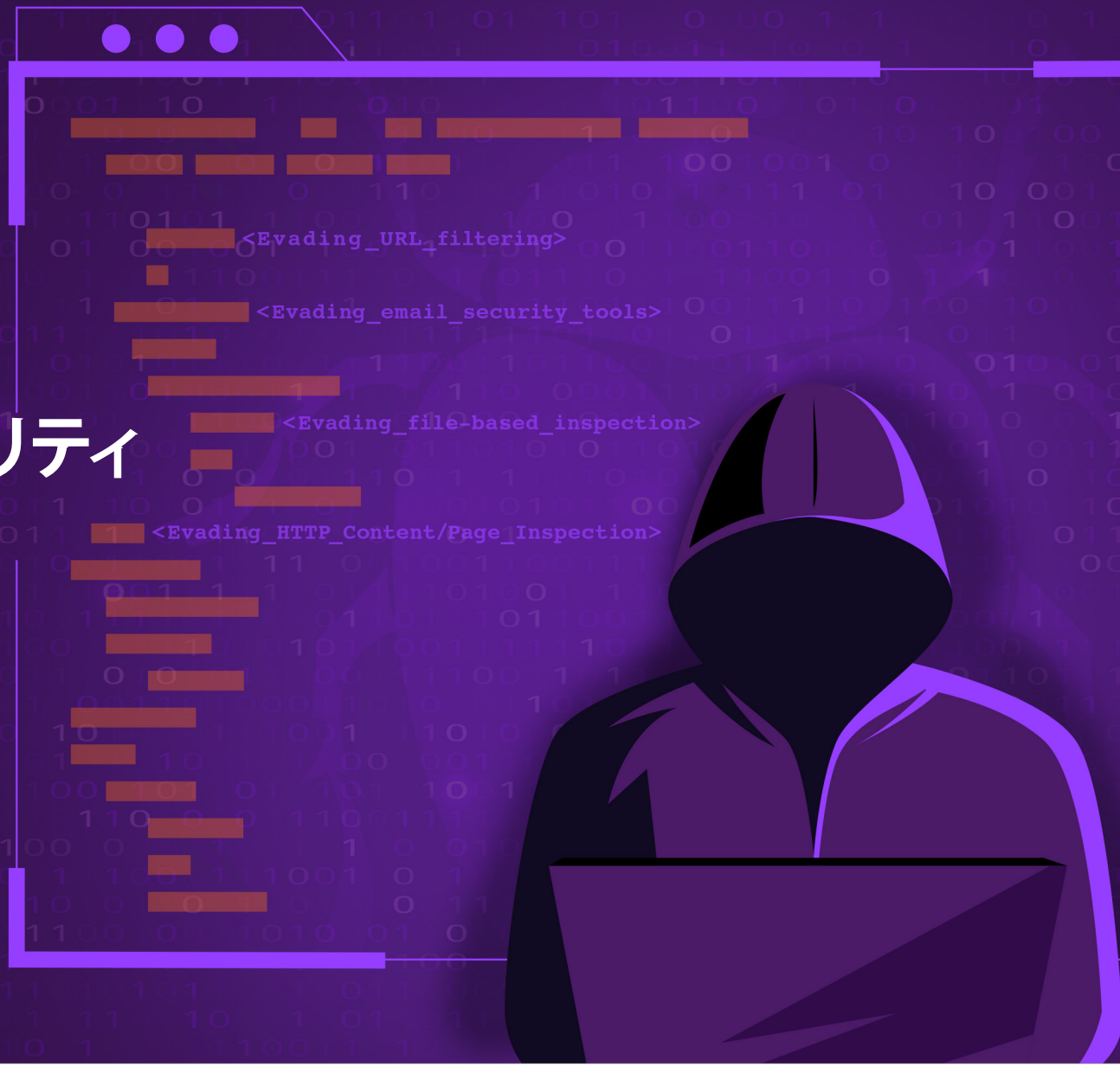
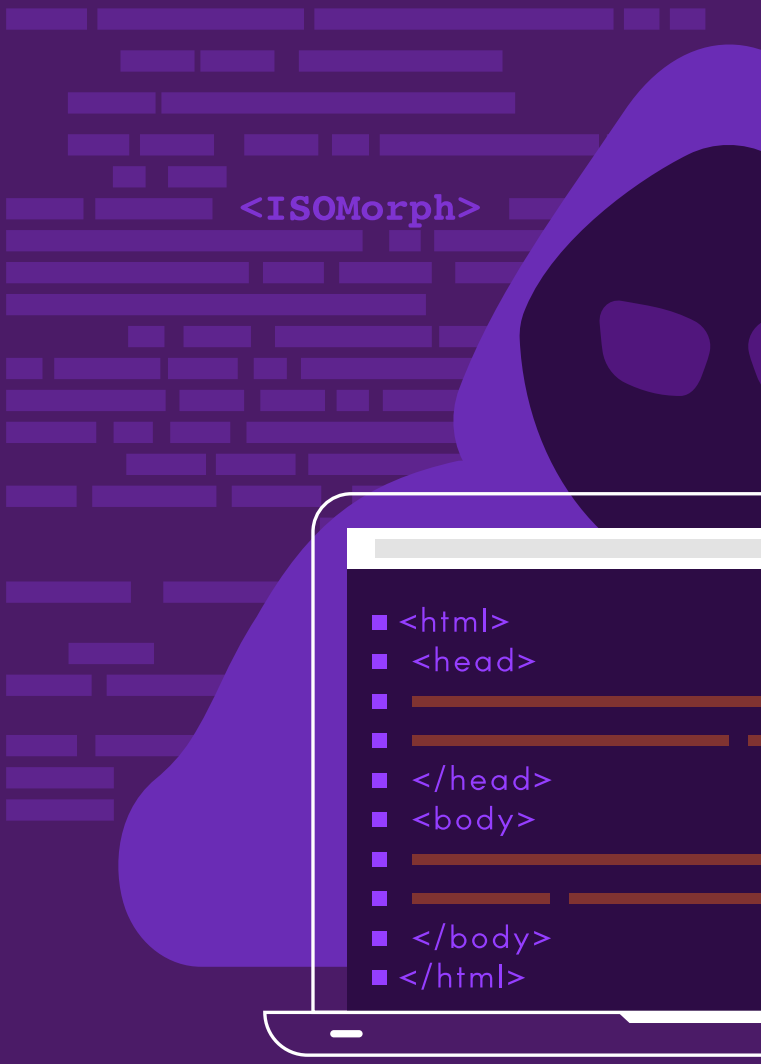
MENLO SECURITY

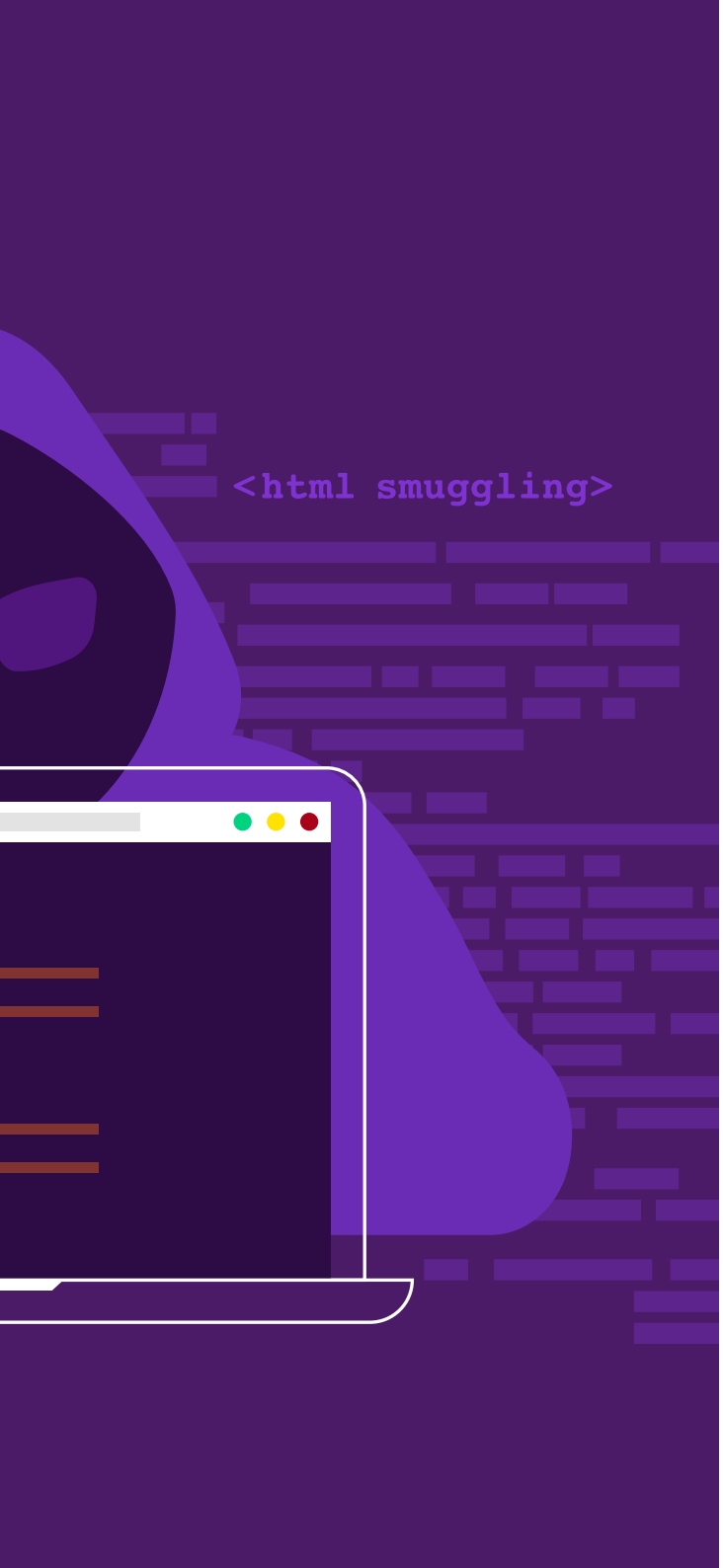
高度に回避的な脅威の仕組み：攻撃者が組織のセキュリティスタックを突破する４つの方法



eBook

目次





時代遅れのセキュリティ技術が **HEAT攻撃を生み出した**

過去数年間で私たちの働き方は大きく変化しましたが、セキュリティは変化しませんでした。現代のナレッジワーカーは、ほとんどの業務をWebブラウザー経由で行っています。ビジネスに不可欠なアプリケーションにアクセスし、コミュニケーションやコラボレーションを行い、ビジネススピードを向上させているのです。これらの生産性を向上させるツールのおかげで、ユーザーはオフィスの枠にとらわれずに業務を行うことができています。しかし現在広く採用されているWebセキュリティ技術は、リモートワークがまだ珍しく、WebブラウザーがWebサイトを閲覧するためだけに使われていた時代に作られたものです。セキュアWebゲートウェイ（SWG）、ファイアウォール、サンドボックスなど、多くの組織が使い続けている検知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は、当初はネットワークとエンドポイントを保護することを意図していましたが、今では最新の業務環境からの要求を満たすことができなくなっています。検知ベースのセキュリティ技術だけに頼っている組織は、これらのツールを簡単にバイパスしてしまう回避的なサイバー攻撃に対し、扉を大きく開いているのです。

ランサムウェアのような脅威を検知するために、従来型のセキュリティツールはネットワーク上のすべてのトラフィックを解析し、それが悪意を持つものであるかどうかを判断します。しかしトラフィックの量が膨大なため、これらのツールが毎回正しい判断を下せるとは限らず、誤検知や検知漏れが避けられません。それを修正するためには、さらなるコストと時間がかかります。侵入を阻止するためには、防御側は常に完璧でなければなりませんが、攻撃側は一度だけ隙を突けば良いのです。脅威が検知されたときには、すでにシステムは侵害されており、ダメージを受けています。

攻撃者はそのことを熟知しており、Webブラウザーを攻撃ベクトルとして使い、検知を回避しようとします。そうすることでネットワークへの初期アクセスや認証情報の窃取、マルウェアの展開が可能になり、それは多くの場合、本格的なランサムウェア攻撃に繋がります。

HEAT（Highly Evasive Adaptive Threats：高度に回避的で適応型の脅威）攻撃は、サイバーセキュリティ業界でもあまり知られておらず、防御策も施されていません。HEATは従来型のセキュリティツールの欠点を突くために特別に考案されたもので、期待通りの機能を持っています。従来型のセキュリティはHEAT攻撃に対抗しようとしていますが、サイバーセキュリティという常に変化する猫とネズミのゲームにおいて、攻撃者が優位に立っていることは明らかです。

このebookでは、**攻撃者がHEATの特徴を活かしてどのように従来のセキュリティツールの検知をすり抜け、**ネットワークを自由に支配するかについて詳しく解説して行きます。

HEAT攻撃は、現在広く使用されている**以下のような従来型のセキュリティ機能および技術を回避します**

攻撃手法 1:
URL フィルタの回避

この手法の**概要**

攻撃者は毎日、大量の悪意のあるドメインを新たに立ち上げています。それを考えると、ユーザーにWebサイトへの自由なアクセスを認めることが災いの元となることはおわかりでしょう。これまでは、この問題を解決するために、ドメインの新しさやレピュテーション、そしてアクセス数などの基準に基づいて、Webサイトを信頼できるものと信頼できないものに分類するというアプローチが取られてきました。しかし攻撃者もこのアプローチについては熟知しており、信頼できると分類されたWebサイトを侵害してそれを利用したり、自ら信頼できるサイトを作成したりして悪意のあるコンテンツの配信に活用することで、このアプローチを**容易に回避**してしまいます。

動作の仕組み

攻撃者は、以下のような手法でURLフィルタ技術を回避します：

悪意のないWebサイトを侵害

攻撃者がURLフィルタ技術を回避する方法の1つは、Webカテゴライズエンジンによってすでに信頼できるものとして分類されていて、かつセキュリティの弱いWebサイトを侵害することです。信頼できるサイトを乗っ取れば、**あとはスイッチを押すだけ**でマルウェアの配布やユーザーのログイン認証情報の窃取を開始することができます。攻撃者は、悪意のあるコンテンツを配置してすぐに削除することが多いため、攻撃の発見は困難です。

CAPTCHAの背後に悪意のあるコンテンツを隠す

正規のWebサイトの多くは、APIボットから身を守り、サイトを訪問しているのが人間かどうかを確認するためにCAPTCHAを使っています。しかしこれはCAPTCHAに対応できないWebカテゴライズのクローラーもブロックすることになり、**本質的には攻撃者が検査を逃れて悪意のあるコンテンツをその背後に隠すことができる壁を作る**ことになります。ユーザーはCAPTCHAを使ったサイトを安全だと思うかもしれませんが、必ずしもそうとは限らないのです。

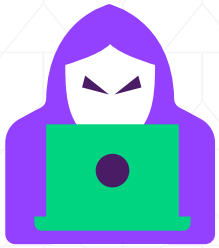
一時的な悪意のあるサイトの構築

信頼できるWebサイトを乗っ取る代わりに、**攻撃者は自らドメインを登録**し、そのレピュテーションを高めることで信頼できるサイトに分類させるということをします。さらに、信頼できるサイトのリポジトリを構築し、後に悪意のあるキャンペーンに使用することも可能です。攻撃が終了すると攻撃者はサイトを元の信頼できる状態に戻し、後で別の攻撃で使用します。

URLフィルタリング技術を回避するその他のHEAT手法：

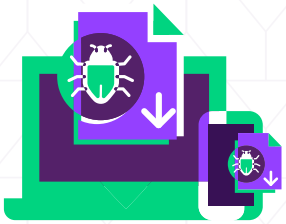
- ブラウザーのゼロデイエクスプロイト
- リバーストンネルおよび短縮URLツール
- 悪意のない一般のコラボレーション/公開/共有サイトでホストされている悪意のある/武器化されたファイル
- 窃取した認証情報の送信/ポストのために動的に生成されるクレデンシャルハーベスティングのURL

実際の攻撃



01. 攻撃者が、信頼できると分類されているWebサイトを乗っ取るか、自ら構築します。

02. 信頼できるサイトが悪意のあるコードで不正に侵害されます。SEO対策を行って侵害されたサイトのページランクを上げ、ユーザーが検索エンジンでこれらのサイトを見つけ、アクセスしやすくすることもあります。



03. ユーザーが一見無害なサイトにアクセスすると、マルウェアをダウンロードさせられたり、ログイン情報を盗まれたりします。

どのような技術を回避するのか：

- Web カテゴライズ技術
- URL レピュテーションエンジン
- 従来型の SWG

攻撃手法 2:
メールセキュリティツールの回避

この手法の概要

ユーザーが悪意のあるリンクをクリックしなければフィッシングの被害に遭うことはありませんし、悪意のあるリンクが受信トレイに届くのを阻止すれば、それをクリックしてしまうこともありません。これが、SEG（セキュア Email ゲートウェイ）などのメールセキュリティツールが**悪意のあるリンクを解析する技術**を採用する元になったロジックです。しかし攻撃者がその戦術を進化させ、メール以外のフィッシング攻撃によってユーザーを狙うようになった今では、このロジックは破綻していると言わざるを得ません。

動作の仕組み

攻撃者は、以下のような手法でメールセキュリティツールを回避します：

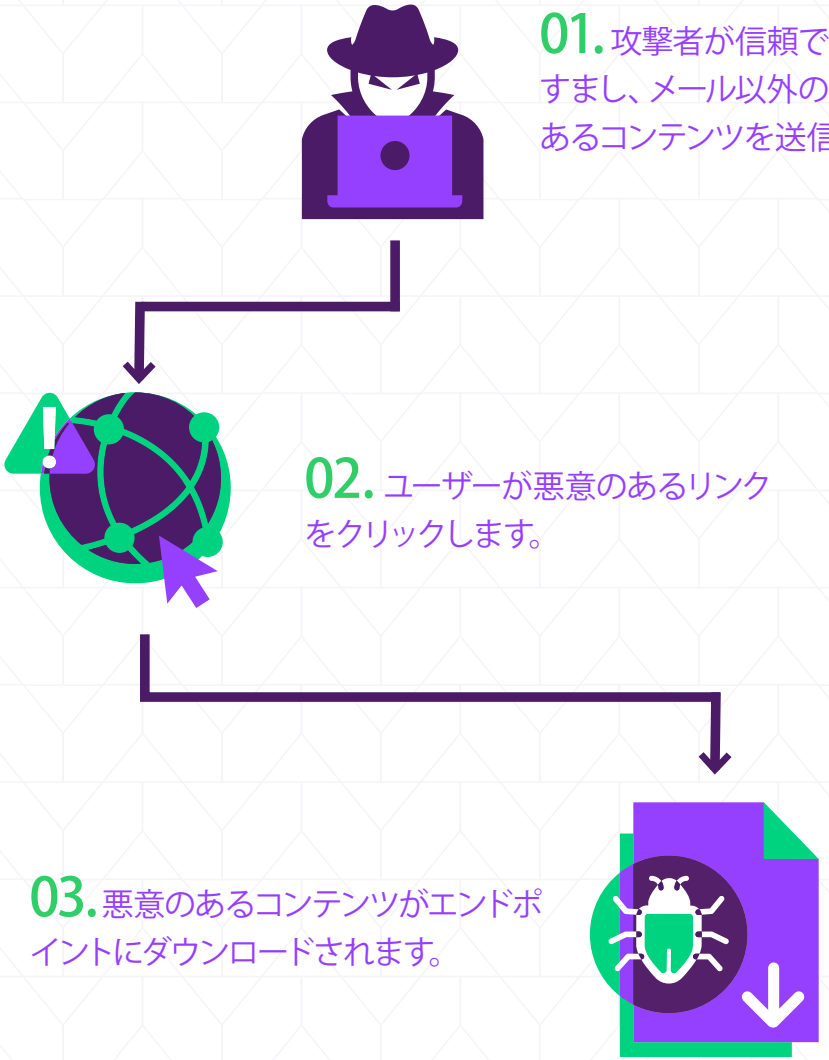
コラボレーションプラットフォーム経由で配信される攻撃

私たちは、フィッシング攻撃は受信トレイに届くことを想定しているため、不審なメールに疑いを持ちます。しかし、**SMSのようなテキストメッセージやソーシャルメディア、あるいはSlackのようなコラボレーションプラットフォームでは、フィッシング攻撃を想定していません。**攻撃者は、このような無意識の信頼を利用して、連絡先の誰かになりすましたり、連絡先のアカウントを侵害したりして、悪意のあるコンテンツを送信します。

悪意のあるOfficeドキュメントや悪意のあるリンクを含むPDFなど

SEGは、メール本文のリンクのみを解析します。ドキュメントやPDFの中にあるリンクは解析の対象外なので、そこに悪意のあるリンクが隠されていたとしても、見つけることはできません。**ユーザーはOfficeドキュメントやPDFを信頼しているため、それらをクリックしてマルウェアやランサムウェアを意図せずダウンロードしてしまう可能性が高くなります。**

実際の**攻撃**



01. 攻撃者が信頼できる連絡先になりすまし、メール以外のチャネルで悪意のあるコンテンツを送信します。

02. ユーザーが悪意のあるリンクをクリックします。

03. 悪意のあるコンテンツがエンドポイントにダウンロードされます。

どのような技術を回避するのか：

- セキュア Email ゲートウェイ（SEG）
- 悪意のあるメールリンクの解析エンジン

攻撃手法 3:
ファイルベース検査の回避

この手法の**概要**

攻撃者は正規のWebブラウザーの機能を悪用して悪意のあるコンテンツの解析をしないようにすることで、**従来型のファイルベースの検査技術をすり抜けられるように設計**した攻撃を作り出します。彼らは、従来型のセキュリティ技術ではすべてのファイルの安全性を完全に確保できないことをよく知っており、検査エンジンによるファイルの例外処理を利用しているのです。

動作の仕組み

攻撃者は、以下のような手法でファイルベース検査エンジンを回避します：

大きすぎるファイル

完全に安全なサンドボックスを作ろうとする場合、ユーザーに送られてくるすべてのファイルを検査しなければなりませんが、これは生産性という観点からは現実的ではありません。そのため**サンドボックスは一定サイズ以上のファイルを検査しません**が、それらには拒否されるものがある一方で、そのままユーザーに送られるものもあります。そのため、脅威がまったく解析されることなく最初の防御層を通過し、気づかれることなく潜り込む可能性があります。

HTML スマグリング

攻撃者は、HTML5やJavaScriptなどのWebブラウザーが持っている正規の機能を活用し、**悪意のあるコンテンツをHTMLコード内に直接隠します**。コンテンツはJavaScriptのBLOB（Binary Large OBject）に隠されており、ユーザーデバイス上のWebページ内で動的に再構築されます。悪意のあるコンテンツは、BLOBの状態でファイアウォール、アンチウイルス（AV）技術、サンドボックスを通過した後、エンドポイント上で再構築されるため、これらのレガシーなセキュリティ技術による検知を完全に回避することができます。

パスワード保護されたアーカイブ

同様の手法として、悪意のあるコンテンツがパスワード保護されたドキュメント内に隠されることがありますが、それをサンドボックスのような従来型のセキュリティ技術で検査することはできません。

PCI（Payment Card Information）データやPII（Personally Identifiable Information：個人を特定可能な情報）のような機密情報を保護するために、サンドボックスによる検査は免除されているからです。攻撃者は、機密情報を含むように見せかけたドキュメントに悪意のあるコンテンツを隠すことで、このセキュリティ対策を容易に侵害することができます。

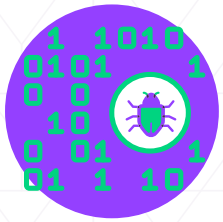
多要素認証（MFA）の回避

この攻撃においては、従来型のセキュリティツールでMFA認証情報やトークンが傍受されたことを検知することはできません。攻撃は迅速で奇襲性があるあるため、防御は非常に困難です。偽のサインインページをブロックできたとしても、攻撃者はすぐに新しいドメインを作成して他のユーザーを狙います。拒否リストやURLフィルタリング、フィッシングトレーニングは十分な対策にはならず、SMSを使用することが多いMFAプロセスはセキュリティチームから見えにくいままです。

実際の攻撃

01. 検査を免れた悪意のあるファイルがブラウザー内で再構築されます。

02. ファイアウォール、サンドボックス、アンチウイルスエンジンなど、従来のセキュリティ技術を回避して悪意のあるファイルを作成します。



03. 通常はセキュアWebゲートウェイ（SWG）でブロックされるファイルタイプでも、ユーザーの操作なしにエンドポイントを侵害する可能性があります。

どのような技術を回避するのか：

- アンチウイルス技術
- サンドボックス

攻撃手法 4:
HTTP コンテンツ/ページ検査の回避

この手法の概要

悪意のあるコンテンツをどれだけ巧妙にWebサイトに隠したとしても、ページのソースコードのどこかには存在しています。そのためHTTPコンテンツ/ページ検査エンジンは、ソースコード全体をスキャンして悪意のあるコンテンツを探します。しかし、コンテンツ全体をスキャンしても、必ずしもすべてを捕捉できるわけではありません。

攻撃者は、正規のWebサイトが機密のコードを難読化する機能をうまく利用して、**このセキュリティ技術を回避する方法を見つけ出します**。

動作の仕組み

攻撃者は、以下のような手法でHTTPコンテンツ/ページ検査エンジンを回避します：

難読化された悪意のあるJavaScript

HTMLスマグリング攻撃と同様に、攻撃者は悪意のあるコンテンツをJavaScriptコードの中に隠し、HTTPトラフィック検査を通過させた後にエンドポイント上で再構築します。悪意のあるコンテンツはエンドユーザーのブラウザー上で再構築されて初めて脅威となるため、それまでは悪意のあるコンテンツは存在しないことになり、検知できないのです。

フィッシングロゴを動的に生成

攻撃者はWebページのソースコードを操作して悪意のあるフィッシングロゴを難読化します。多くの場合、これらの攻撃は洗練されたフィッシングページから始まり、巧妙なCSSトリックを使用して一見無害な画像の下に既知のフィッシングロゴを隠すことで、検知を回避します。このフィッシングロゴはHTTPトラフィック検査エンジンによってまったく解析されることなく、エンドユーザーのデバイスに表示されます。

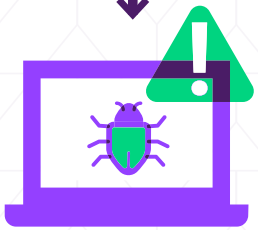
コンテンツ検査を回避するHEATの追加技術

- 解析のためのページリソースの抽出を困難にする個別の機能をエンコードしたり活用したりすることで、フィッシング対策ツールを回避します。

実際の攻撃

01. 攻撃者はJavaScriptやCSSによって悪意のあるコンテンツを難読化します。

02. 悪意のあるコンテンツがエンドポイント上で再構築されます。



03. 被害者がフィッシングロゴをクリックしたり、マルウェアをダウンロードしたりします。

どのような技術を回避するのか：

- HTTP コンテンツ検査技術
- 従来型の SWG

HEAT 攻撃からの防御

サイバーセキュリティの予算を増やしたとしても、これら最新の脅威から防御することはできません。従来型のセキュリティツールは、HEAT攻撃を阻止するようには作られていないからです。これらのツールは検知に依存しているため、脅威に対する視野がネットワーク上で検知できるものに限られてしまいます。そしてこれは、攻撃者に明確な青写真を与えることになります。つまり、最初の検知を回避しさえすれば、侵入することができるということです。その後はネットワーク上を自由に動き回り、データを盗んだり重要なシステムを侵害したりできます。

まったく新しいセキュリティパラダイムが必要なことは明らかです。では、HEAT攻撃を阻止するための最善の方法とは何なのでしょうか? それは、「そもそもHEAT攻撃が起きないようにする」ことです。アイソレーション技術は、セキュリティにゼロトラストアプローチを適用することで、これを実現します。それが悪意のあるものであろうとなかろうと、すべてのWebコンテンツを悪いものとして扱い、クラウド上の抽象化されたレイヤーで実行します。ユーザーが閲覧するWebページやクリックするリンク、そしてダウンロードするメールの添付ファイルなどはすべてクラウド上の仮想ブラウザー内で実行されるため、マルウェアやランサムウェアなどの潜在的な脅威がエンドポイントに到達することはありません。アイソレーション技術はブラウザーの可視性を高め、適応的なセキュリティポリシーを提供するため、セキュリティチームはHEAT攻撃やWebサイトでの疑わしい行動、そしてゼロアワー脅威などからユーザーをリアルタイムに保護することができます。ユーザーに届くのはサニタイズされた安全なコンテンツのみということになり、攻撃者がネットワークに初期アクセスするチャンスを完全に阻止することができます。脅威が侵入できなければ、それは脅威ではないのです。

Menlo Security について

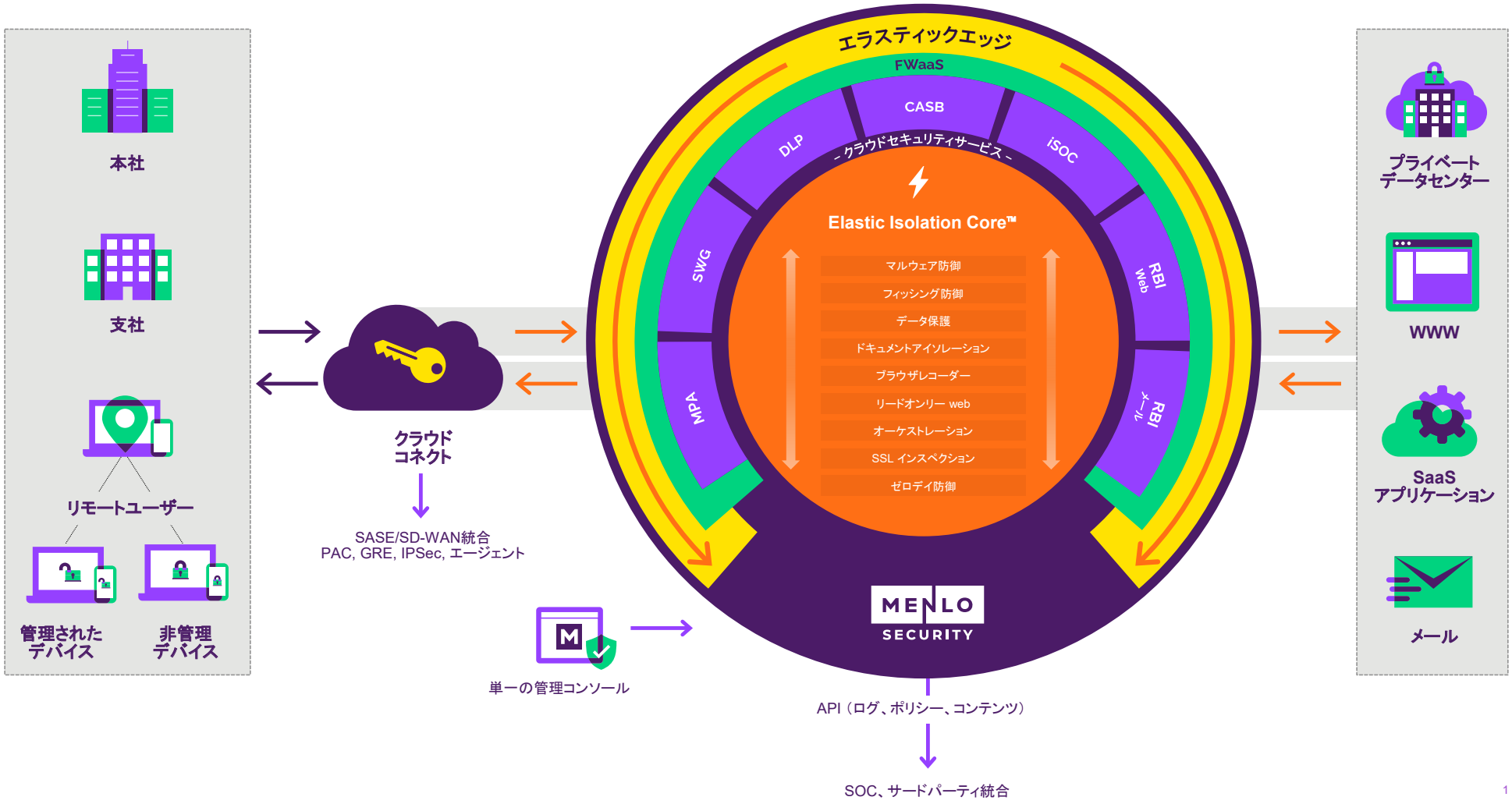
Menlo Securityは、Webやドキュメント、そしてメールからマルウェアの脅威を排除することで、サイバー攻撃から組織を保護します。また、ナレッジワーカーにとって最大の生産性向上ツールであるWebブラウザーの保護に重点を置いています。

Menlo Cloud Security Platformは、脅威が組織に侵入しないように防御し、データとアプリケーションへのアクセスを単一のグローバルなクラウドによって保護します。Menlo SecurityのElastic Isolation Core™は、ユーザー、コンテンツ、アプリケーションを分離し、セキュリティ、ポリシー、可視性を適用します。検知して対応するのではなく、脅威を未然に防ぐことで、企業はWebやメール、SaaSアプリケーション、そしてプライベートアプリケーションに存在するHEAT（Highly Evasive Adaptive Threats：高度に回避的で適応型の脅威）などの脅威を排除することができます。

HEATcheck

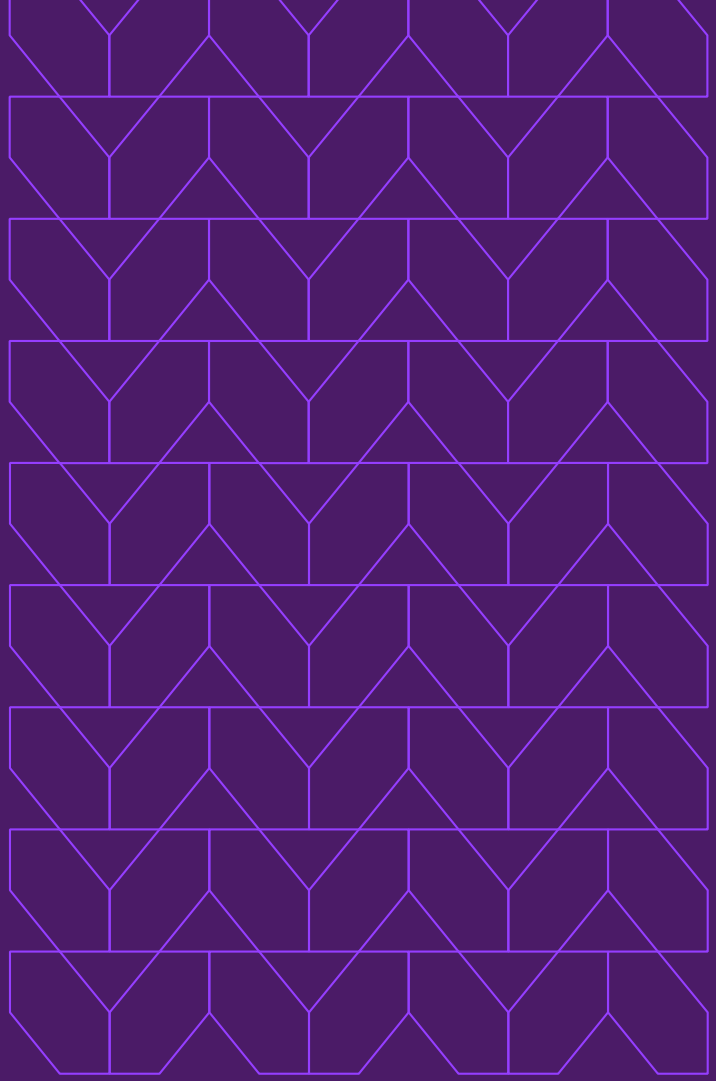
Menlo Securityは、様々なHEAT攻撃に対する組織の耐性をより良く理解するために、軽量のペネトレーションアセスメントを行っています。このアセスメントでは、攻撃者が現実に使用している様々なHEATの手法を使い、組織がそれらにどれくらい影響されやすいかを安全に推測することができます。Menlo SecurityのHEAT Checkツールは、実際に悪意のあるコンテンツを配信することはありません。

Menlo Cloud Security Platform



今すぐ
ご連絡下さい

お客様の組織が現在HEAT攻撃に対して脆弱かどうかを確認するために、**今すぐ私たちにご相談ください**。しかし最も重要なことは、最初にHEAT攻撃を起こさせないようにすることです。



menlosecurity.com/heatcheck

japan@menlosecurity.com

MENLO SECURITY