー犯罪者にとっては魅力的です。攻撃者はこれらのドメイン上でフィッシングページやマルウェアをホストし、多くの場合ユーザーを偽のログインページにリダイレクトします。*

認証情報フィッシングが企業を脅かし続ける理由

2024年も企業を標的とした認証情報フィッシングが蔓延しましたが、その主な理由は、ファイアウォールやセキュアWebゲートウェイ、ウイルス対策ツールなどの従来型のセキュリティ対策が、サイバー犯罪者が使用する認証情報フィッシングやその他の高度な手法に対して効果が無くなっていることです。多くの企業がブラウザのセキュリティ向上に努めていますが、ネットワークやエンドポイントレベルのセキュリティに重点を置く傾向があり、回避的な脅威に対抗する準備が整っていません。

クラウドネットワークサービスはこの問題に対処しようとしていますが、高度なフィッシング攻撃に対する効果的な保護は提供できておらず、むしろ複雑さが増し、管理コストが高くなることも珍しくありません。さらに、従来型のRemote Browser Isolation（RBI）のようなチェックボックスソリューションは、LURE攻撃のような回避的なブラウザベースのフィッシング攻撃に対してはほとんど効果がないことが判明しています。
LURE（Legacy URL Reputation Evasion：レガシーURLレピュテーション回避）攻撃は、暗黙の信頼に基づいてドメインをカテゴリー分けしようとするWebフィルターを回避します。そうしてセキュリティが不十分なWebサイトを侵害し、エンドポイントに侵入してマルウェアを送り込み、組織内を横方向に移動してより深く侵入します。またサイバー犯罪者は従来型のセキュリティ層を回避するためにAIを活用し、セキュリティが不十分なWebサイトへの侵入、偽造サイトの作成、既存のツールでは検知できないファイルにマルウェアを埋め込むなど、活動の規模を拡大しています。その結果、検知や防止メカニズムを回避し続けることが可能となるため、企業は引き続き認証情報フィッシングに対して脆弱なままとなるのです。

従来型のセキュリティツールがゼロデイ攻撃による脅威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

初期アクセスを獲得するための回避テクニックが急増

Menlo Threat Intelligenceによると、2024年のブラウザセキュリティの状況は、企業に対するゼロアワーフィッシング攻撃が130%増という驚くべき値を示し、新しい戦術が定期的に出現するという結果になりました。これらの回避テクニックは、ブラウザを通じて初期アクセスを獲得するために使用されるため、サイバーセキュリティ上の重大な懸念事項となっています。サイバー攻撃者は、ブラウザの脆弱性を悪用し、悪意のあるコードを難読化し、ファイルレスマルウェアやメモリオンリーのペイロードなどの回避戦術を駆使して、従来型の防御を回避しようとする傾向が強まっています。これらのテクニックでは、一見正当なWebトラフィックの中に悪意のある活動を隠すことが多く、それが検知を困難にしています。企業がより強固なエンドポイントセキュリティ対策を採用する中、攻撃者はブラウザベースのエクスプロイトに重点を移しつつあります。ブラウザベースのエクスプロイトでは、巧妙で回避的なアプローチによって従来型のセキュリティツールを回避し、さらなる侵害の足がかりを作ることができます。

2024年第4四半期の時点で、ゼロアワーフィッシング攻撃の標的となった上位5か国は、米国、台湾、日本、シンガポール、韓国でした。

フィッシング攻撃におけるブランドなりすましロゴの急増

ブラウザを標的としたフィッシング攻撃でなりすましロゴを使用することは、企業ネットワークへの初期アクセスを獲得するための一般的な戦術となっています。サイバー犯罪者はブランドロゴを利用して、正規のビジネスポータルやサービスを模倣した説得力のある偽のWebサイトを作成し、従業員を騙して重要な認証情報を収集したり、悪意のあるペイロードをダウンロードさせたりします。

Menlo Threat Intelligenceによると、ブラウザベースのフィッシング攻撃の約51%は、利用するユーザーに信頼できる組織とやりとりしているように思わせるために、何らかの形でブランド名を偽装しており、その筆頭はMicrosoftです。この手法は、侵害が成功する可能性を著しく高めます。なぜならユーザーは、見た目が正規のビジネスに似ているサイトを信用する傾向が高いためです。

Menlo Threat Intelligenceによると、
ブランドのなりすましを伴うフィッシング攻撃は2024年に急増し、
ブラウザベースのフィッシング攻撃で最もなりすましが多かったブランドは
Microsoft、Facebook、Netflixでした。

Menlo Security Threat Intelligenceからの洞察

これまで見てきたインシデントから、ブラウザがサイバー犯罪者にとって絶好の標的になったことは明らかです。Menlo Threat Intelligenceは、従来型のセキュリティ制御（特にブラウザベースの脅威）を回避しようとするサイバー犯罪フィッシングキャンペーンを多数検出しました。

過去に広く使用されていた「スプレイ＆プレイ」の手法とは異なり、これらの攻撃はさらに高度で、ブラウザを通じてユーザーを具体的に標的とする回避的なテクニックを使用しています。これらのキャンペーンの主な目的は、ランサムウェアの配信と認証情報の窃取です。特に、ランサムウェア攻撃は多くの場合フィッシングから始まりますが、それを検知できるようになるまでには5日間、あるいはそれ以上かかる場合があり、従来型のセキュリティシステムが対応する前に、攻撃者は悪意のある活動を行うことができます。Menlo Threat Intelligenceは、これらの脅威が進化しており、その勢いに衰える兆候は見られず、組織に対するリスクが増大しているという憂慮すべき傾向を、過去12か月間にわたって観察してきました。

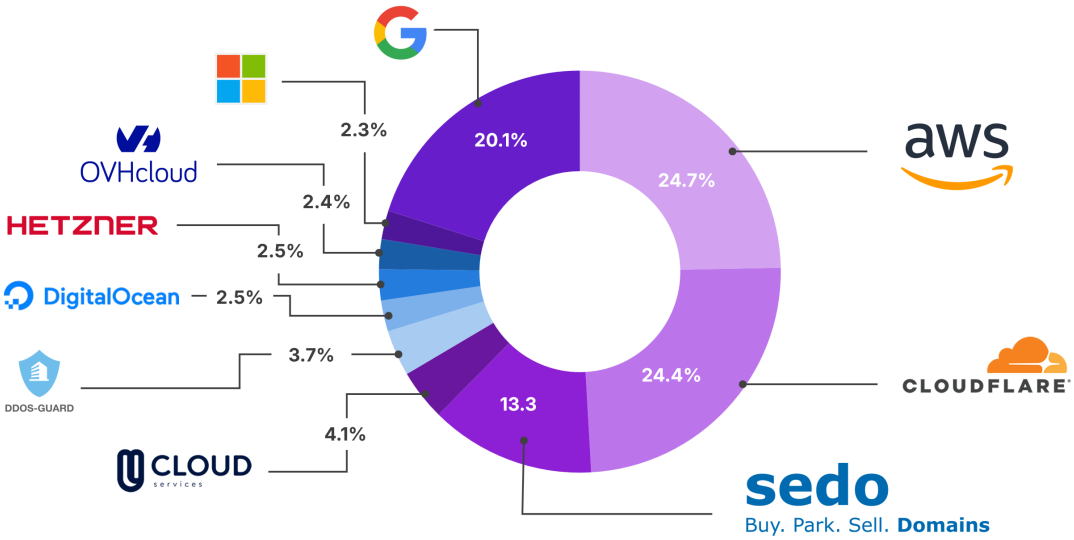
- Menlo Securityは、過去12ヶ月間に752,500件以上のブラウザベースのフィッシング攻撃を検知しました。
- これは、前年同期比で140%の増加です。
- 2024年には、5件の攻撃のうち1件は何らかの回避的な手法を使っていました。これらは、従来型のネットワークおよびエンドポイントベースのセキュリティ制御を回避するように設計されています。
- Menlo Threat Intelligenceは、過去12か月間にMenlo Securityのお客様に対して行われた17万件のゼロアワーフィッシング攻撃を特定しました。これは、2023年から130%の増加です。
- Menlo Securityが特定した、2024年になりすましの被害が最も多かったブランドはFacebook、Microsoft、Netflixでした。
- 生成AIの脅威は昨年から急増しており、生成AIサイトの名前を偽装して、疑いを持たない被害者を操って侵害する事件が600件近く確認されています。

クラウドホスティングサービスの悪用の増加

サイバー犯罪者がクラウドサービスを悪用してフィッシングサイトやランサムウェア、コマンド＆コントロール（C2）インフラストラクチャなどの悪質なコンテンツをホストするケースが急増しています。こうしたクラウドホスティングサービスの悪用の増加は、企業にとって大きな懸念事項となっています。

従来型のホスティングサービスとは異なり、クラウドプロバイダーは違法または有害な行動を監視することが少ないと考えられるため、攻撃者が身を隠しやすくなります。また、こうしたプラットフォームはスケーラビリティが高く迅速に拡張できるため、従来型のセキュリティ対策では脅威を検知して緩和することが難しく、企業にとって特に危険です。さらに、悪用されるクラウドサービスは匿名性と回復力も提供するため、攻撃者は迅速に攻撃や移動を行うことができ、インシデント対応が複雑になり、企業のデータとネットワークの完全性に重大なリスクをもたらします。

悪用されたクラウドホスティングサービスとその割合



Vextrio：進化するマルウェアテクニック

Vextrioキャンペーンは、ブラウザベースの脅威がますます巧妙化していることを浮き彫りにしました。これは、Webインフラストラクチャそのもの（つまり私たちが信頼しがちな広告ネットワーク）を悪用してユーザーに感染し、企業環境への足掛かりを得ます。javascriptコードの難読化技術を使用し、正規に見える広告を統合しているため、従来型のエンドポイントセキュリティソリューションでは、これらの攻撃を検知してブロックすることは困難です。

ポイント

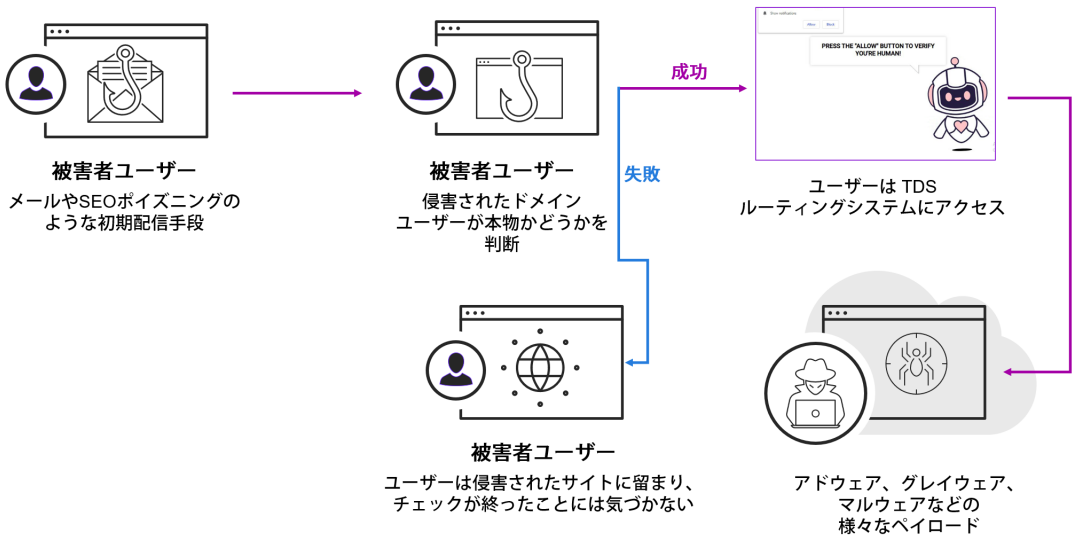
- 悪意のある TDS as-a-service
- マルウェア、バックドア、広告、グレイウェアにつながる可能性がある
- インフラが急速に変化する可能性がある

狙われる主な業種

- 全業種

使用されるテクニック

- TDS
- WordPressサイトの侵害
- ソーシャルエンジニアリング



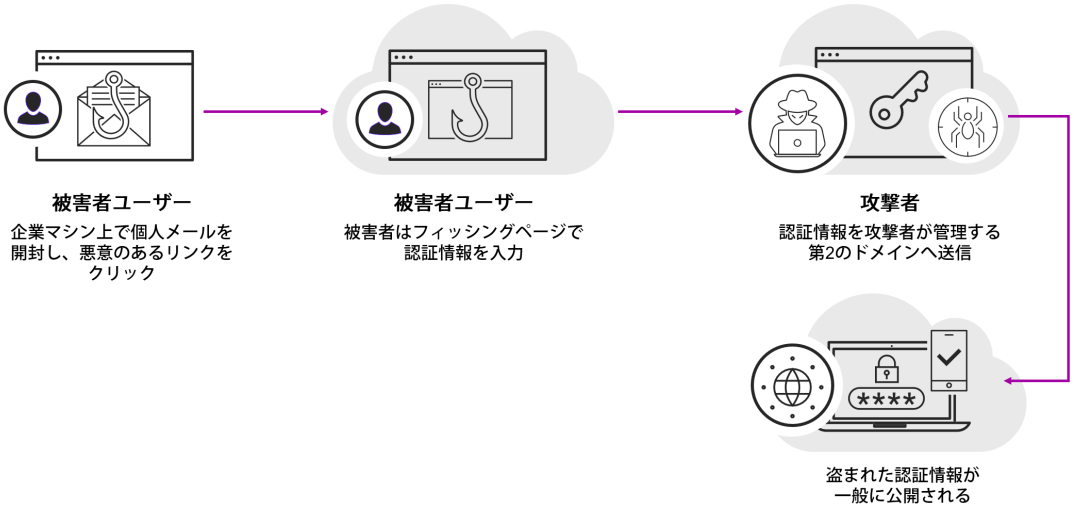
オープンウォーターのフィッシングキャンペーン

2024年に、Menlo Threat IntelligenceはCloudFlareのサービスを利用した別のキャンペーンを特定しました。このキャンペーンでは「Powered by Jehova」というキャッチコピーを持つ出来合いのフィッシングキットが使用されており、Menlo Securityの分析によると、過去3年間にわたって流通していたようです。注目すべき点は、これらのキャンペーンで使用されるC2はオープンディレクトリであるようで、通常C2インフラストラクチャに保存される盗まれた認証情報や、場合によってはキット全体が公開されています。ホスティングサービスの悪用によって攻撃の規模を迅速かつ低コストで拡大できれば、悪意のあるドメインが増え、攻撃者にとって成功率を高めやすい環境が整うため、この状況は特に危険です。Secure Cloud Browserソリューションは、AIによるランタイム分析とリアルタイムのロゴ検知機能によって悪意のあるコンテンツをセキュアなクラウド環境に分離することで、回避的なフィッシングキットから保護します。これによりブランドなりすましの手法を防ぎ、認証情報の窃取やソーシャルエンジニアリング攻撃からユーザーを保護するための動的なセキュリティ制御を提供します。

ポイント
- 攻撃者はベトナムを拠点としている可能性が高い
- 同じインフラストラクチャ上で見つかるオープンディレクトリには、多くの場合盗まれた認証情報が含まれている

狙われる主な業種
- 全業種

使用されるテクニック
- ホスティングサービス
- C2通信
- メールC2通信



Greatness 2FAフィッシングキット

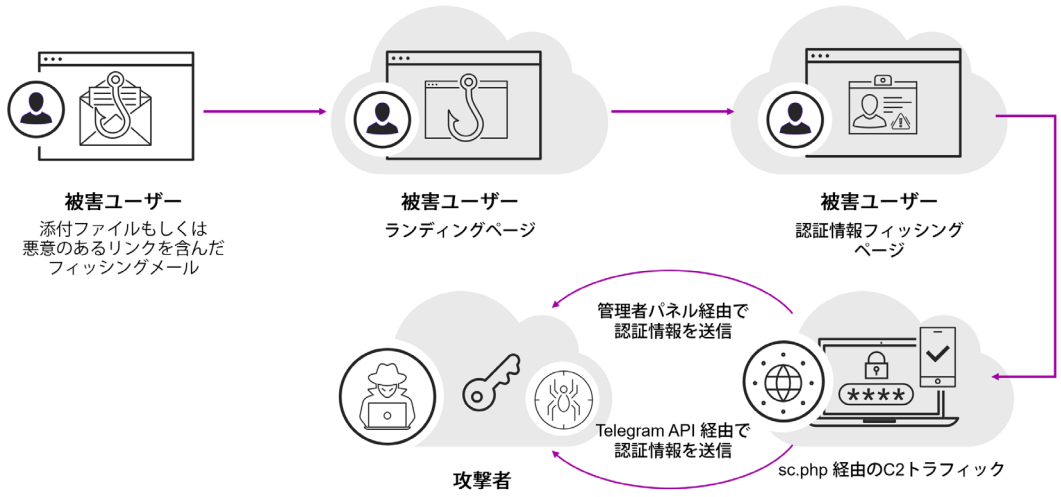
Menlo Threat Intelligenceは、「Greatness」というフィッシングキットを使ったフィッシングキャンペーンを発見して分析しました。このキットはPhishing-as-a-Service（PhaaS）インフラストラクチャの一部であり、Telegram経由で購入することができます。Greatness PhaaSには、メールテンプレート、C2パネルアクセス、キットそのもの、Telegramサポート、その他のTelegramオプションが含まれています。

PhaaSは、フィッシングキャンペーンを実行する機能を、ほぼすべての人に提供します。インフラストラクチャを自前でセットアップする必要がなく、キャンペーンの終了も容易であるため、攻撃者は匿名性のレイヤーを得られます。Secure Cloud Browserにより、企業はセキュリティを堅牢化したローカルブラウザのデジタルツインをクラウドに構築して、悪意を持つかもしれないWebサイトやメールのリンクをエンドポイントから分離します。これにより、ユーザーが2FAの認証情報を盗むように設計されたフィッシングページに直接アクセスすることを防ぎ、安全なリモート環境で実行させます。

ポイント
- 2FAコードの入力を求める
- 堅牢なPhaaSを提供

狙われる主な業種
- 全業種

使用されるテクニック
- アンチボット検知
- Telegram C2
- 管理パネル
- サーバーサイドスクリプトを使用



未来を見据えて：2025年を決定づける変化

2025年に入ると、サイバー犯罪者はより高度で専門的な手法を採用し、より標的を絞った影響の大きい攻撃に重点を置くようになると予想されます。考えられる傾向としては、サイバー犯罪グループの増加や、攻撃チェーンの特定のセグメントに特化した精巧なPhaaSキットの増加があり、より正確で効率的な侵害が可能になります。複数のクラウドプロバイダーへの依存が高まる中、攻撃者はクラウド固有の脆弱性を狙うため、クラウド環境は攻撃者にとってさらに大きな標的となるでしょう。さらに、ダークWebのマーケットプレイスでの自動ハッキングツールが急増し、ブラウザベースのフィッシングキットやRansomware-as-a-Service（RaaS）が蔓延するでしょう。

また、生成AIが作り出す脅威も急増しており、正規の生成AIプラットフォームを装った詐欺サイトがユーザーを騙しています。Menlo Securityはこの1年だけで、これらの偽サイトが生成AIの名前を使用して無防備な被害者を操って侵害するインシデントを600件近く発見しました。AIと大規模言語モデル（LLM）がこれらのサイバー犯罪サービスに統合されることで、攻撃のスケーラビリティと自動化がさらに強化されます。サイバー犯罪者はブラウザベースの高度なフィッシングテクニックと自動化されたソーシャルメディアの偵察を活用して、より効果的なフィッシングキャンペーンを展開できるようになります。

2025年に向けたMenlo Threat Intelligenceの予測トップ5：

1. ランサムウェアは今後も活発に活動し、重要なインフラを標的にして多額の金銭的利益を得る

新しい年には、サイバー犯罪者はブラウザベースの攻撃を利用してランサムウェアを展開し、従来型の防御を回避して医療、エネルギー、輸送などの重要な分野を標的にするケースが増えるでしょう。2019年以降最も一般化した脅威となっているフィッシング攻撃は、今後もその頻度と巧妙さを増し、システムやユーザーデバイスへの侵入に使用され続けるでしょう。企業は、機密情報を盗み、内部システムを侵害し、金銭目的でシステムやブラウザの脆弱性を悪用する多面的な攻撃戦略に直面することになります。2024年のChange Healthcareに対する大規模なフィッシングキャンペーンによるランサムウェア攻撃がもたらした甚大な影響は、組織がブラウザセキュリティを優先し、強力な対策を採用し、最新の脅威インテリジェンスと事業継続プロトコルを常に更新する必要性を浮き彫りにしました。

2. AIによるディープフェイクとユーザーの信頼の悪用は、従来のセキュリティツールを回避し続ける

2025年にはAIを活用したサイバー詐欺が増加し、正規のサイトと悪質なサイトを区別することが難しくなります。AIを活用して信頼できるブランドや個人になりすますディープフェイクは、従来型のセキュリティ対策を回避し、パッチが適用されていない脆弱性を悪用して、標的型フィッシングや認証情報の盗難を助長し、企業がAIを活用した防御策を採用しない限り、広範囲に侵害されるリスクをもたらします。プレミアムなAIサービスを提供すると見せかけた偽のAIツールなどの詐欺行為が、ログイン認証情報や個人情報を盗んだり、ユーザーをフィッシングフォームに誘導したりするために使用されるでしょう。また、巧妙なソーシャルエンジニアリング技術を用いてユーザーの信頼を悪用することが、ソーシャルメディアや検索エンジンを標的とする上での鍵となります。こうした詐欺サイトや偽AIサイトの成功率を高めるためにAIを統合する動きは、すでに企業のデバイス全体に広がりつつあります。

3. 企業間の格差の拡大：大企業がサイバーセキュリティとAIに多額の投資を行う一方で、中小企業は攻撃に対して脆弱であり続ける

今後12か月間は、ランサムウェアやその他のブラウザベースの脅威の影響を受ける中小企業の割合がさらに増加すると予想されます。それは、ユーザーの行動を効果的に監視できず、ブラウザに動的なセキュリティ制御を提供できないためです。大企業はブラウザセキュリティ戦略を取り入れ、セキュリティツールにAIを導入することで、これまでのような煩雑で人為的ミスの余地が大きい防御戦略を補完するでしょう。そして組織はSecurity Operations Center（SOC）を強化するためにAIを活用し始め、SOCの運用にそれほど多くのリソースを必要としなくなります。組織の規模に関係なく、ブラウザセキュリティはもはや任意のオプションではなく、積極的な保護と予防的なセキュリティを伴う必須の生存戦略なのです。CISOは、セキュリティへの取り組みをビジネス目標に合わせるために、使いやすさと強力な保護のバランスが取れたセキュリティ製品を導入し始めるでしょう。

4. エッジデバイスとIoTデバイスに対する脅威の増大

2025年にさらに増加すると思われるもう1つのテーマは、エッジデバイスとInternet of Things（IoT）デバイスがサイバー犯罪者の標的になることです。その理由は、これらのデバイスのセキュリティ対策が限られること、そしてこれらのデバイスが広い範囲で利用されていることです。スマートカメラからウェアラブルデバイス、そしてホームアシスタントまで、こうしたデバイスの導入が進むにつれて、ゼロデイ脆弱性が悪用されるケースが増えると予想されます。攻撃者はこれらの脆弱性を悪用してデバイスを乗っ取り、DDoS攻撃やその他の悪意のある活動に使用する可能性があります。さらに、ヘルスケア（ペースメーカーや血糖値モニターなど）、産業用SCADAシステム、公益事業などの重要分野のデバイスは、サイバー犯罪者が利益や混乱を狙い、スパイ活動のために脆弱性を悪用しようとする際のますます魅力的な標的となるでしょう。このような脅威の増加は、すべてのコネクテッドデバイスにおけるセキュリティ対策の改善が急務であることを浮き彫りにしています。

5. リモート環境とハイブリッド環境によりインサイダー脅威リスクが悪化

最後に、2025年には、内部関係者による脅威は、高度な標的型攻撃の犠牲になる善意のユーザーから発生することがますます増えると予想されます。リモートワークやハイブリッドワーク環境が広く普及すれば、このリスクはさらに悪化するでしょう。この新たな脅威に対抗するために、ユーザーを支援する新しいツールやテクノロジーが登場し、潜在的なリスクを自ら特定して緩和するための負担が軽減されます。これらのツールは悪意のある行動を検知し、人間による手動での分析能力をはるかに超えて機能します。

ブラウザセキュリティはセキュリティチームとエンドユーザーの双方にとって重要な課題であり、それは2025年も変わりません。技術の進歩と業務環境の変化により、サイバー脅威のランドスケープは急速に変化しています。サイバー犯罪者や国家が支援する攻撃者は常に戦術を進化させているため、組織はブラウザの安全性を優先した堅牢なセキュリティ対策を実装し、脅威を検知するための革新的なツールを活用することが、これらのリスクを緩和する上で不可欠となるでしょう。

次世代のリモートブラウザアイソレーションであるSecure Cloud Browserは、主要なローカルブラウザと連携して企業のブラウジングを保護し、クラウドベースのセキュリティを提供してエンドポイントを中心としたアプローチの根本的な欠点を解決します。Secure Cloud Browserは、回避的なフィッシング攻撃、ブラウザの脆弱性、セキュリティを低下させるデバイスのリスクを緩和する一方で、使い慣れたブラウザと生成AIツールを使い続けられるため、ユーザーの生産性を向上させます。AIを活用した脅威防御とSecure Cloud Browserのソリューションにより、企業は常に最新の情報を入手して新たな課題に対応することができ、現実と欺瞞の境界線がますます曖昧になって行く時代において、データをより適切に保護し、信頼を維持することができます。

MENLO SECURITY

メンロ・セキュリティ・ジャパン株式会社

住所：〒100-0004 東京都千代田区大手町 1-6-1 大手町ビル 4F FINOLAB
Webサイト：https://www.menlosecurity.jp
お問い合わせ先：japan@menlosecurity.com