Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

HEAT（高度な回避性を持つ適応型脅威）で「ヒート」アップする脅威ランドスケープ

ESG シニアアナリスト：John Grady

2022 年 1 月

本 ESG White Paper はメンロ・セキュリティの依頼で制作されたもので、
ESG からの許諾を得て配布されています

目次

はじめに

この 10 年間で職場環境や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基本的プラクティスやツール、戦略はほとんど変わっていません。その一方で攻撃者は高いモチベーションを持ち、常に防御側の先回りをすべく進化を続けています。攻撃者は従来型のサイバーセキュリティについて、その限界も含めて十分に理解することで、攻撃を確実に成功させるための青写真を明確に描いています。

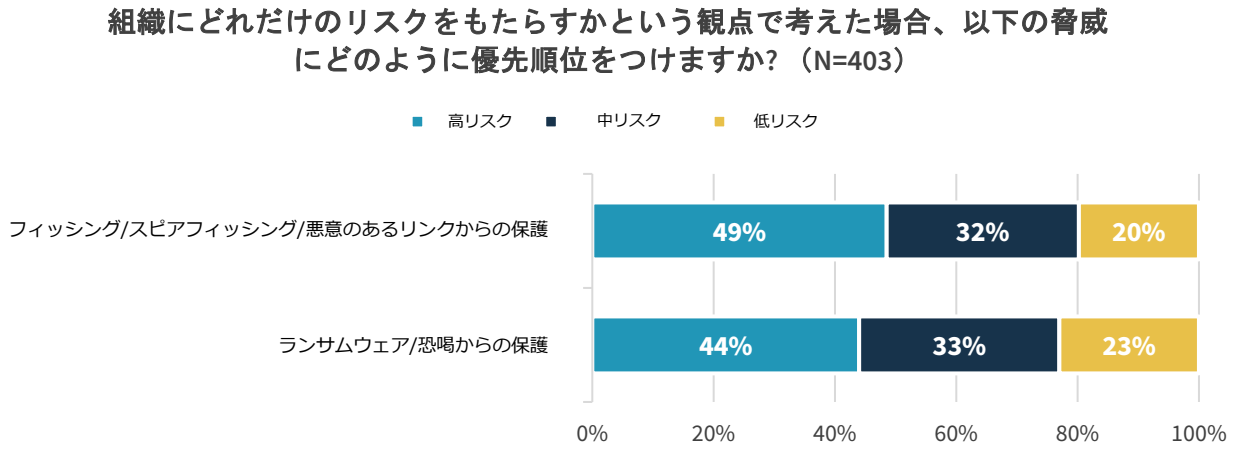
メンロ・セキュリティは、攻撃者がランサムウェアやフィッシング攻撃を成功させるために使用しているさまざまな技術を研究し、これらをまとめて「HEAT（Highly evasive adaptive threat：高度な回避性を持つ適応型脅威）」と名付けました。HEAT 攻撃は、既存のセキュリティスタックに統合されているすべての技術を十分に理解し、それらの検知を逃れるための配信メカニズムを構築することで、既存のセキュリティ防御を回避します。組織が HEAT 攻撃による脅威に対処するためには、侵入を検知するという考え方から、脅威がエンドポイントに到達する前の段階で阻止するという「予防」の考え方に移行する必要があります。

> HEAT（Highly evasive adaptive threat）攻撃は、既存のセキュリティスタックに統合されているすべての技術を十分に理解し、それらの検知を逃れるための配信メカニズムを構築することで、既存のセキュリティ防御を回避します

脅威ランドスケープの進化

多くの組織では、ここ数年でサイバーセキュリティが IT 部門の問題からビジネス上の優先課題へと昇格しました。これは、クラウドの導入やデジタルトランスフォーメーションなどの広範な取り組みを進める上でサイバーセキュリティが果たす役割が拡大したことに加え、脅威ランドスケープの進化や、攻撃が成功した場合のビジネスへの悪影響が認知されたことも要因です。どのようなサイバー攻撃もビジネスに混乱を引き起こす可能性がありますが、ランサムウェア、サイバー恐喝、フィッシング攻撃などは特に重大な影響を及ぼす恐れがあるため、多くの組織で優先リストの上位に上がってきています。実際、ESG の調査[1]によると、約半数の組織がフィッシングやランサムウェアの攻撃を組織にとっての重大なリスクと考えています。（図 1 参照）

図 1. フィッシングおよびランサムウェア攻撃に対するリスク認識



出典: *Enterprise Strategy Group*

さらに興味深いのは、22%の組織がランサムウェアへの対策を最も重要なビジネス上の優先事項であると回答し、46%がビジネス上の最優先事項のトップ 5 のうちの 1 つであると回答[2]していることです。Colonial Pipeline のような重要なインフラや、Acer や Kaseya などの IT サプライヤーに対する攻撃が広く知られたことで、この問題は取締役会で真っ先に取り上げられる議題になりました。

[1] 出典： ESG Research Report, *Trends in Email Security*, August 2020.

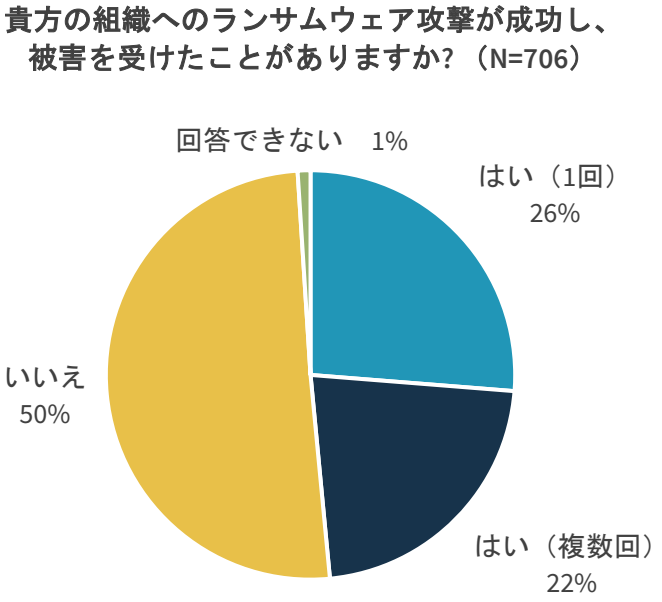
[2] 出典： ESG Complete Survey Results, 2022 Technology Spending Intentions Survey, November 2021.

22%の組織がランサムウェアへの対策を最も重要なビジネス上の優先事項であると回答し、46%がビジネス上の最優先事項のトップ 5 のうちの 1 つであると回答しました

しかし、世界有数の大企業で発生し、大きなニュースになったランサムウェアの事例だけに注目していると、あらゆる種類、規模、セキュリティレベルの組織が日々この問題と闘っているという事実が見えなくなる可能性があります。ESG の調査によると、36%の組織が毎日、毎週、または毎月ランサムウェアの攻撃を受け、さらに 27%の組織が過去 12 ヶ月の間に散発的にランサムウェアに遭遇していることが分かっています。[3]

そして残念ながら、これらの攻撃はしばしば成功しています。ESG の調査への回答者の 4 分の 1 以上（26%）が、ランサムウェアの攻撃を一度は受けたことがあり、22%が複数回受けたことがあると回答しています[4]。（図 2 参照）セキュリティチームは十分にこれらの問題を認識しており、セキュリティベンダーはこれらの攻撃から防御するために製品の更新を続けています。しかしそれでもなお、多くの組織がランサムウェアや金銭的な動機による攻撃の被害を受けているのです。攻撃者はどのようにして防御策を回避し続けているのでしょうか。

図 2. 成功したランサムウェア攻撃



出典： *Enterprise Strategy Group*

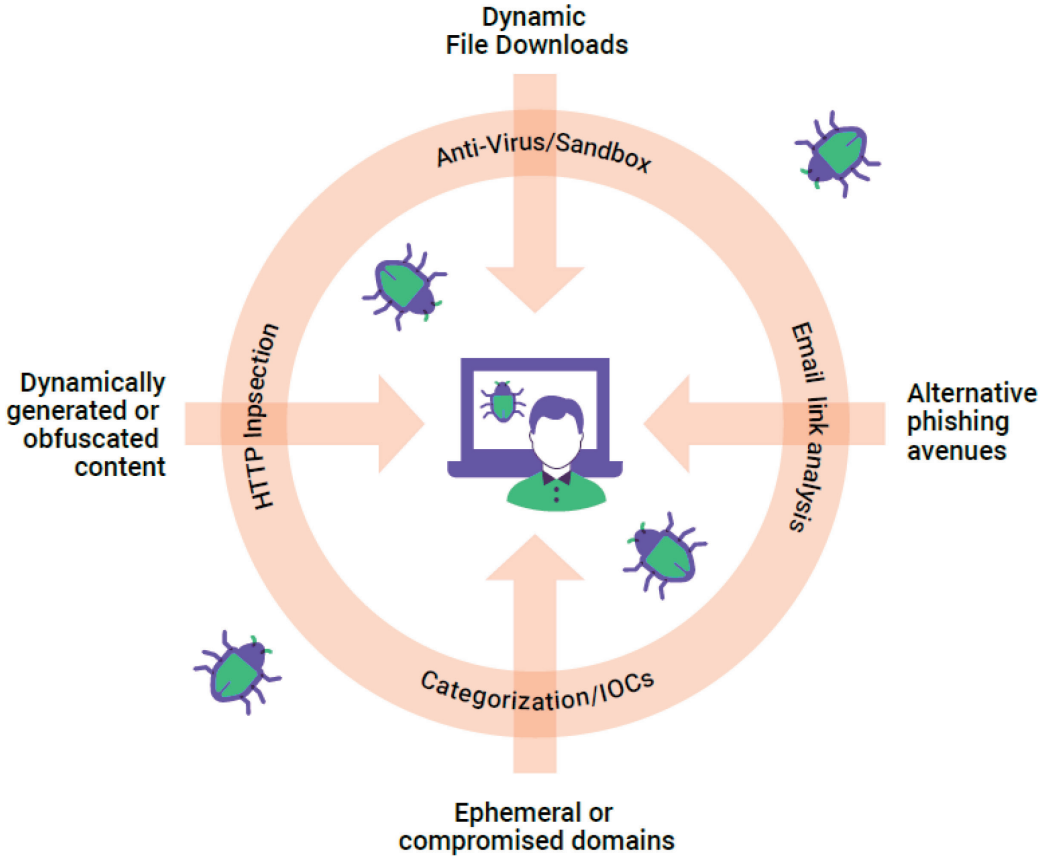
「高度な回避性を持つ適応型脅威」の定義

攻撃者は、従来型のセキュリティツールによる検知を免れるために、さまざまな技術を組み合わせて使うようになっており、メンロ・セキュリティでは最近そのような一連の技術を特定しました。これらの攻撃をまとめて「HEAT（Highly Evasive Adaptive Threats：高度な回避性を持つ適応型脅威）」と呼んでいます。HEAT はランサムウェアを始め、ユーザー、エンドポイント、アプリケーションを標的とするあらゆるタイプの攻撃に使用されます。（図 2 参照）これらの攻撃は、以下の 4 つの主要な技術のうち 1 つ以上を使っています：

[3] Ibid.
[4] Ibid.

1. **ファイルの動的なダウンロード：**HEAT 攻撃は、HTML スマグリングを利用して、シグネチャおよびコード分析ベースの検知手法を回避します。この技術は、HTML5 と JavaScript の標準機能を使用して、目立たないようにエンドポイントにダウンロードを配信します。攻撃者はエンコードされた JavaScript blob を作成し、ユーザーがそのリンクをクリックすると、ブラウザーがスクリプトをデコードしてデバイス上で悪意のあるペイロードを組み立てます。マルウェアはデバイス上で構築されるため、悪意のあるファイルが従来のスキャン機構を通過することはありません。JavaScript を無効にすれば攻撃を緩和することができますが、そうすると正規の Web ページの閲覧にも影響を与えるため、現実的ではありません。この手口は新しいものではありませんが、使用される頻度は増加しています。SolarWinds 社への侵入やその他の著名な攻撃を行ったハッキンググループ Nobelium はこの手法を使用しており、Menlo Labs では、HTML スマグリングを巧妙に利用している Duri や ISOMorph とラベル付けされたキャンペーンを監視しています。
2. **代替のフィッシング経路：**フィッシング攻撃は従来、攻撃経路としてメールを使うのが一般的でした。しかし、ユーザーが不審なメールに気をつけるよう訓練され、メールセキュリティツールがフィッシングリンクを検知する能力を向上させたため、HEAT 攻撃は他の経路にシフトしています。今では LinkedIn やその他のソーシャルメディアサイトを利用したスピアフィッシングが、フィッシング対策ツールを回避するための一般的な経路となっています。攻撃者は、友達申請、コンテンツの投稿、仕事の依頼などを利用して、マルウェアのペイロードを直接、または悪意のある URL 経由で配信します。同様に、攻撃者が無防備な受信者に悪意のあるリンクを送信するために SMS メッセージを使用することが多くなっています。どのような経路で行われるにせよ、結果は同じです。セキュリティチームが問題の存在に気付く前に、認証情報やその他の機密情報が盗まれてしまうのです。
3. **一時的な、または危険なドメインの使用：**これは新しい手法ではありませんが、攻撃者は簡単に悪意のあるサイトを立ち上げることができるため、サイトのカテゴリ分けエンジンが HEAT 攻撃に追いつくことはますます困難になっています。オフラインの Web クローラーが悪意のある行動を特定する前に、攻撃者はそのサイトを削除して別のサイトを作成します。また攻撃者は、短期間しか存在しない一時的なサイトやドメインを使用するだけでなく、サイトを構築して数日、数週間、あるいは数カ月待ってから悪質な行動に出るという、持続的なアプローチを取ることもあります。どちらの場合も、CAPTCHA を使用することでサイトを合法的に見せかけ、オフラインの Web クローラーを回避し、そのサイト自身が悪意のあるコンテンツを配信することが多くなっています。さらに、攻撃者は防御が不十分な正規のサイトを侵害してマルウェアの配信に利用し続けるため、善悪のカテゴリ分けを前提とした防御は、あまり効果的ではありません。
4. **動的に生成されたコンテンツや難読化されたコンテンツの使用：**HEAT 攻撃は、シグネチャによる Web ページのソースコード検査で JavaScript の Eval()関数の使用などを検知されることを避けるために、ブラウザー上でエクスプロイトコードを生成することがあります。さらに、攻撃者は JavaScript を難読化し、セキュリティ研究者と検知エンジンの両方から読み取れないようにすることもあります。そして攻撃者は視覚的な検知に依存するエンジンを回避するために、JavaScript を使用して Web サイトのコードを操作し、有名ブランド（Office365 など）から本物のロゴを持ってくることもあります。

図 3. HEAT（高度な回避性を持つ適応型脅威）



出典： *Menlo Security*

セキュリティチームが HEAT 攻撃に取り組まなければならない理由

サイバーセキュリティが難しくなっているということには、ほとんどの IT プロフェッショナルが同意しています。ESG の調査によると、回答者の 64%が、エッジにおけるネットワークセキュリティは 2 年前よりも困難になっていると回答しています。そして 41%が、脅威ランドスケープの進化がエッジでのネットワークセキュリティを困難にしている要因の 1 つであると回答しており[5]、それがこの複雑さをもたらしている主な要因です。この様な状況下で、特に HEAT 攻撃に注意すべき理由とは何なのでしょうか。

その最大の理由は、HEAT 技術を使用する攻撃と攻撃者のタイプにあります。マイクロソフトは、2021 年 5 月に Nobelium グループが高度なスピアフィッシングキャンペーンで HTML スマグリングを使用していることを観測しました[6]。 同様に、ランサムウェアに使用されることが増えている Trickbot は、攻撃初期のペイロードを配信するために HEAT 技術を使用していました。この 2 つの脅威アクターの攻撃対象は幅広く、あらゆる規模や種類の組織に影響を与える可能性があり、これらの手法が実際の攻撃に使われているという事実は、HEAT 攻撃が今後ますます拡大する可能性を示唆しています。

このような攻撃の増加が問題となるのは、従来型のツールや戦略ではこれらの攻撃に対抗しきれないという現実があるからです。マルウェア検知は、シグネチャベースのアプローチからサンドボックスや分析を使ったアプローチへと変化してきましたが、その進化はわずかなものに過ぎません。これらの技術は依然として悪意のあるコードを検知することに依存しており、攻撃者に防御を回避する機会を与えてしまいます。

[5] 出典： ESG Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.

[6] 出典： Microsoft Threat Intelligence Center (MSTIC), *New sophisticated email-based attack from Nobelium*, May 2021.

ネットワーク型であれエンドポイント型であれ、従来型のセキュリティモデルでは、シグネチャや解析エンジンが適正に更新されるためには、どこかで誰かが最初の被害者になる必要があります

例えばサンドボックスは、難読化されたファイルや特定のサイズのファイルを処理できない場合があります。さらに、マルウェアはサンドボックスを回避することがあるため、企業は配信後にも分析を行ったりファイルを一時保留したりする必要がありますが、それがユーザーの生産性に影響を与える可能性についても検討しなければなりません。エンドポイント製品はデバイスそのものに常駐するため有利に見えるかもしれませんが、これらのツールは管理されていないデバイスに導入することが難しいため、攻撃の最初の段階でハッカーによって無効化されてしまうことも少なくありません。ネットワーク型であれエンドポイント型であれ、従来型のセキュリティモデルでは、シグネチャや解析エンジンが適正に更新されるためには、どこかで誰かが最初の被害者になる必要があります。

さらに、業務の進め方は根本的に変化しています。ほとんどの従業員は、多くの時間を Web ブラウザーに費やしています。SaaS アプリケーションへのアクセス、増加している Web ベースのプライベートアプリケーション、Web 上でのリサーチ、あるいはメールへのアクセスなど、多くのユーザーは日常業務の基礎としてブラウザーを使っています。ブラウザーが新たなオフィスになり、同時にインターネットも新たな社内ネットワークとなったことで、アプリケーションとデータは至る所に存在するようになりました。その結果、可視性と制御性が損なわれ、攻撃者はその空隙を狙っています。

それに加えて、スキル不足が引き続き大きな問題となっています。セキュリティ関連の支出は全体的に堅調なため、大企業が有利な状況にあることは確かですが、多くの組織ではセキュリティチームに十分な資金と人員を割り当てられていません。ESG の調査によると、サイバーセキュリティへの支出を増やす予定のある企業は、他のどの技術分野よりも多い（69%）ことが分かっています。しかし同時に、半数近くの組織（48%）が社内のスキル不足が問題であると報告しており、これも他のどの技術分野よりも多くなっています[7]。大規模な組織であっても、セキュリティに特化した人材はほんの一握りしか採用できていません。ノイズの多いセキュリティツールは正確性やコンテキストに乏しいアラートを大量に生成するため、人員不足の IT チームが効率的に作業を進めることは困難です。その結果、セキュリティチームは次から次へと問題に取り組まなければならなくなり、最終的にはセキュリティの有効性が失われ、攻撃者に優位な立場を与えてしまいます。

HEAT 攻撃を阻止するために

サイバーセキュリティに特効薬はありません。攻撃者は、防御システムを出し抜くために戦術を進化させ続けるでしょう。これは一般的にもそうですが、特に HEAT 攻撃について当てはまります。組織がこの種の攻撃への耐性を高めるためには、3 つの原則に従う必要があります。

組織がこの種の攻撃への耐性を高めるためには、3 つの原則に従う必要があります。それは、考え方を検知から予防へと転換すること、脅威がエンドポイントに到達する前に阻止すること、高度なアンチフィッシングおよびアイソレーション機能を組み込むことです

それは、考え方を検知から予防へと転換すること、脅威がエンドポイントに到達する前に阻止すること、高度なアンチフィッシングおよびアイソレーション機能を組み込むことです。

確実な検知のためには、死角のない包括的な可視性、さまざまなソースにまたがる相関性の高いデータ、インシデント発生時に即座に対応できる能力が必要になります。しかし最も洗練された組織でも無い限り、これは非常に高い目標です。そのため、脅威が発生してから対応するのではなく、デバイスやシステムに影響が及ぶ前に、できるだけ多くの脅威を防ぐことに目標を定める必要があります。ゼロトラストに広く関心が集まっているのは、このような背景によるものです。複雑さと多様性が増しているため、影響の範囲を限定し、環境から暗黙の信頼を取り除くことが、これまで以上に重要になってきています。予防の考え方に転換し、ゼロトラストの原則を取り入れることで、セキュリティチームは「消火」という考え方から脱却し、脆弱性の特定と緩和、設定の堅牢化、脅威ハンティングによって、組織のセキュリティ体制をプロアクティブに強化することに集中することができます。

[7] 出典： ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021.

そこで、次の疑問が生じます：予防はどこで行うべきなのでしょうか? 従業員やリソースが高度に分散しているため、防御も分散させることが重要です。同時に HEAT 攻撃は、デバイス上でマルウェアを組み立てることでエンドポイントツールを回避するように設計されているため、多くの場合配信後に対応することができません。このような攻撃からユーザーを守るためには、クラウドベースで Web に主眼を置いた保護が最も理にかなっていると考えられます。しかしセキュリティチームは、これらのツールを慎重に評価する必要があります。従来オンプレミスに導入されていたセキュア Web ゲートウェイ（SWG）は、利用規定の適用に重点を置き、シグネチャベースの脅威防御に依存し、アプリケーションに対する可視性が低いため、HEAT 攻撃を防ぐことはできません。セキュリティチームは、アプリケーションのきめ細かい可視化と制御、インラインのコンテンツ検査、および HEAT 攻撃を事前に阻止するための高度な脅威防御機能を提供できる、最新のクラウドネイティブな SWG を探す必要があります。

最後に、高度なアイソレーションとフィッシング対策を含む防御機能が不可欠です。脅威の中にはシグネチャや分析によって防ぐことができるものもありますが、HEAT 攻撃に対抗するためにはさらなる防御層が必要です。ブラウザーとエンドポイントの間を分離することで、HEAT のようなステルス型の脅威が足場を固めることができないようにできます。同様に、フィッシング脅威が従来のメールという経路を超えて拡大していることから、Web やソーシャルメディア、SMS を経由した攻撃に対する一貫した保護がますます重要になっています。

大きなトレンド

他のビジネスや業界と同様、サイバー犯罪者も全体のトレンドや市場力学の変化に応じて、革新的で適切な技術を常に探し求めています。リモートワークやハイブリッドワークへの移行、クラウド導入の加速により、多くのユーザーの日常業務が変化し、そのほとんどがブラウザーを中心としたものとなっています。攻撃者の立場からすれば、多くの魚が泳いでいるところに釣り糸を垂れることは当然です。

HEAT 攻撃は、従来型のセキュリティ防御との間に生じる間隙を侵害するための攻撃技術の重要な進化を象徴しています。最も有名なハッカー集団が、すでにランサムウェアやその他の高度な攻撃にこれらの技術を使用しているという事実は、攻撃者がいかに機敏であるかを示しており、セキュリティチームはそれに迅速に対応しなければなりません。これらのことを念頭に置き、セキュリティリーダーは HEAT 攻撃から身を守るために、予防、エンドポイントから離れた場所での分散した保護、高度なアンチフィッシングおよびアイソレーション機能に取り組む必要があります。

Enterprise Strategy Group は、IT 分析/研究/検証/戦略立案を行う会社であり、グローバル IT コミュニティにマーケットインテリジェンスと実用的なインサイトを提供しています

www.esg-global.com contact@esg-global.com 508.482.0188