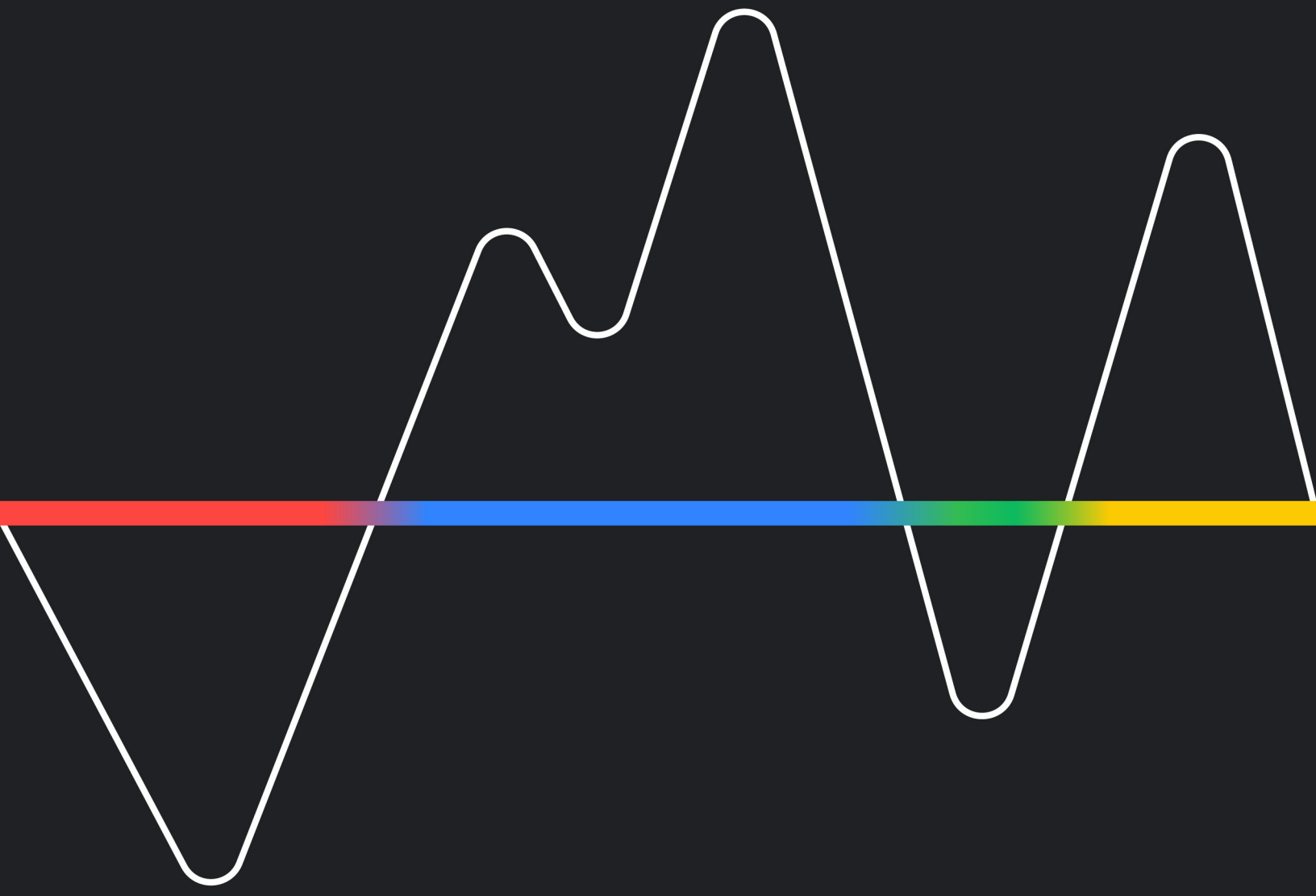
Mandiant

Google Cloud Security

# M-Trends

## 2026 レポート

エグゼクティブ エディション



# M-Trends 2026 エグゼクティブ エディション

## 前書き

M-Trends は Mandiant が 2025 年に実施した 50 万時間以上にわたるインシデント調査に基づき、脅威活動と侵害行為で使用された戦術を明確に分析したレポートです。Google Threat Intelligence Group (GTIG) と協力し、現代の脅威ランドスケープと将来の攻撃につながる新たな脅威の全体像を包括的に把握することができました。

最近の GTIG のレポートによると、攻撃者の AI 導入が進んでいることがわかっています。脅威アクターは大規模言語モデル（LLM) を使用して、高度にパーソナライズされたソーシャル エンジニアリング、実行中に LLM にクエリを送るマルウェアによる検知の回避、各社独自の機械学習ロジックを標的とした「蒸留攻撃」を行っています。Mandiant のレッドチームでは、このような脅威に備える組織の取り組みに AI を活用した手法を採用していますが、M-Trends 2026 の調査結果によると、セキュリティ侵害を許すような人為的ミスやシステム障害を軽減することがミッション クリティカルであることがわかっています。

2025 年のインシデント対応からわかった重要なポイントは、攻撃者のうち特定のグループが比較的長期間ネットワーク上で検知されずに活動しており、その多くは、通常標準的なテレメトリーを備えていないエッジデバイスで永続性を確立していることです。Mandiant が 2025 年に、この種のインシデントに相当数対応した結果、世界全体における滞留時間の中央値が前回の報告期間の 11 日から 14 日に上昇したことがわかりました。この上昇の大部分が長期間のスパイ行為と北朝鮮の IT ワーカーの活動に起因するものです。

また、スピードを優先する脅威グループもあります。闇市場でアクセス権を売買するのではなく、初期アクセス パートナーが二次グループと直接連携する傾向が高まっています。そのためアクセス権の「ハンドオフ」が 30 秒以内に行われることもあり、「軽微な」アラートが瞬時に大規模な侵害インシデントになる可能性も出てきました。

同時に、攻撃者はバックアップ、ID サービス、仮想化レイヤなどのインフラストラクチャを組織的に攻撃対象とすることで、復旧を阻止し、身代金を支払うか、復元不可能となるリスクを負うかの選択を迫ります。

真のオペレーショナル レジリエンスを構築するには、企業は攻撃者に負けないスピード感で取り組む必要があります。そのためには、攻撃者がどのようにして侵害に成功しているかを理解することが重要です。可視性のギャップを埋め、M-Trends 2026 で詳述されている防御策を導入することで、企業は事後対応としての復元から、予防的な封じ込めへと転換し、軽微なアラートが壊滅的な侵害へと発展するのを防ぐことができます。

# 数値で見る被害の統計

M-Trends 2026 で報告されている指標は、2025 年 1 月 1 日から 2025 年 12 月 31 日の間に行われた標的型攻撃アクティビティを Mandiant Consulting が調査した内容に基づいています。

## 重要なポイント

攻撃者が戦略を転換しつつあるものの、初期アクセスの方法として依然としてエクスプロイト（脆弱性の悪用）が最も一般的です。一方、インタラクティブ性の高い音声ベースのソーシャル エンジニアリングが次点にまで増加しています。同時に、世界全体における滞留時間の中央値が増加しています。これは、高度なスパイ行為を行うグループやインサイダー脅威がステルス性の高い長期的なアクセスを優先するようになったためです。攻撃者は AI の武器としての活用、エッジデバイスのゼロデイ脆弱性の悪用、初期アクセス パートナーとサイバー犯罪グループの間でのアクセス権のハンドオフの機会を求めているため、企業は静的なセキュリティ対策を進化させ、継続的に ID の動作と、従来 EDR や同様のセキュリティ ツールの対象外だった仮想化などのインフラストラクチャを監視する必要があります。

## 知っておくべきこと

- 金銭目的のグループは、2025 年の調査で判明した脅威クラスタのうち 41% を占め（2024 年の 55% から減少）、サイバー エスピオナージは 16%まで増加（前年 8%）しました。
- 初期感染ベクトルとして最も多かったのは、6 年連続でエクスプロイト（32%）でした。ビッシングが 11% に急増し、2 番目に多いベクトルになっています。一方、メール フィッシングは減少を続けており、2024 年の 14% から、2025 年には 6% まで減少しました。メール フィッシング、ビッシングはともに広義のソーシャル エンジニアリングの一種ですが、防御にあたってはこの 2 つを区別することが不可欠です。インタラクティブな攻撃は、自動化された技術的な制御よりもはるかにレジリエンスが高く、異なる検出戦略が必要だからです。
- ランサムウェア関連のインシデントでは、過去の侵害が初期感染ベクトルとして最も多く観測され、その割合は 30% でした。脅威クラスタの一部は、大量の日和見的な感染ベクトルによって多くの組織において初期の足掛かりを築くことに注力しています。確立したアクセス権は他の脅威クラスタに売却または引き継ぎされ、侵害後に悪用されます。
- 最も標的とされやすい業界は、ハイテク、金融、商業、プロフェッショナル サービス、医療で、インシデント全体では 16 以上の業種が影響を受けています。特筆すべきなのは、ハイテク業界での調査結果が、2023 年、2024 年に最も大きい割合を占めていた金融業界を上回ったことです。
- 2025 年の調査全体では、悪意のあるアクティビティを内部で発見した事例の割合は 52%（2024 年の 43% から増加）であるのに対し、外部機関から指摘を受けるまで認識していなかった事例は 34%（43% から減少）でした。組織が攻撃者から侵害の通知を受けた事例は 14% でした。
- ランサムウェアの場合、攻撃者から通知を受けた事例の割合は 44% で、内部での発見が 41%、外部機関からの通知が 15% でした。攻撃者からの通知の割合が顕著に高いのは、ランサムウェアのビジネスモデルと整合しています。
- 全世界での滞留時間の中央値は、2024 年の 11 日間から 14 日間に増加しました。2024 年と 2025 年の分布を比較すると、1 週間以内に発見されたインシデントがわずかに減少し、滞留時間が長くなっている（1 週間～6 か月）傾向がわかります。この傾向はサイバー エスピオナージと北朝鮮の IT ワーカーによるインシデントの増加を反映したものです。これらの脅威クラスタはステルス性、長期的なアクセスの維持を優先するため、滞留時間の中央値は 122 日です。
- 2025 年の調査では、マルウェア ファミリーのうち バックドアが 36%、ダウンローダが 11%、ランサムウェアとドロッパーがそれぞれ 10%、認証情報の窃取が 9% でした。
- Mandiant の調査において 5 年連続で最も頻繁に観測されていたマルウェア ファミリーの Cobalt Strike BEACON は、4 位に転落しました。最も頻繁に観測されたマルウェア ファミリーは GOLDVEIN.JAVA ダウンローダで、次点が REDBIKE（Akira）ランサムウェアでした。
- 脅威クラスタは、EDR をサポートしていないアプライアンス上でステルス性の高い戦術と軽量なマルウェア（例: BRICKSTORM バックドア）を使用しています。金銭目的のグループとサイバー エスピオナージ グループの両方が、オンプレミス環境とクラウド環境でネイティブ機能や正規ツールを不正使用することで、検知される可能性を低減しています。

- 脅威クラスタは、偵察、ソーシャル エンジニアリング、マルウェア開発の生産性の向上のために AI ツールを採用することが増えています。さらに、攻撃者は侵害した環境で AI を攻撃の道具としています。たとえば、認証情報窃取ツールである QUIETVAULT は、標的のマシンの AI CLI ツールを悪用し、事前定義されたプロンプトを実行して構成ファイルを探します。

# 必要とされる行動

- **従来のエンドポイントを超えて可視性を拡大:** エコシステム全体にわたって高度な脅威検知をデプロイします。特に、EDR のないエッジ アプライアンス向けにネットワーク トラフィックの分析を組み込み、仮想化インフラストラクチャを対象とした厳格なテレメトリーを適用します。
- **インターネット経由の攻撃経路の管理を徹底する:** エクスプロイトは 6 年連続で初期感染ベクトルの最上位を維持しています。そのため、組織は迅速なパッチ適用、脆弱性スキャン、ゼロデイ キャンペーンと N デイ キャンペーンの対象になりがちな外部と接するウェブ アプリケーション サーバーの厳格な分離を優先する必要があります。
- **セキュリティ意識向上トレーニングの対象をメール以外にも拡大する:** メール フィッシングは依然として脅威アクターの定番ではあるものの、その他の初期感染ベクトルを使用する脅威アクターが増加していることもわかっています。たとえば、インタラクティブなビッシング、認証情報窃盗、ClickFix のような戦術があります。従業員と IT ヘルプデスクのスタッフを教育します。特に、音声ベースのソーシャル エンジニアリング、メッセージ アプリへの仕掛け、不正な MFA の再設定リクエストについて教育します。
- **継続的な ID 検証への移行:** インタラクティブなソーシャル エンジニアリングでは従来の MFA を回避することが多く、北朝鮮の IT ワーカーなどさまざまな脅威アクターは長期間のアクセスを維持しようとします。そのため、付与する権限は厳格に最小限として、定期的に SaaS / クラウドのインテグレーションを監査し、従業員やリモートの契約社員の ID について異常な行動がないか先回りで探し出す必要があります。
- **IR プレイブックを最新の恐喝の手口に対応して更新する:** インシデント対応と復元に関する計画で、暗号化ベースのランサムウェアと純粋なデータ窃取による恐喝の両方に対応できるようにします。日和見的な感染の検知に焦点を当てた机上演習を実施して、対応時間の短縮と、初期アクセス パートナーから二次グループへのアクセス引き継ぎの防止ができるようにします。
- **安全な開発環境と AI ツールチェーン:** 脅威クラスタは侵害された環境で AI を武器化していることがわかっています。マルウェアが正当なローカルの AI コマンドライン ツールを悪用して GitHub や NPM のトークンを見つけて盗む事例が見つかっていることから、組織は Google セキュア AI フレームワーク（SAIF）の原則を導入する必要があります。具体的には、「検知と対応機能を拡張」して脅威モデルに AI ツールを組み込むことで、セキュリティ チームは行動のベースラインを確立し、これらのユーティリティに起因する異常なプロンプトや不正なデータ盗難を監視します。
- **レッドチームを起用して最新の脅威をエミュレーションする:** 最新の攻撃戦術を現実の環境に即してエミュレーションし、防御システムを定期的にテストします。セキュリティ チームが環境寄生型の手法、エッジデバイスのエクスプロイト、インタラクティブなソーシャル エンジニアリングを検知して対応するまでの時間を測定します。

# 軽微な感染が呼び込む ランサムウェア攻撃

## 重要なポイント

サイバー犯罪者間の密な連携で防御の隙がなくなり、1 つのグループが日和見的な初期アクセスをしてから二次脅威グループがアクセスできるまでの時間の中央値が、以前は 8 時間近かったものが 22 秒まで短縮されました。この変化により、組織は、影響の少ないアラートでも重要な指標として扱い、影響の大きいアクターがアクセスを悪用できるようになる前に即座に修復する必要に迫られています。

## 知っておくべきこと

- **「ハンドオフ時間」の消滅:** 初期アクセス イベントから二次脅威グループへのハンドオフのの時間の中央値は、2022 年の 8 時間以上から、2025 年には 22 秒まで減少しました。この減少が意味するのは、初期アクセスを担当する脅威グループが、確立したアクセスを後でアンダーグラウンド チャネルで売買するのではなく、二次グループと直接連携して即座に使用するようになっているということです。
- **影響が小さい侵入でも影響の大きい攻撃の先駆けの可能性がある:** 脅威アクターは分業モデルを採用しており、専門のグループが足掛かりを築くために悪意のある広告（マルバタイジング）や偽のブラウザ アップデートなどの影響の小さい手法を用いています。これらの初期ベクトルは影響の小さなマルウェアに見えるため、影響の大きい攻撃のみにターゲットを絞っている組織では見落とされがちで、手遅れになってしまうこともあります。
- **パートナーによる事前準備:** 初期アクセス パートナーは、単に闇市場でアクセス手段を販売するのではなく、最初の感染の段階で二次グループの使用したいマルウェア、トンネル、バックドアを準備します。闇市場を回避し、事前に環境を構成することで、その後の攻撃者は都合のよいタイミングで確立された足場を使用できるようになります。つまり、最初にネットワークにアクセスした瞬間には影響の大きなオペレーションを実行する準備が整っているということです。

## 必要とされる行動

- **影響の小さいアラートを重要な指標とする:**
  初期感染での重要度の低さとその潜在的な影響の大きさに乖離があるため、対応プレイブックを再構築する必要があります。セキュリティ チームは日常的なマルウェア アラートを、二次グループへの引き継ぎが差し迫っている優先度の高い指標として取り扱わなければなりません。
- **事前に承認されたツールの基準を適用する:**
  IT チームやセキュリティ チームは事前承認済みの一元的に保存されたユーザー向けツールを定義してデプロイする必要があります。それにより、管理されていないインストールにわずらわされることが減り、通常動作からの逸脱をすばやく見つけて対応できます。
- **イベント相関とコンテキストを最適化する:** 防御のワークフローの焦点を個々のアラートの確認からイベント相関に移す必要があります。アラートにコンテキスト データを追加することで、アナリストは大きな影響を与える可能性のある侵入が進行していることを示す行動パターンを見つけられます。
- **インタラクティブなアクティビティが開始される前に修復する:**
  防御者の目標は、初期アクセス段階（非インタラクティブなイベントであることが多い）で、二次グループがキーボード操作を開始する前に侵入を修復することです。攻撃が単一のシステム上にとどまっている段階で阻止することは、その後の影響の大きいアクティビティから回復を試みるよりはるかに効果的です。

# ランサムウェアはもはや レジリエンスの問題

## 重要なポイント

ランサムウェア グループは現在では単にデータを暗号化するだけではありません。復元の能力を破壊しようとしてきます。最も重要なシステムを標的とすることで、身代金を払うか、再構築するかの選択を効果的に迫ります。現在、真のレジリエンスとは、復元ツールがセグメント化され、保護されるようにネットワークを設計することを意味します。コアシステムへのアクセスを制限して攻撃者のネットワーク内での行動を困難にすることで、セキュリティ チームが最新のランサムウェアの脅威に優位に対抗できるようにします。

## 知っておくべきこと

- **ランサムウェアは復旧不能に進化:** ランサムウェアのオペレーターの第一目標は、単純なデータ窃取から復旧不能へと移行しています。現在、攻撃者はシステムと管理の経路、特に、ID サービス、仮想化管理プレーン、バックアップ インフラストラクチャを標的とすることで、組織の復元能力を低下させ、身代金を支払わざるをえない状況へと追い込もうとします。
- **ID が新しい境界:** 高度な脅威グループは ID コントロール プレーンを操作して、標的環境を完全に制圧します。攻撃者が構成ミスを悪用して証明書を発行し、管理者アカウントを作成して、多要素認証（MFA）とパスワード ローテーションを回避する事例も確認されています。攻撃者はデータベース全体を盗むか、クラウド テナントを侵害してインフラストラクチャ バックエンドを破壊することで、危機発生時に防御者が緊急アカウントを使用できないようにするケースもあります
- **従来のセーフティ ネットは破壊されつつある:** 攻撃者は積極的にバックアップ アーキテクチャを探して破壊しようとしているため、バックアップ頼りの戦略は機能しません。脅威アクターは偵察を行って保存場所をマッピングし、暗号化の設定を取得してから、クラウド ストレージとローカル システムからバックアップ オブジェクトを体系的に削除します。オンプレミスでは、攻撃者が仮想化環境をバックアップ プラットフォームから切り離したり、ローカルの復旧ポイントを暗号化したりする事例が確認されており、その結果、標準的なインシデント対応プレイブックを実行するために必要なツールが利用できなくなるため、ハンドブックが用をなさなくなってしまいます。

# 必要とされる行動

- **必要最小限のセキュリティ水準を引き上げる:** 組織は ID を第一の境界として扱う必要があります。これには影響が大きい経路を強化する必要があります。そのために、特権 ID 管理と条件付きアクセスを実装して、管理者権限に時間制限と監視を課します。セキュリティ チームはすべてのアクセスに MFA を適用し、セキュリティ強化された特権アクセス ワークステーションを活用して、サービス プリンシパル名を監査します。テレメトリーは、「環境寄生型（LotL）」の動作を検知して、環境に広範な影響を与える前に管理者の乗っ取りを特定できるように調整する必要があります。
- **重要なティア 0 のコントロール プレーンを隔離:** 仮想化と管理プラットフォームは最も厳格なアクセス制限が課せられた「ティア 0」アセットとして取り扱う必要があります。組織はゼロトラスト セグメンテーションを導入してこれらのシステムを隔離し、正式に Active Directory（AD）との統合を切断し、単一の ID の侵害によって大量の暗号化が発生しないようにする必要があります。ローカルの MFA で保護されたアカウントを使用して専用の帯域外管理を活用し、構造的に分離して、本番環境の機能とリカバリー環境の機能の両方が同時に失われることがないようにします。
- **復元パスの信頼性を向上:** 復元機能は、本番環境が侵害されても維持される必要があります。組織は専用の分離されたリカバリー環境を確立する必要があります。その環境において、システムの復元をクリーンアップ、検証、段階的に準備することで、再感染のループを軽減します。これには、本番環境ネットワークの影響を受けない、オフラインまたは不変のティア 0 アセット（具体的には、ID とバックアップのカタログ）を維持する必要があります。障害復旧計画には、プライマリ ID ファブリックが完全に失われた場合について、明示的に記載する必要があります。

# 数年にわたる侵入で判明した著しく高い永続性

## 重要なポイント

侵入阻止が理想ではありますが、準備はしておかねばなりません。高度な脅威アクターは、監視が手薄な箇所や管理者への信頼を巧妙に利用することで、数年にわたってアクセスを維持しています。ロギングのギャップのために侵入範囲を証明できない場合、最悪のケースではデータが窃盗されたものとして公表しなければならないため、顧客の信頼を失うリスクがあります。可視性を継続的な監査とみなし、管理不能な危機に陥る前に、これらの脅威を検知して修復できるようにします。

## 知っておくべきこと

- **浸透するステルス性と永続性:** 脅威アクターの中には 1 年を超える滞留時間を達成しているものもあります。多くの場合は、独自開発のマルウェアではなく、正規の認証情報を不正利用した結果です。仮想化インフラストラクチャや管理されていないエッジデバイスを標的として、組み込みのツールを使用して、標準の管理アクティビティに紛れ込み、検知を回避します。
- **重大な可視性のギャップ:** 現在のロギング戦略では、これらの侵入についての全体像を把握することはできません。BRICKSTORM（ステルス型バックドア）が使用されたケースでは、滞留時間が平均で 393 日と長く、標準的なログの保持期間が 90 日の組織では、初期アクセス ベクターを特定できません。さらに、EDR への依存により監視が手薄になる箇所が生まれます。これは、アクターが標的とするのは、ネットワークのエッジ アプライアンスと認証プロトコルで、エンドポイント エージェントからは管理できないためです。
- **アンチフォレンジックが対応を阻む:** 巧妙なアクターはインシデントのスコープを調べるのに必要な証拠を破壊することが観察されています。ファイルの変更を隠す手法を採用し、システムログを消去することで、脅威アクターはデータ窃取のタイムラインの再現をほぼ不可能にします。決め手となるフォレンジック調査を踏まえた決定的な証拠がない場合、最悪のシナリオでの侵害を受けたと想定して公表せざるを得ないため、組織は厳しい制裁を受け、評判が失墜するリスクがあります。

## 必要とされる行動

- **ログの保持期間と範囲を拡大:** 巧妙な脅威アクターの中には滞留時間が長期間に及ぶ場合もあるため、標準の 90 日間の保持ポリシーでは侵入の範囲を特定するのに不十分です。組織はログを一元管理された長期保持できるストレージに転送することを優先する必要があります。具体的には、標準的な EDR ツールが見落としがちな、ネットワーク エッジデバイス、ハイパーバイザ、認証プロトコルなどの監視が手薄な部分からデータを収集する必要があります。
- **ログの整合性を確保:** ローカルなログの消去やタイムスタンプの改ざんなどのアンチ フォレンジックな手法に対抗するには、ログを一元管理された場所に即座に転送することを優先します。これにより、ホストが侵害された場合でも、証拠が保全されます。さらに、リポジトリを構成して、予期しないログの終了についてアラートを発行します。それにより、攻撃者が攻撃の痕跡を隠すために意図的にセキュリティ管理を無効にしたときに、運用チームがそれを特定できるようになります。
- **プロアクティブな脅威ハンティングに移行:** セキュリティ チームは事後対応のアラートから前進して、プロアクティブな脅威ハンティングをルーティンとして取り入れる必要があります。これには、承認済み動作の外れ値の識別を目的とした、スタック ランキング データなどの高度な分析手法の使用が含まれます。最新の脅威インテリジェンスを取り込むことで、害のない管理アクティビティと、ネイティブ ツールを使用して無害を装った攻撃者とを区別できるようになります。
- **アセットと前提を検証:** リーダーは、セキュリティ チームとインフラストラクチャ チームの連携を徹底させ、環境を監査する必要があります。定期的に前提をテストして、重要なアセットが想定されるテレメトリーを実際に生成しているかを確認します。また、このプロセスによって、使用されていないテクノロジーやシステムを特定して削除することで、管理上の負荷を軽減し、攻撃対象領域を縮小します。

# 攻撃者に狙われる 仮想化インフラストラクチャ

## 重要なポイント

仮想化プラットフォームはバックエンド インフラストラクチャから主なターゲットへと変化しています。攻撃者はハイパーバイザの「ティア 0」の性質を悪用することで、ゲストレベルの防御を無効化し、標準的な修復に耐える高度な永続性を確立して、従来の復元が不可能になるレベルのランサムウェアをデプロイします。このプラットフォームを保護するには、管理プレーンを隔離された重要アセットとして取り扱い、ログの取得が難しい箇所がなくなるように可視性を回復する必要があります。

## 知っておくべきこと

- **ハイパーバイザはセキュリティが手薄:** ハイパーバイザでは独自のオペレーティング システムを実行していることも多く、標準の EDR ツールとは互換性がありません。そのため、可視性のギャップが生まれ、攻撃者はそれを狙ってマルウェアをデプロイ、または管理されていない仮想マシンを作成し、EDR や SIEM のアラートを起動することなく、段階的な攻撃を実施します。
- **攻撃者はゲスト防御を回避:** 巧妙な攻撃者は、データ窃取のために標的のシステムにログインすることすら不要にしています。仮想化ストレージ レイヤを直接標的とすることで、仮想ディスクのクローンを作成し、ゲスト オペレーティング システムやそのセキュリティ管理を操作することなく、機密性の高い Active Directory データベースを抽出することができます。
- **ランサムウェアの現在の標的はデータストア:** 現在のランサムウェア キャンペーンは、下位のレイヤを標的として、個々のマシンではなく、ハイパーバイザのデータストアを暗号化します。この戦術により、脅威アクターはホスト上のすべてのサーバーを同時にシャットダウンしてロックし、すべての関連する仮想マシンを操作不能かつ修復不可能にしておとしいれます。
- **攻撃者が高度な永続性を確立:** 攻撃者はハイパーバイザの基盤となるシェルを標的として、隠しバックドアや不正な仮想マシンをデプロイするようになっています。これらのメカニズムは標準的なサーバー環境の下位層で実行されるため、通常、標準的なインシデント修復作業やシステムの再起動をすり抜けて存続し、攻撃者に永続的なバックドアへのアクセスを提供します。

## 必要とされる行動

- **ID と管理を分離:** 企業の Active Directory ドメインからハイパーバイザとバックアップ インフラストラクチャを削除します。本番環境とインフラストラクチャの両方で同じ ID プロバイダを使用しているため、単一障害点となります。インフラストラクチャ専用の ID プロバイダ（IdP）をデプロイするか、ジャストインタイム（JIT）アクセスを適用します。
- **管理プレーンを隔離:** 仮想化インターフェースをティア 0 アセットとして扱います。管理トラフィックをセキュリティ強化された特権アクセス ワークステーション経由でのみアクセス可能な、専用のファイアウォール ネットワーク セグメントに制限し、フィッシング耐性の高い MFA を適用します。
- **不変なレジリエンスを適用:** 復元機能の破壊に対抗するには、バックアップ環境を隔離し、不変ストレージを使用する必要があります。このようなエアギャップのあるコピーで定期的に復元テストを実施し、切迫した復元イベントにおいて意図したとおりにバックアップが機能するかを検証する必要があります。
- **インフラストラクチャ テレメトリーを一元管理:** 仮想化管理とハイパーバイザ レベルのログを中央の SIEM に転送するよう義務付けます。攻撃者はゲスト オペレーティング システムを回避しているため、現時点ではハイパーバイザ テレメトリーが、未承認のアクセス、スナップショット操作、不正な仮想マシンの作成を検出する唯一の方法です。

# 組織的な不正使用:
# エッジデバイスとコア ネットワーク デバイス

## 重要なポイント

攻撃者は、エッジおよびコアネットワーク機器を武器化しての道具として、最新のセキュリティ ツールを回避しています。パッチがリリースされるよりも速く脆弱性を悪用し、デバイスのネイティブ機能を不正に利用して密かにデータを盗みます。これらの重要なゲートウェイはカタログ化されず、監視もされないことが多いため、検出されない長期間のアクセスを攻撃者に許すことになります。組織は緊急で包括的なアセット検出、厳格なパッチ管理、一元的なロギングを優先し、ネットワーク境界の制御を回復する必要があります。

## 知っておくべきこと

- **ゼロデイ攻撃が加速している:** 脆弱性が悪用されるまでの平均時間は激減しました。これは、ベンダーがパッチをリリースする前に、脅威アクターがエッジデバイスとコア ネットワーク デバイスを含むシステムを侵害するケースが増えているということです。
- **ネットワーク デバイスはセキュリティの監視が手薄になっている:** エッジ アプライアンスでは従来の EDR ソフトウェアを実行できないため、攻撃者は安全な隠れ蓑として利用しています。攻撃者は、テレメトリーが脆弱な環境で検知を回避して存続する、独自のインメモリ マルウェアをデプロイしています。
- **攻撃者はエンドポイントを回避している:** 高度な攻撃者は、偵察からデータ窃取に至るまで、攻撃ライフサイクルのほぼ全体を、ネットワーク インフラストラクチャ上で直接実行し、監視が行き届いたワークステーションやサーバーは完全に回避します。
- **インシデント対応が著しく阻害されている:** エッジデバイスには最小限のストレージしかなく、厳格な稼働時間要件があります。侵害が発生したとき、標準のファイル システム フォレンジックは不可能な場合が多く、証拠が失われる前に攻撃の存在を確認するのが難しくなっています。
- **攻撃者はネイティブ機能を攻撃の道具とする:** 攻撃者は組み込みの管理者用サブシェルと、ネイティブのパケット キャプチャ機能を使用して、デバイスを通過するライブ トラフィックのコピーを収集します。これにより、攻撃者はクリアテキスト ネットワーク プロトコルからパスワードを抽出し、防御を回避して操作できるため、検知される可能性のあるマルウェアをデプロイする必要がありません。

## 必要とされる行動

- **ネットワーク ログを一元化して保持:** エンドポイントのデータのみに依存しないでください。アプリケーション ログや管理ログなど、重要なネットワーク デバイスログを一元化された SIEM に転送し、管理ログは最低でも 1 年間保持することで、調査時の可視性を確保します。
- **厳格な脆弱性の管理を徹底:** ネットワーク デバイスを包括的な脆弱性スキャンとアセット管理プログラムに統合します。明確な責任範囲を確立し、段階的なパッチ適用スケジュールを作成することで、攻撃者が悪用する前に、ビジネス運営を中断することなく欠陥を修復します。
- **ネットワークに特化したインシデント対応ハンドブックを作成:** セキュリティ チームは詳細なアーキテクチャ図と対応ハンドブックを作成します。フォレンジック データの収集手順を事前に計画することで、重要な揮発性の証拠が、標準的な再起動または電源再投入イベントで破壊されないようにします。
- **カタログ化されていないネットワーク インフラストラクチャを特定:** エッジ アプライアンスは頻繁にデプロイされ忘れられがちなため、セキュリティ チームは包括的な検出スキャンを使用して、カタログ化されていないシステムを特定する必要があります。組織は存在を知らないアセットを防御、パッチ、監視することはできません。

# 連鎖的な影響:
# サードパーティの SaaS の侵害

## 重要なポイント

クラウド ファーストのインフラストラクチャへの移行により、SaaS アプリケーションは大規模なサプライ チェーン攻撃への経路となっています。脅威アクターは統合トークンを盗み、未検証のサードパーティ アプリケーションを悪用することで、標準の防御を回避し、単一ベンダーの侵害から連鎖的に企業を危機に追い込みます。組織は継続的な ID 検証に移行し、エンドユーザー アプリケーションの同意を厳密に管理して、調達の前に、厳格なサードパーティのリスク管理を徹底する必要があります。

## 知っておくべきこと

- **MFA が回避される:** 攻撃者はただパスワードを盗むのではなく、有効期間の長い OAuth トークンやセッション Cookie を収集しています。これらはログアウト後も有効になっていることが多いため、攻撃者は MFA アラートを発生させることなく、セッションを乗っ取ることができます。
- **SaaS 間連携が新たな境界 (ペリメター) に:** 脅威アクターは、サードパーティの SaaS ベンダーを侵害して、ハードコーディングされたキーや、個人のアクセス トークンを盗み、その盗んだシークレット情報を使用して、ダウンストリームの顧客の環境にシームレスに侵入することで、大規模なデータ窃盗を実行します。
- **ソーシャル エンジニアリングが増加:** 金銭目的のグループは IT ヘルプデスクを標的とした、音声ベースのフィッシング (ビッシング) を積極的に行っています。攻撃者は従業員になりすまして管理機能を回避し、SaaS への初期アクセスを獲得して、高い権限を持つキーを環境から探し出します。

## 必要とされる行動

- **SaaS 資産を検出して管理:** 従来のアセット管理では、クラウド アプリケーションを見落としがちになります。SaaS セキュリティ ポスチャー管理 (SSPM) ツールをデプロイして、すべてのアプリケーション、インテグレーション、隠されたシークレット情報 (API キーなど) を積極的に調査することで盲点を排除します。
- **ID 管理を強化:** すべての SaaS アプリケーションを中央 ID プロバイダ (IdP) 経由でルーティングするよう義務付けます。サードパーティの API キーには最小権限の適用を徹底し、ワイルドカード権限を排除して、ジャストインタイム (JIT) アクセスを活用して常設特権を最小限に抑えます。
- **ライフサイクル管理を自動化:** すべてのシークレットとサービス アカウントの認証情報に自動ローテーションを実装します。アクセス トークンとブラウザのセッションの有効期限を極端に短くすることで、盗まれた Cookie がダークウェブで販売される際の価値を瞬時に下落させます。
- **エンドユーザー アプリケーションの同意をロックダウン:** 管理者は、エンドユーザーが承認されていないサードパーティのアプリケーションに同意する機能を無効にする必要があります。これにより、検査済みのアプリケーションのみが永続的なトークンを取得でき、環境へのアクセス権を得ようとする悪意のある OAuth アプリケーションを効果的にブロックします。
- **厳格なベンダーリスク管理を徹底:** サードパーティのアプリケーションで許容されたリスクは、本番環境のコア部分に対するリスクとなります。組織は堅牢なサードパーティ リスク管理プログラムを実装して、ベンダーをオンボーディングの前に審査し、シングル サインオン、詳細な監査ログ、安全な開発手法などの機能を調達プロセスの一部として義務付けます。

**レポート全文をダウンロード。**

サイバー インシデントが疑われる場合や、セキュリティ侵害が発生した場合は、Mandiant のインシデント対応サポートにお問い合わせください。

Google Cloud

詳細: cloud.google.com