高度に回避的な脅威を防御するための究極のガイド

eBook

MENLO SECURITY

目次

脅威ランドスケープは予測不能

セキュリティ業界で「燃え尽き」が大きな問題となっているのも無理はありません。サイバー脅威のランドスケープは常に変化しており、既知および未知の攻撃に対して、およそ不可能なレベルの準備が必要とされています。しかも、常に変化しているのはそれだけではありません。

リモートワークやハイブリッドワークへの移行やクラウド投資の増加などにより、ビジネスのダイナミクスや環境は急速なペースで変化しています。これは企業にとって無限の可能性ですが、その可能性は一面的なものではありません。攻撃者もまたその動向を注視しており、変化する環境を利用して大きな報酬を得ようとしています。防御側は、脅威対策を考え直す必要に迫られています。

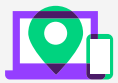
世界的なパンデミックの影響で業務の進め方は大きく変化しましたが、サイバーセキュリティの習慣、ツール、戦略はほとんど変化していません。その結果攻撃者は、防御側が進化することを気にすることなく、サイバーセキュリティの方法論とその限界について研究する時間を持つことができました。その結果、攻撃者は明確に定義された目標と、それを実現するための計画を持つに至ったのです。

数字で見る：現代の仕事と脅威ランドスケープ

スタッフの **75%** が、Webブラウザーを使用して業務を行っている[1]

ランサムウェア攻撃の **49%** は、デスクトップまたはラップトップのWebブラウザーを経由して遂行される[2]

組織の **99%** が、SaaSアプリケーションを使用している[3]



企業の **70%** が、ハイブリッドオフィス/リモートワークモデルを採用しており、SaaSの急速な普及に拍車をかけている[4]

2021年に起きた侵害の **82%** に、何らかの形でソーシャルエンジニアリングが関与している[5]

セキュリティインシデントの **60%** 以上（過去1年間）が、Webアプリケーションを通じて行われた[6]

1 https://cloud.google.com/blog/products/chrome-enterprise/chrome-is-helping-it-teams-support-cloud-first-workforce
2 https://info.menlosecurity.com/Assessing-ransomware-readiness-in-2022.html
3 https://info.menlosecurity.com/Assessing-ransomware-readiness-in-2022.html
4 https://www.mercer.us/our-thinking/the-future-of-flexible-working-is-hybrid.html?bsrc=mercer
5 https://www.verizon.com/business/resources/reports/dbir/
6 https://www.verizon.com/business/resources/reports/dbir/

HEATの急増

拡大する脅威ランドスケープが新たな環境に適応するにつれ、私たちが目にする脅威にも変化が生じています。新しいものではありませんが、HEAT（Highly Evasive Adaptive Threats：高度に回避的で適応型の脅威）と呼ばれる種類のサイバー脅威が急速に成長してきており、Lazarus、Gorgon、Guildmaなどの主要な攻撃グループがその成功率の高さを認めています。

HEAT攻撃とは?

HEAT攻撃は、攻撃ベクトルとしてWebブラウザーを利用し、現在のセキュリティスタックにおける複数レイヤーによる検知を回避するためのさまざまな技術を活用するサイバー脅威の一種です。

1. HEAT攻撃は、従来型のWebセキュリティ対策を回避します。ブラウザーに到達する前に実行されるすべてのセキュリティ防御は無力です。

   これには、セキュアWebゲートウェイ（SWG）のアンチウイルスエンジンやサンドボックスが行うファイル検査、ネットワークやHTTPレベルの検査、悪意のあるリンク分析、オフラインでのドメイン分類、IOC（Indicator of compromise）フィードが含まれます。

2. Webブラウザーの機能を活用してマルウェアを配信したり、認証情報を漏洩させたりします

3. 多くの場合ランサムウェアの配信につながります

HEATを好む攻撃者の代表的な例として、2020年のSolarWindsサプライチェーン攻撃に関与したNobelium（ロシアが支援する組織）が挙げられます。

2021年後半には、HEAT攻撃が224%増加しました[7]。

7　https://www.menlosecurity.com/ja-jp/%E7%86%B1%E3%81%99%E3%81%8E%E3%81%A6%E8%A7%A6%E3%82%8C%E3%81%AA%E3%81%84%EF%BC%9A%E5%83%8D%E3%81%8D%E6%96%B9%E3%81%AE%E5%A4%89%E5%8C%96%E3%81%8Cheat%E6%94%BB%E6%92%83%E3%82%92%E7%94%9F%E3%82%93/

古い技術の再利用

Menlo Labsのチームが分析した50万個の悪意のあるURLのうち、69%がHEAT技術を利用していました。[8] これは、攻撃者が古くからの攻撃技術をうまく活用し、採用を拡大しているという懸念すべき傾向を浮き彫りにしています。

最近のWeb経由の脅威を分析すると、攻撃者はブラウザー環境で利用可能な正規の機能とツールをうまく利用して、悪意のあるペイロードをエンドポイントに配信していることがわかります。

攻撃者はその成功率の高さから、HTMLスマグリングやその他のHEAT技術に注目しています。これらの攻撃は、SWGやそれによるマルウェア対策、サンドボックス機能、ネットワークおよびHTTPの検査、悪意のあるリンク分析、オフラインドメイン分析、脅威インテリジェンスフィードなどの一般的な防御技術を回避してエンドユーザーのブラウザーに到達します。

8 https://www.menlosecurity.com/ja-jp/%E7%86%B1%E3%81%99%E3%81%8E%E3%81%A6%E8%A7%A6%E3%82%8C%E3%81%AA%E3%81%84%EF%BC%9A%E5%83%8D%E3%81%8D%E6%96%B9%E3%81%AE%E5%A4%89%E5%8C%96%E3%81%8Cheat%E6%94%BB%E6%92%83%E3%82%92%E7%94%9F%E3%82%93/

HEAT攻撃の4つの回避特性

HEAT攻撃の急増を調査していると、「*この手法は従来型のセキュリティスタックに対してなぜこれほど有効なのか?*」という疑問を持ちます。その答えは、一般的なHEATの特徴である回避的な特性にあります。

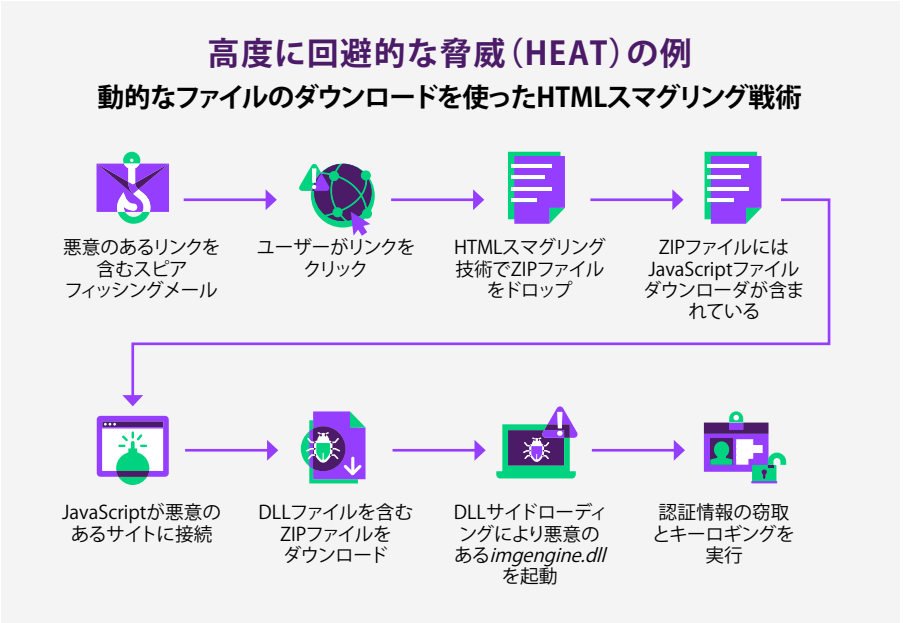
HEAT攻撃に分類されるためには、その脅威が以下の4つの特性の1つ以上に該当している必要があります:

1 WebカテゴライズとURLレピュテーションを回避する

業務でのWebブラウザーの利用が増えたことで、攻撃者はWebカテゴライズを回避する脅威で行動のホットスポットを狙います。

攻撃の概要:

1. 攻撃者は**新しいWebサイト**を作成し、しばらくそのサイトを維持して信頼を確立してから悪意のある運用に切り替え、**そして/または**
2. 攻撃者は**正規のWebサイトを侵害**し、マルウェアの配信ベクターとして使います



有名な攻撃はHEATを活用している

ブラウザーのエクスプロイトが脚光を浴びることがあります。Log4j、Lazarus Groupによる攻撃、SolarWindsなどの有名な攻撃は、金銭や知的財産の窃取のためにHEAT攻撃の技術を使用しています。

2 セキュアメールゲートウェイ（SEG）や悪意のあるリンク解析を回避する

企業はメールセキュリティを強化し、マルウェアや悪意のあるリンクのスキャンを積極的に行っています。これは一般的には良いことですが、そのために攻撃者はそれを回避して内部に侵入する新しい方法を見つける必要に迫られたのです。また、技術の向上と共に、人々がより注意深くなり、悪意のあるリンクに気づくようになりました。これでフィッシングとの闘いは非常に有利になりました。

攻撃者はフィッシングの成功確率を高めるために、メール以外のフィッシング経路に軸足を移しています。HEAT攻撃では、Web、ソーシャルメディア、プロフェッショナルネットワーク、コラボレーションツール、SMSなどのチャネルがトラブルの温床となるのが一般的です。これらの経路では、人々は相手を盲目的に信頼し、迷うことなくリンクをクリックしてしまう傾向があります。

攻撃の概要：

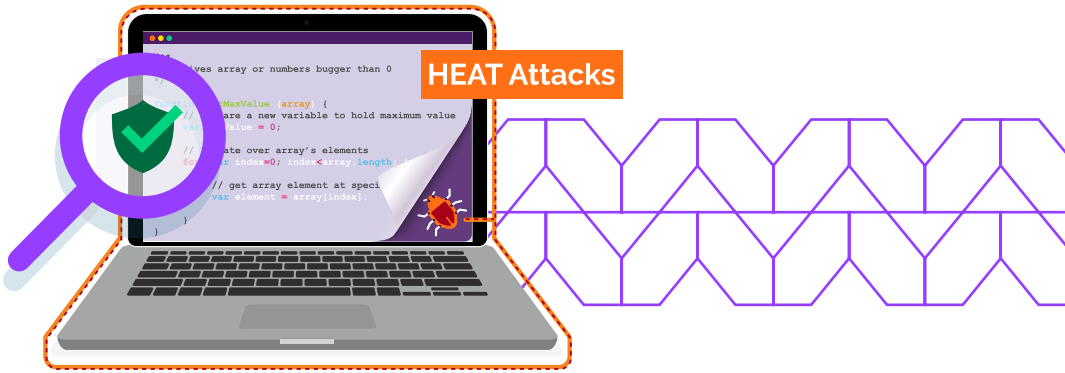
1. メール以外のコミュニケーションチャネル（コラボレーションアプリケーション、SMS、共有ドキュメント、LinkedIn、Facebookなど）を通じて、ユーザーが悪意のあるリンクで狙われたり、スピアフィッシングのターゲットにされたりします
2. 悪意のあるリンクの先で認証情報を要求されたり（個人情報ではなく、企業認証を狙うものが増えている）、マルウェアを配布されたりします
3. HTMLスマグリング攻撃のようなHEATの特徴の1つ以上と組み合わせることで、従来のセキュリティ制御や技術を回避する確率を高めることができます

3 ファイルコンテンツ検査（AV＆サンドボックス）を回避する

ユーザーはブラウザー上で業務を行う時間が長くなっているため、攻撃者はソフトウェアの脆弱性や設計上の欠陥を利用する代わりに、最新のブラウザーが持っている正規の機能を悪用しようとしています。これには、ダウンロード速度を最適化する機能や、ユーザーのWebエクスペリエンスを向上させるために開発者が普通に使用する技術も含まれています。具体的には、HEAT攻撃は多くの場合ブラウザー環境内でHTMLスマグリングやJavaScriptのトリックを使用して悪意のあるペイロードをエンドポイントに配信します。

攻撃の概要：

1. 検査が可能なリモートファイルへのリクエストを行わず、ブラウザーレベルで悪意のあるファイルを構築します
2. マルウェアを転送し、レガシーなプロキシでのサンドボックスやアンチウイルスなど、様々なファイアウォールやネットワークセキュリティソリューションを効果的に回避します
3. SWGのポリシーがブロックするはずのファイルタイプでも、ユーザーの操作無しでエンドポイントに到達させることができます



4 HTTPトラフィック検査を回避する

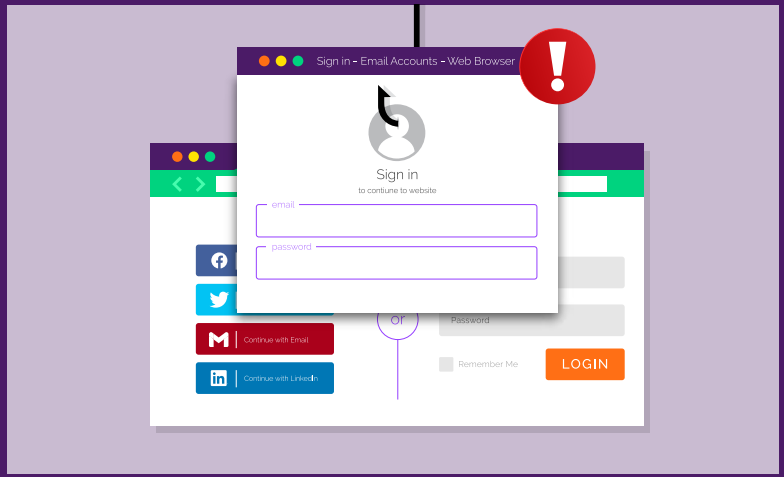
HTTP解析エンジンは、フィッシングキットやマルウェア、そしてブラウザーに流入する悪意のあるコンテンツなどのエクスプロイトを探します。攻撃者は現在の保護機能を熟知しており、検査を回避するようになりました。

攻撃者は検査を回避するために、本物のように見える巧妙なフィッシングページや、エンドユーザーに近いブラウザーレベルでのCSS操作を使うようになっています。

攻撃の概要：

1. 攻撃者は、HTTPトラフィックが検査エンジンを通過した後に、JavaScriptの難読化を使用して悪意のあるコンテンツを動的に生成します
2. コンテンツはエンドポイントのWebブラウザー内で作成されます
3. 画像やコードはローカルのJavaScriptエンジン内でレンダリングされたり実行されたりするため、攻撃のためのコードがエンドポイントに到達する前に行われるセキュリティ検査を回避します

現代のWebサイトがHEAT攻撃に対して非常に脆弱である一例として、Log4jの脆弱性が挙げられます。アプリケーションのエラーメッセージを記録するために使用されるこのオープンソースライブラリは、ほとんどのサイトで使われており、パッチが適用されていないバージョンは容易に侵害されてしまいます。



現場で多く見られるHEAT攻撃を知ろう

Browser in the Browser（BitB）攻撃は、ユーザーがサイトにアクセスし、サードパーティ（GoogleやFacebookなど）を経由してサインインしようとしたときに開始されます。

ユーザーがリンクをクリックすると、HTMLとCSSで完全に構築された別のポップアップが表示されます。ポップアップに表示されるURLは正規のサイトのように見えますが、その下にあるiframeはフィッシングサイトにつながっています。

最近のBitBキャンペーンでは、複数のフィッシングサイトに関与するドメインゲートウェイが宝の山をホストし、一般的なメールのログインページから偽のCDCランディングページへのリンクを参照していました。被害者が認証情報を入力すると、BitB攻撃はJavaScriptを使って被害者の認証情報を悪用するために送信しました。

防御を真剣に考える

Menlo Securityの「The State of Threat Prevention」レポートで調査した企業の60%が、企業ネットワークを保護するためのテクノロジーへの投資を増やすと回答しています[9]。

サイバーセキュリティがビジネスの拡大に不可欠なものとして扱われている以上、支出が増加するのは驚くことではありません。しかし、*より多くの投資を行うことがセキュリティの向上につながることをどのように確認するのか?*という疑問が生じます。

HEAT攻撃が急増する中、企業は保護のための投資に対するリターンを向上させるために、脅威がネットワークやエンドポイントに侵入するのを初期段階で阻止する技術を必要としています。

迅速な検知と防御は違う

従来のセキュリティ技術や現在販売されている多くのサイバーセキュリティソリューションは、検知と対応というコンセプトの下で開発されています。HEAT攻撃が従来型のセキュリティ技術を回避し続ける中、私たちは一歩引いて、攻撃を阻止するためにネットワークへの攻撃を待つことは、実際には防御ではないということを考える必要があります。

検知と修復は、今後もセキュリティスタックの重要なレイヤーであり続けますが、それが最初のレイヤーであるべきではありません。脅威ランドスケープが脅威の発生を前提とするのであれば、防御の第一段階は、脅威がネットワークやエンドポイントに到達する前にブラウザーで阻止することであるべきなのです。

検知の欠点

修復の作業は、サイバーセキュリティチームに多大な負担をかけます。検知して対応するというアプローチでは、セキュリティアナリストはアラートに忙殺されます。アナリストはアラートを調査し、本物の脅威かどうかを特定しなければなりません。本物の脅威が発見された場合、アナリストは取締役会に報告し、修復し、機密情報がダークWebに流出したかどうかを確認する必要があります。

すべての作業が終わった後でも、攻撃者が見えないところに隠れていないと100%確信することはほぼ不可能です。

9 https://resources.menlosecurity.com/midmarket-heat/the-state-of-threat-prevention-evasive-threats-take-center-stage

ランサムウェアへの備え

Verizonの「2022 Data Breach Investigations Report」によると、ランサムウェアビジネスは活況を呈しています。2021年にランサムウェアは前年比で13%増加し、マルウェアによる侵害の約70%が何らかの形でこの迷惑行為に関与しています[10]。この劇的な増加は過去5年間の増加分を合わせたのと同じくらい大きく、記録に残るものとなりました。

HEATがランサムウェアの急増に貢献

ランサムウェアの増加とHEAT攻撃の復活は、偶然の一致ではありません。ハイブリッドワークへの移行が生み出したセキュリティギャップと、ブラウザーへの依存度の高さは、ランサムウェアの攻撃者がHEAT攻撃を活用する絶好の機会となっています。

イニシャルアクセスブローカーを使うことで、誰でもランサムウェアを配信するHEAT攻撃を行えます

サイバー犯罪者は、もはや専門的なハッカーである必要はありません。Initial Access Brokers（IAB）は、ターゲットとなる組織へのアクセス手段を収集し、それを販売することで市場を開拓しています。クレジットカードや暗号通貨のアカウントを使ってRaaS（Ransomware-as-a-Service）を利用することで、犯罪者は監視や調査といった手間のかかる作業をせずに、簡単に初期アクセスの手段を手に入れることができます。攻撃者はこの初期アクセス手段を使って、企業の情報やシステムを押さえて身代金を要求したり、貴重なデータを盗んだり、ペイロードを配信したり、業務を妨害したりすることができます。

このような、IABを使ったランサムウェア攻撃を開始するのがHEATです。攻撃を阻止するための鍵は、組織への最初の足場作りやアクセスを阻止する技術を使用することです。多くの企業がセキュリティ戦略の骨格としてMITRE ATT&CK®フレームワークを採用しているのは、そのためです。

バックアップでは不十分

ランサムウェアに対するこれまでの対策は、安全なバックアップとリカバリーでした。しかし、HEAT攻撃を知ればわかるように、従来のセキュリティ対策ではこれらに太刀打ちできません。攻撃者は一度侵入してしまえば、後は好きなだけ盗むことができます。

たとえランサムウェア攻撃を検知できたとしても、攻撃された環境の詳細な調査など、長時間の作業が必要になり、情報が盗まれなかったことを保証できるものでもありません。

犯罪者はボタンひとつで暗号化を行うことができ、それは身代金が支払われた後でも、もう一度行うことができます

10 https://www.verizon.com/business/resources/reports/dbir/

防御のための3つの重要な考え方

防御側と攻撃側の戦いについては、昔から語り継がれていることです。しかし私たちが気づいたのは、単一の完璧なソリューションがあるわけではなく、様々な脅威を考慮した多階層のアプローチが最も効果的であるということです。

高度なマルウェア、ランサムウェア、バンキング型トロイの木馬、恐喝型マルウェアが組織にプレッシャーをかけ続ける中、これらの攻撃を成功させないために注力すべき3つの重要な考え方があります：

1. 検知型から防御型への移行
2. 脅威がエンドポイントに到達する前に阻止
3. 高度なフィッシング対策とアイソレーション機能の採用

対応ではなく、防御で先行する

企業が防御のためにサイバーセキュリティソリューションを購入する場合、最高の結果を得るためには明確な意図を持つ必要があります。つまり、攻撃がデバイスやシステムに影響を与える前に、可能な限り多くの脅威を防ぐという目標に照準を合わせなければならないのです。

サイバー犯罪者がすでに対応策を持っている防御技術を重ねるのではなく、犯罪者がお金を稼ぐためにさらなる努力が必要なように仕向けるのです。

脅威ランドスケープの変化に合わせた多階層防御を構築するためには、ゼロトラストアプローチを採用した防御的な対策が必要であり、業務が行われる場所で保護しなければなりません。

アイソレーションはこれを達成する方法の一つです。作業をエンドポイントから離れたクラウドベースのリモートブラウザーで行わせることで、すべてのコンテンツが実際の良し悪しと関係なく悪意のあるものとして扱われ、安全であることが証明されるまで保護が強化されます。

脅威防御の考え方とその実現

未来の仕事がどうなるのか、という質問への答えで唯一確実なのは「変化する」ということです。そしてこれは、脅威にも当てはまります。将来何が起こるにしても、組織は高速かつ信頼性の高い、安全な業務環境を提供し続けるための準備をしておく必要があります。

あらゆる変化に対応できるセキュリティスタックはありません。しかし、攻撃者やその戦術を出し抜くためには、防御的な考え方を身につける必要があります。

脅威から防御するための3つの必須アイテム

1 グローバルな弾力性

ハイブリッドワークとは、従業員、サードパーティ、コントラクタが世界のどこにいても良いということです。ユーザーがクラウド上のどこにいても、ボタンひとつでセキュリティを確保できることを確認してください。これは、プロビジョニングや追加の設定作業、ベンダーへの通知、あるいは新たな契約は不要ということを意味します。

2 統一されたプラットフォーム

ブラウザー上で多くの業務が行われるようになったことで、その活動を監視し、他のセキュリティソリューションを管理できるようにしたいという要望が出てきました。セキュリティチームが単一のコンソールを通じて、Web、SaaSアプリケーション、プライベートアプリケーションを横断的に制御し、数十万人のユーザーに対してWebセキュリティを適用できるようにする必要があります。

3 シームレスなユーザーエクスペリエンス

最も効果的なセキュリティは、シームレスなエクスペリエンスを提供できるものです。使い勝手が悪いためにユーザーがセキュリティ機能を回避してしまうようでは、意味がありません。問題を最小限に抑えながらユーザーエクスペリエンスとセキュリティを融合させるのは簡単なことではありませんが、このような保護目標を達成できるように設計されたソリューションがいくつか存在します。例えばアイソレーションは、エンドポイントソフトウェアを必要とせず、操作性に影響を与えることなく、本来のユーザーエクスペリエンスを維持できます。

アイソレーションのような脅威防御技術を導入する際の最大の課題は、多くの場合スケーラビリティです。グローバルな弾力性こそが、あらゆる場所であらゆる仕事を守ることのできる、唯一の方法なのです。

侵害が起きないようにする

侵害やセキュリティインシデントからの復旧には膨大なコストがかかり、企業価値も損なってしまいます。そのような状況を回避する最善の方法は、そもそも侵害が起きないようにすることです。これまで使われてきた検知や修復によるアプローチは、脅威が組織内に侵入して初めて効果を発揮しますが、Menlo Securityの防御的なアプローチは、攻撃に最初の足場を作らせないようにすることで、ランサムウェアやその他の脅威から組織を確実に保護することができます。

脅威が入り込めなければ、それは脅威にはなりません。

Menlo Security Isolation Core™

Menlo SecurityのElastic Isolation Core™は、既知および未知の脅威がユーザーに到達する前にそれらを分離することで、ユーザーを保護します。ゼロトラストのアイソレーションは、特別なソフトウェアやプラグインを必要とせずにWebやメールからマルウェアを完全に分離し、100%の保護を可能にします。ユーザーはパフォーマンスへの影響やワークフローの中断を感じることはありません。

Menlo SecurityのElastic Isolation Core™は、ランサムウェアのペイロード、バンキング型トロイの木馬、その他の高度なマルウェアを配信するHEATを使った脅威を軽減することができる、ユニークな位置にあります。Menlo SecurityがブロックするHEAT攻撃の手法は以下の通りです：

- デスクトップおよびモバイルデバイスのゼロデイエクスプロイト
- HTMLスマグリングまたは動的なファイルのダウンロード
- すでに良性として分類されている無名のサイトや保護の弱いサイトでペイロードをホスティングするLURE（Legacy URL Reputation Evasion）
- 攻撃者が最もよく使う初期アクセス方法であるクレデンシャルフィッシング

Menlo Securityで攻撃者を出し抜き、打ち勝つ

- 1,000人から300万人以上のユーザー数まで、グローバルにオンデマンドでスケールアップし、パフォーマンスを低下させることなく分離
- あらゆるものを分離
- すべてのセキュリティソリューションに対応した単一の管理・レポートコンソール
- リモートワークのための効果的なWebおよびメール保護機能
- わかりやすい課金設定

既知および未知の脅威にスポットライトをあてましょう

インサイト、専門知識、文脈、そしてツールについては、Menlo Labsのサイトをご確認ください。

https://www.menlosecurity.com/ja-jp/

MENLO SECURITY