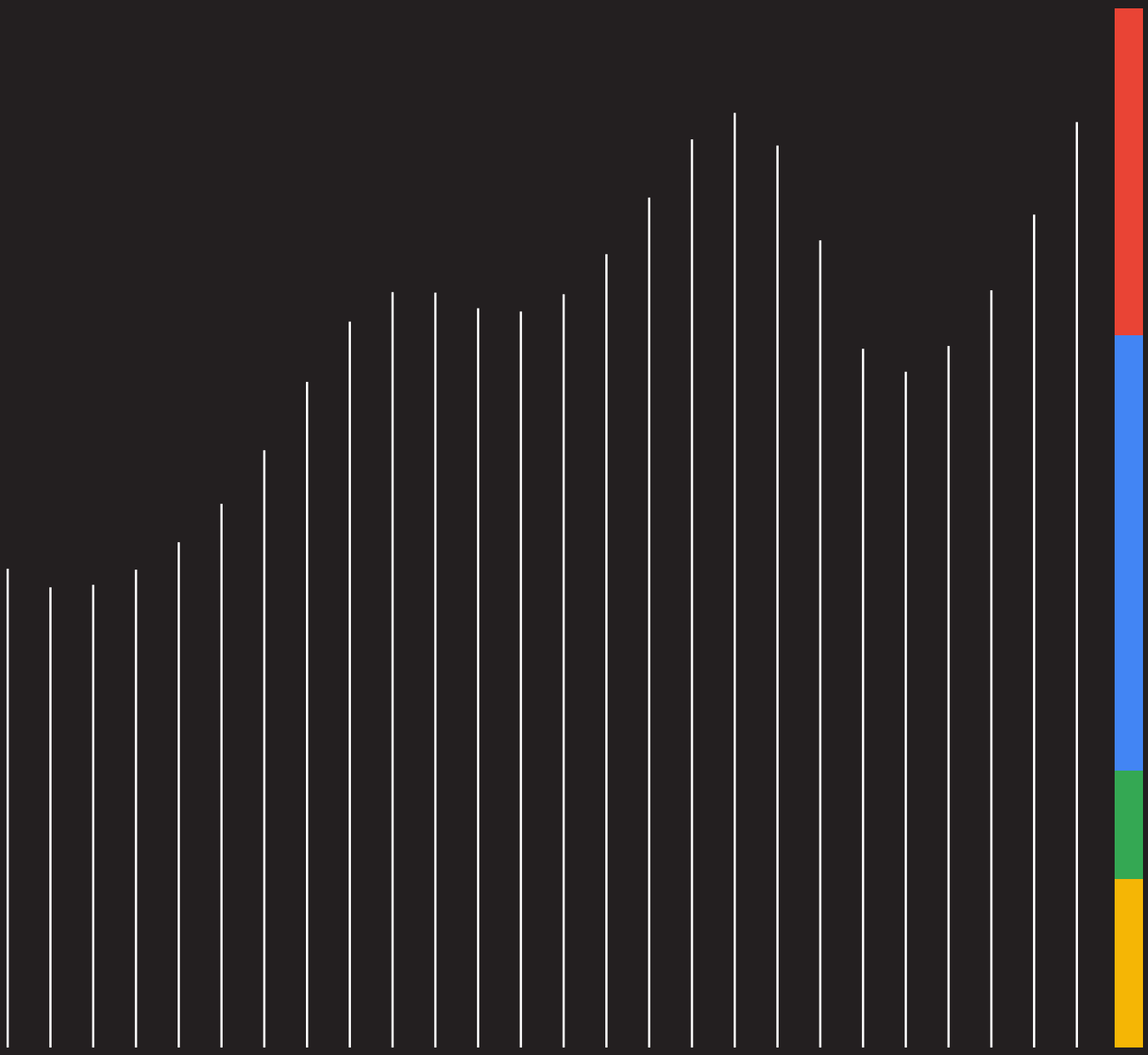
Mandiant

Google Cloud Security

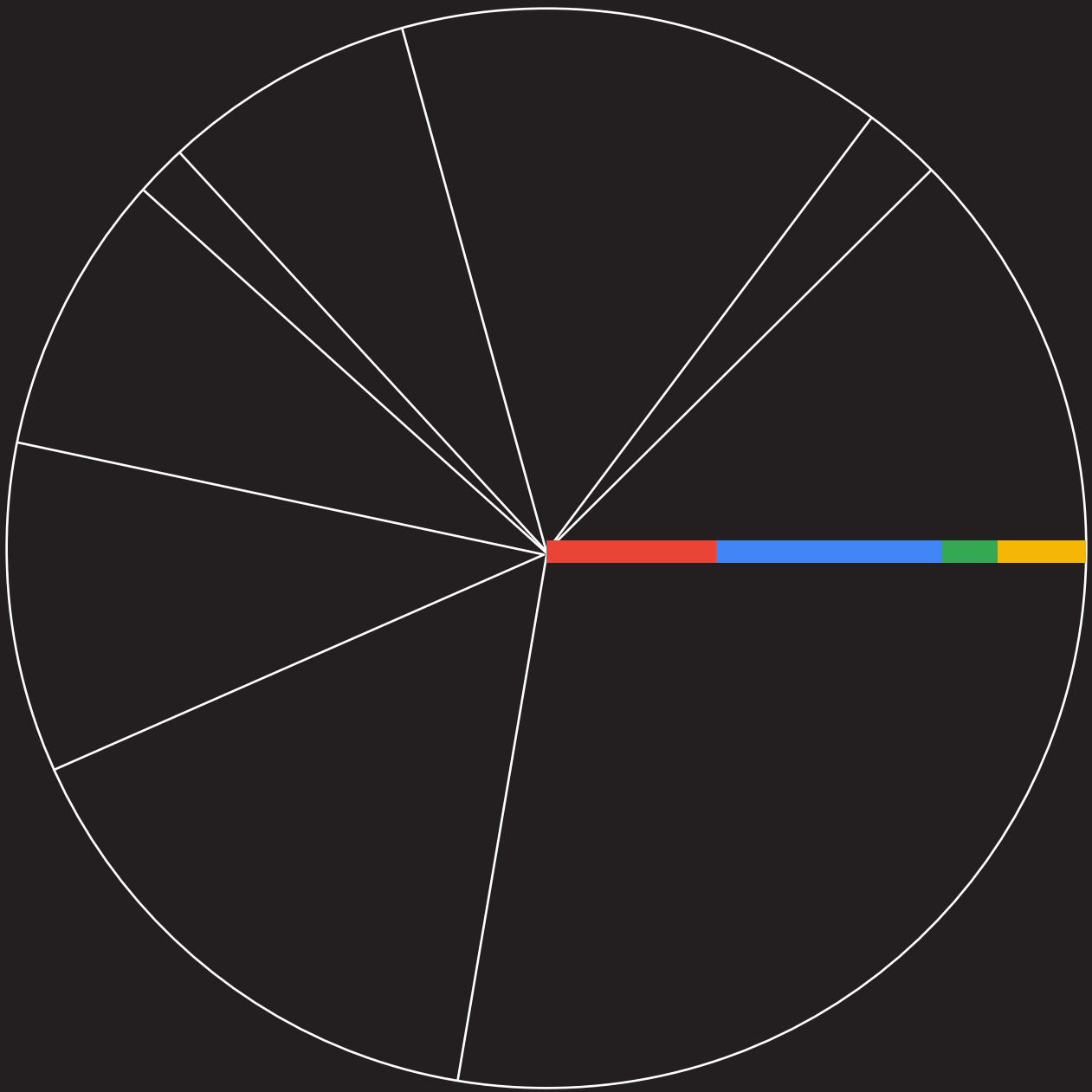
M-Trends

2024 スペシャル レポート



目次

はじめに



2023 年の侵害調査から得られた重要なポイントの一つであり、M-Trends 2024 の主要テーマでもあることとして、攻撃者が検出回避に重点を置き始めていることがあります。その目的は、検出テクノロジー（エンドポイントでの検出と対応など）を回避し、可能な限り長くネットワーク上に存在し続けることです。そのために、攻撃者は、エッジデバイスを標的としたり、「環境寄生型（LoTL）」の手法を利用したり、全社で広く使用されているセキュリティ ソリューションやその他のソリューションに潜むゼロデイ脆弱性を悪用したりしています。

攻撃者は検出の回避に懸命ですが、防御側は侵害を特定する能力を継続的に高めています。攻撃者がシステムに侵入してから検出されるまでの日数を滞留時間と言いますが、世界全体の滞留時間の中央値は、2023 年も減少傾向が続き、現在は 10 日間（前年は 16 日間）となっています。防御する側にとって大きな勝利です。ただし、ランサムウェアは滞留時間の短縮に依然として大きな影響を与えています。なぜならランサムウェアが検出されるまでの時間は短縮される傾向にあるためです。さらに、Mandiant のレッドチームが目標を達成するには通常 5〜7 日かかることを踏まえると、防御側は常に警戒を怠らないようにする必要があります。

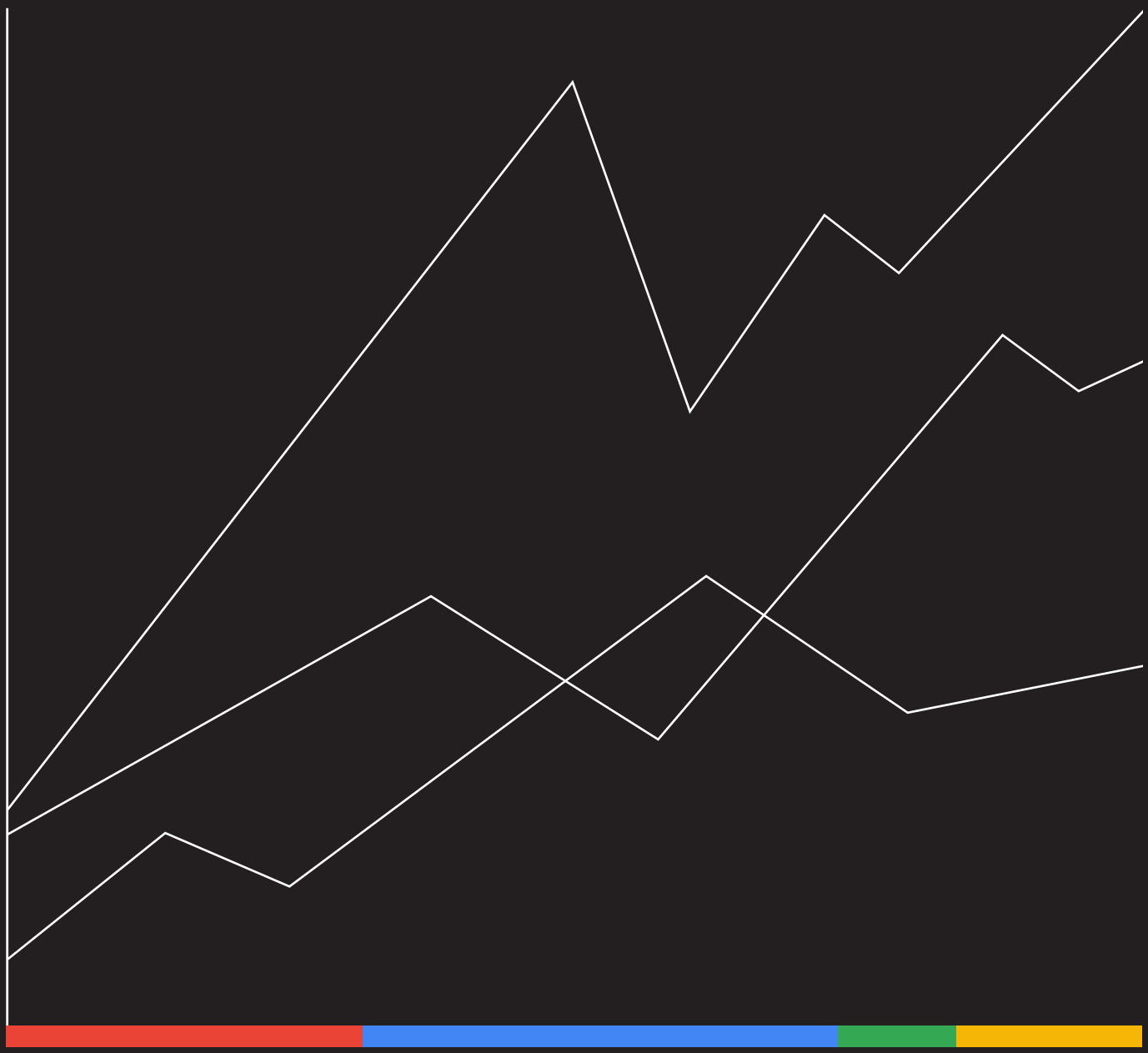
M-Trends 2024 では、読者が期待するデータやその他のセキュリティ指標を取り上げ、スパイ活動者や金銭目的の攻撃者によるゼロデイ攻撃に焦点を当て、特に中国のスパイ活動グループが行う検出回避活動について詳しく説明しています。本レポートのその他の重要なポイントは以下のとおりです。

- 攻撃者によるソーシャル メディア、SMS、その他のコミュニケーション技術の使用など、進化するフィッシングの動向
- 多要素認証を迂回する戦術（中間者攻撃などの手法）
- クラウド インフラストラクチャの標的化や攻撃者によるクラウド リソースの使用など、クラウド侵入の動向
- 新しいテクノロジーが組織により良い影響をどのようにもたらすかに焦点を当てたレッドチームとパープルチームの活動における AI の活用

Mandiant のコンサルタントは、常に最前線に立ち、最新のサイバー攻撃の調査と分析を行って、最善の防御方法を把握しています。コンサルタントは、攻撃者の最新の戦術、手法、手順に対してクライアントを先を見越して評価し、復旧、変革、教育をサポートします。

組織の防御担当者に重要な知識を提供するための献身的な取り組みに基づき、M-Trends の年次レポートをリリースすることで、優れたセキュリティ コミュニティで学んできたことを紹介します。本レポートの情報は、被害者の身元とそのデータを保護するためにサニタイズされています。

統計
データ



世界の動向

M-Trends 2024 で報告されている指標は、2023 年 1 月 1 日から 2023 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。

内部検出とは、社内セキュリティ アプライアンスによるアラートや、不審なアクティビティに関する社内担当者による通知などを通じて、組織が独自に侵害を発見することです。

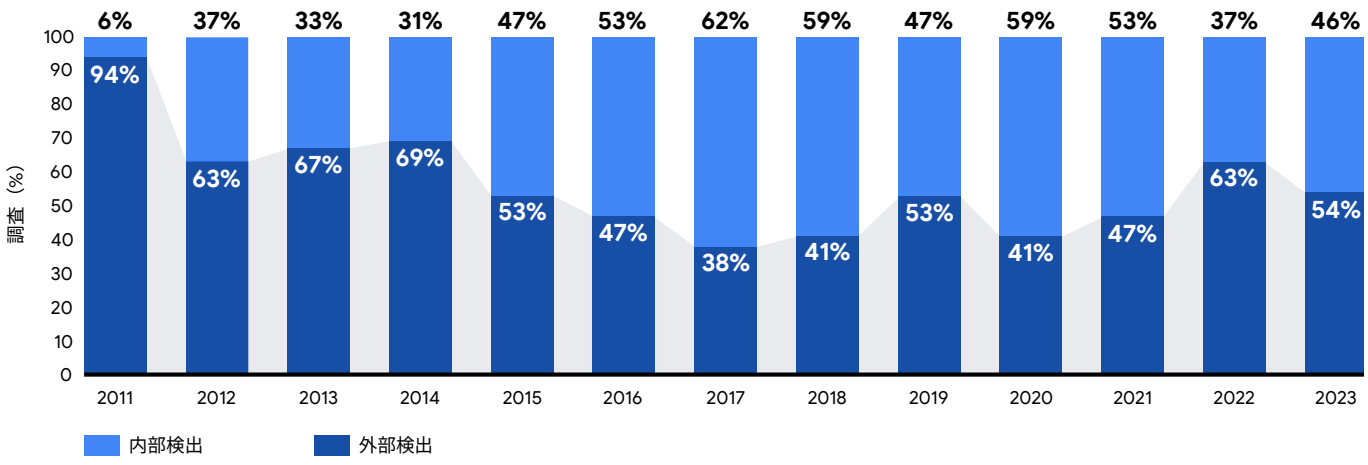
外部通知とは、法執行機関、サイバーセキュリティ企業、業界パートナーなどの外部の機関が、組織に情報漏洩があったことを通知することです。場合によっては、攻撃者がランサムノートなどでこの通知を行うこともあります。

検出元

2023 年には、侵害された組織の半数以上（54%）が、最初に外部の情報源から侵害の事実を知らされ、46% が最初に社内で侵害の痕跡を特定しました。しかし、ランサムウェア関連の侵入を切り分けたところ、ランサムウェア関連のインシデントを外部の情報源から知らされることのほうがはるかに一般的であることが明らかになりました。ランサムウェア関連の侵入については、70% の組織が外部から通知を受けており、そのほとんどが攻撃者からの身代金要求によるものでした。ランサムウェアに関連していない侵入の場合、内部検出と外部検出の比率は 50% 対 50% と互角でした。なお、内部で検出された侵入のうち、85% はランサムウェアに関わるものではありませんでした。

外部から通知された侵入の割合は、2022 年の 63% から 2023 年には 54% に減少しました。また、Mandiant は、2023 年には 2022 年よりも多くのランサムウェア関連の侵入に対応しました。ランサムウェアの事象は、ほとんどの場合、外部の手段で検出されています。それにもかかわらず、Mandiant は外部通知が 9 ポイント減少したことを観測しました。ランサムウェア以外のケースで内部検出された侵害の割合が大きいことと、この前年比の変化はネットワーク上の悪意ある行為の検出率が高くなっていることを示しています。

検出元（2011～2023 年）

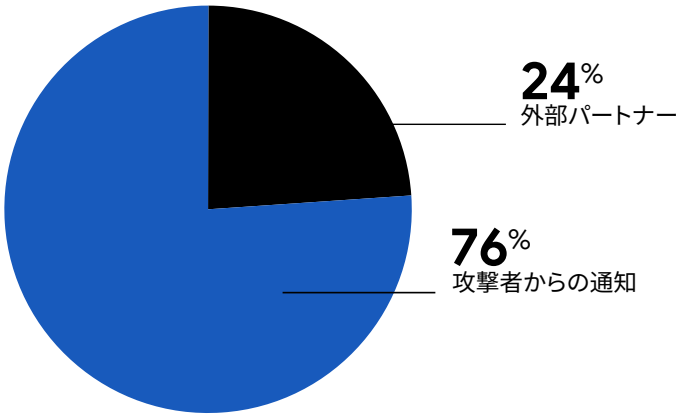


ランサムウェア関連の侵入とは、データの暗号化を主な目的とする攻撃者にアクセス手段を提供すること、あるいはそのような攻撃者と関わりを持つことを指します。これ以上の被害を回避するか、悪意ある行為を元に戻すことを条件に、標的に金銭を支払わせることが狙いです。

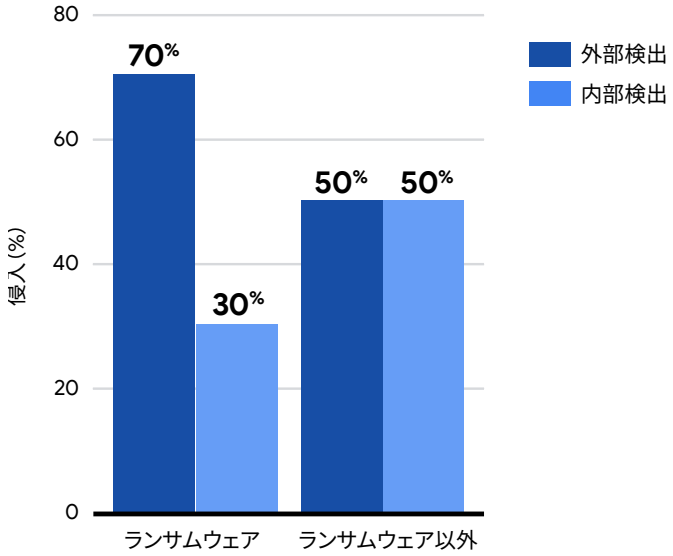
ランサムウェア関連の侵入

事例の 70% において、組織はランサムウェア関連の侵入を外部の情報源から通知されていました。その侵入の 4 分の 3 では、攻撃者のランサムノートによって組織がランサムウェアのインシデントを認識していました。これは、攻撃者がランサムウェアの侵入を意図的かつ唐突に組織に通知し、支払いを要求するという恐喝ビジネスモデルと一致しています。ランサムウェア侵入に関する外部通知の残り 4 分の 1 は、法執行機関やセキュリティ企業などの外部パートナーからのものでした。2022 年は、ランサムウェア侵入に関する外部通知のうち、攻撃者からの通知が 3 分の 2 を占めたのに対し、外部パートナーからの通知は 3 分の 1 でした。

ランサムウェアの外部通知元（2023 年）



検出元（2023 年）



滞留時間とは、攻撃者が検出されるまでに侵害した環境に存在する日数のことです。中央値は、大きさで分類されたデータセットの中点の値を表します。

滞留時間の中央値の変化

16 日間（2022 年） ↘ 10 日間（2023 年）

滞留時間

世界全体の滞留時間の中央値は引き続き減少傾向にあり、M-Trends レポートの全対象期間において初期侵入から検出までの期間が最短であったことも、注目すべきことの一つです。2023 年には、ほとんどの組織が初期侵入から 10 日以内に侵入を検出しました。2022 年の 16 日間と比べると、ほぼ 1 週間短くなっています。

Mandiant は、世界全体のすべての通知元において滞留時間の中央値が 2023 年に顕著に改善していることを観測しました。全体的に最も期間が短いところでは、外部通知元について世界全体の滞留時間の中央値が、2022 年の 19 日間から 2023 年には 13 日間に短縮しました。これは、標的組織と通知を行う外部の関係者とのコミュニケーションが改善されたためと考えられます。このほか、ランサムウェアに関連する攻撃者からの通知が増加していることも短縮の理由である可能性があります。

現在も引き続き、防御側が攻撃者の侵入を内部で検出する場合、全体の滞留時間の中央値よりも早く検出されるという傾向が続いています。侵入を内部で検出した場合の世界全体の滞留時間の中央値は、2022 年の 13 日間、2021 年の 18 日間から短くなっており、2023 年は 9 日間でした。

世界全体の滞留時間の中央値（2011〜2023 年）

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
すべて	416	243	229	205	146	99	101	78	56	24	21	16	10
外部	—	—	—	—	320	107	186	184	141	73	28	19	13
内部	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9

世界全体の滞留時間の分布

滞留時間の分布は、Mandiant が調査した侵入を、特定の範囲の滞留時間で分類した際の割合を示すものです。2023 年も、Mandiant の専門家は侵入の早期検出を確認しており、侵入の 43% が 1 週間以内に検出されていました。また、2023 年には、すべての侵入のうち 3 分の 2 近くが 30 日以内に検出されていました。これは、標的型攻撃のライフサイクルの初期感染や偵察の段階で防御側が脅威の通知を受けられるようになり、以前の M-Trends のレポートと同様に、組織全体で検出能力が向上し続けていることを示していると考えられます。

Mandiant は、検出されずに長期間放置される侵入が例年に比べて減少していることを観測しています。2023 年に、調査の 6% において 1〜5 年間未検出のアクティビティを特定しました。2022 年は 11% で、2020 年以前はさらに高い割合となっています。長期間検出されないままの侵入は依然として存在していますが、セキュリティ ベンダーや法執行機関などの外部関係者がさらに関与し、通知のペースが上がれば、防御側は滞留時間の分布が左側に移動するのを確認できるようになるはずです。その一方で、環境全体での検出能力と継続的なハンティングは、長期侵入の検出において効果を発揮しています。実用的な情報が共有されるにつれ、検出能力は引き続き向上していくでしょう。

概して、滞留時間の中央値が減少し、侵入の内部検出率が上昇するという傾向が長く続いていることから、組織の防御能力は有意義で測定可能な改善を遂げていると考えられます。

世界全体の滞留時間の分布（2018〜2023 年）

ランサムウェアに関する全世界の調査からわかった変化

18% → 23%

2022 年 2023 年

全世界の滞留時間の変化 - ランサムウェア

9 → 5

日間 (2022 年) 日間 (2023 年)

全世界の滞留時間の変化 - ランサムウェア以外

17 → 13

日間 (2022 年) 日間 (2023 年)

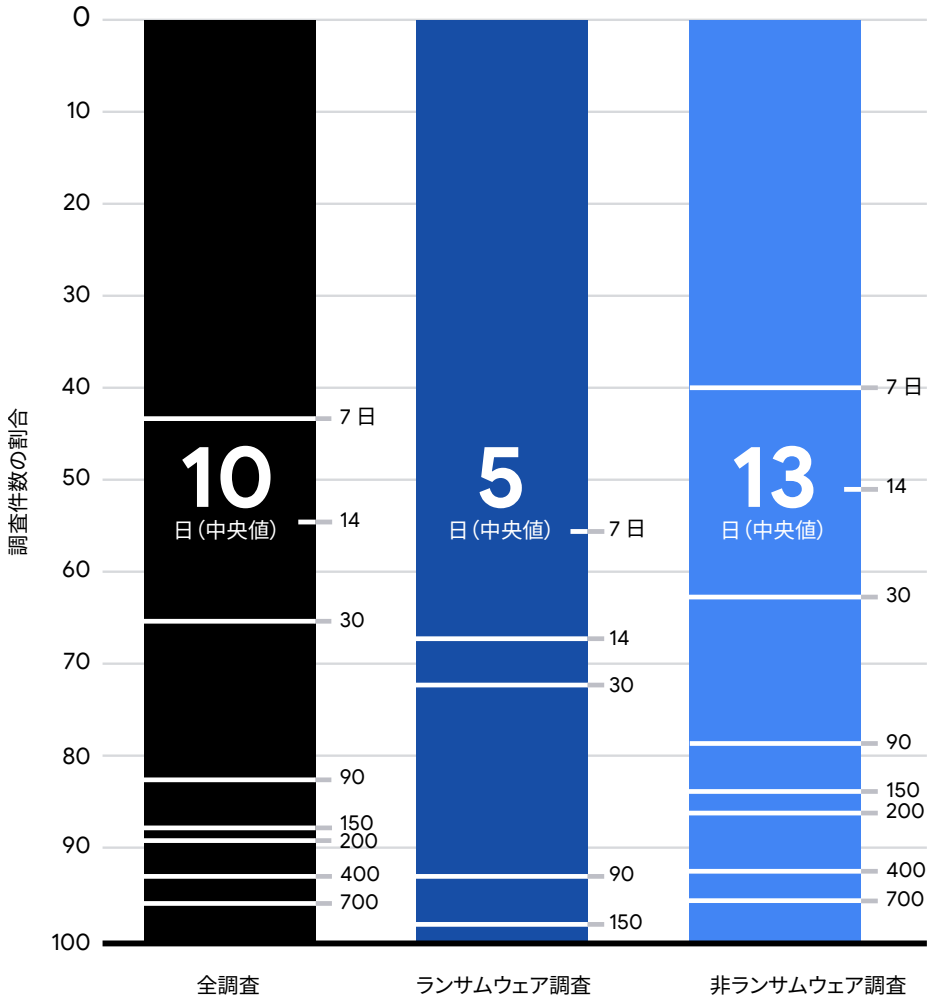
ランサムウェアに関する調査

2023 年、世界のランサムウェアに関わる調査は、2022 年の 18% から 5 ポイント増加し、23% となりました。これにより、ランサムウェア関連の侵入の割合は、2021 年の水準に戻っています。

世界全体では、ランサムウェアを検出したり、身代金の要求を受けたりするまでの期間は、通知元を問わず、2022 年の 9 日間から 2023 年は 5 日間と短くなっています。ランサムウェアに関連しない侵入が検出されるまでの期間は 13 日間で、2022 年の 17 日間から短くなっています。

なお、ランサムウェアが関与する侵入が検出されるまでの期間は、内部からの通知の場合には 6 日間で2022 年の 12 日間から短くなっています。その一方で、ランサムウェアが関与する侵入に関する通知を防御側が外部から受けるまでの期間は、2023 年は 5 日間と 2022 年の観測よりも 2 日間短くなっています。

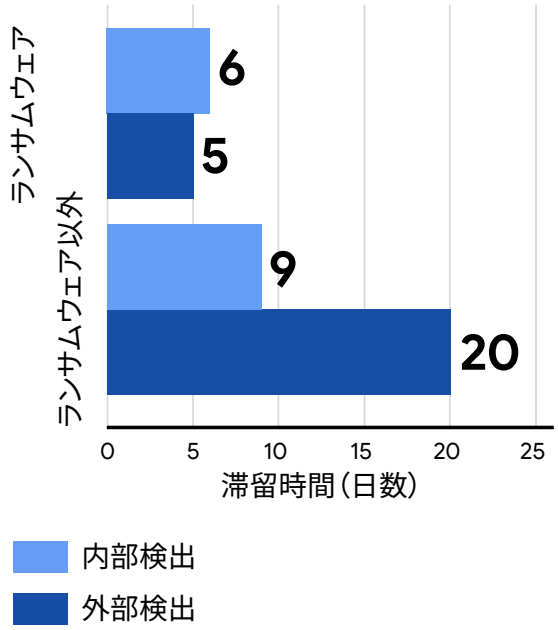
全世界の滞留時間 (調査タイプ別) (2023 年)



ランサムウェア攻撃は、長年にわたる滞留時間短縮の推進要因であり続けています。しかし、2023 年、Mandiant の専門家は、すべての通知元と調査タイプにおいて、滞留時間の短縮という顕著な改善を観測しました。

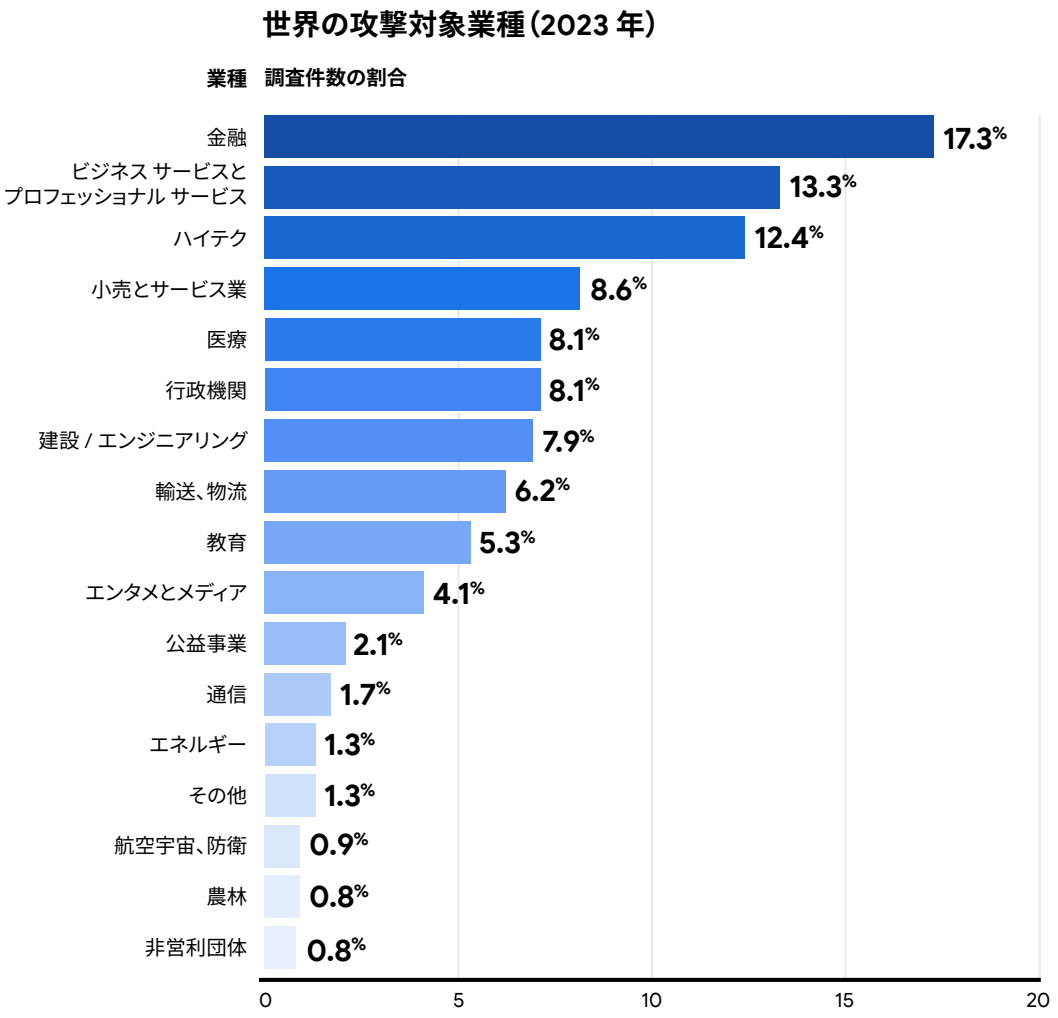
ランサムウェアが関与しない侵入を特定するまでの期間は、2023 年のほうが短くなりました。そのことは、2023 年に発生した侵入が内部において 1 週間あまりで特定されたことからも明らかです。初期侵入から検出までの期間が 9 日間と、2022 年の 13 日間に比べて短くなっています。外部関係者から侵入の通知を受けるまでの期間は、2022 年が 27 日間だったのに対し、2023 年は 1 週間短くなっており、その結果、外部関係者から通知されたランサムウェアを伴わない侵入の滞留時間の中央値は 20 日間になっています。

世界全体の滞留時間の中央値（検出元別）



標的となった業種

2023 年、Mandiant が最も頻繁に侵入に対応したのは金融サービス機関で、次いでビジネス サービスおよびプロフェッショナル サービス、ハイテク、小売およびサービス業、医療の順でした。こうした業種のいずれでも、独自のビジネス情報、個人を特定できる情報（PII）、保護医療情報（PHI）、財務データなど、さまざまな機密情報にアクセスできます。また、攻撃者は、サービス プロバイダやテクノロジー企業を悪用して第三者による侵害を容易にしたり、一度の侵害で多くの組織に属するデータやネットワークへのアクセスを獲得したりしています。こうした業種が常に調査対象の上位に名を連ねていることを Mandiant は確認しています。行政機関を対象とした調査は、2023 年には 1 位から医療部門と同じ 5 位に後退しましたが、これは 2022 年に比べてウクライナ戦争に関連する新たな調査が減少したことが反映されている可能性があります。



標的型攻撃

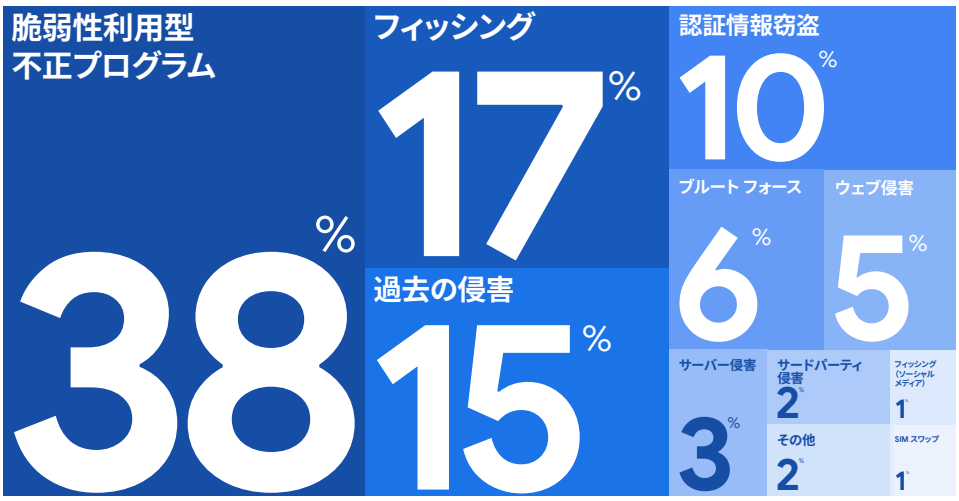
初期感染ベクトル

2023 年、Mandiant の専門家は、攻撃者が使用する最も一般的な初期感染ベクトルが、セキュリティ上の脆弱性を利用した不正プログラムであることを再び確認しました。初期侵入ベクトルが特定された侵入の 38% がセキュリティ上の脆弱性を利用した不正プログラムから始まっていました。2022 年から 6 ポイント増え、2021 年に防御側が直面したものと一致しています。詳しくは、「さまざまな動機に基づくゼロデイ攻撃」をご覧ください。

フィッシングは依然として 2 番目に多い侵入ベクトルでした。しかし、2023 年は侵入の 17% を占め、2022 年の 22% と比べて減少しました。フィッシングは、最初の足がかりを築くうえで効果的な手法であり、攻撃者がよく使っている脅威ベクトルです。詳細な分析は、「セキュリティ管理が変化する中でのフィッシングの進化」をご覧ください。

過去のセキュリティ侵害は、2023 年に攻撃者が使用した主要な侵入ベクトルの第 3 位でした。Mandiant の調査担当者は、2023 年において、侵入の 15% が過去のセキュリティ侵害で獲得したアクセスから始まっており、2022 年の観測と比較すると、このような侵入は 3 ポイント増加したことを指摘しています。この増加には、ランサムウェアのエコシステムが関連しているものと見られます。ランサムウェアのアフィリエイトと、初期アクセスを販売するさまざまなマルウェア運営者との提携が続いているようです。

初期感染ベクトル（特定した時点）



認証情報の窃盗は、組織に深刻なセキュリティ リスクをもたらします。2023 年には、よく利用される初期侵入ベクトルの第 4 位になっています。攻撃者は、パスワードが再利用されたことや、ユーザーが誤って社内デバイスにトロイの木馬ソフトウェアをダウンロードしたことを契機に認証情報を入手します。情報窃取型マルウェアは、トロイの木馬ソフトウェアを通じて配布されることがよくあります。2023 年は、侵入の 10% が認証情報の盗難の痕跡から始まっており、2022 年に観測された 14% から減少していますが、蔓延する情報窃取型マルウェアと認証情報購入の両方が、防御側を悩ませ続けています。

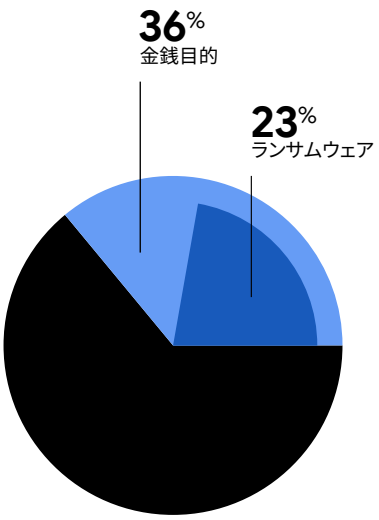
ブルート フォース アタックは 2023 年に観測された初期侵入ベクトルの上位 5 位に入っており、侵入の 6% を占めています。多要素認証の適切な実装は、環境の侵害を企てる攻撃者の活動を遅らせる転換点となりました。

攻撃者は、有効な戦術を利用して標的環境にアクセスし、活動し続けています。広く利用される感染ベクトルは変動するため、組織は多層防御戦略に注力する必要があります。このアプローチは、初期侵入方法のうち使用頻度が高いものと低いものの両方の影響を軽減する際に役立ちます。

2023 年は、初期侵入ベクトルを特定した時点において、38% で脆弱性利用型不正プログラムを観測しました。Mandiant は、サイバー エスピオナージと金銭目的の攻撃者の両方がゼロデイ脆弱性を利用して活動していることを継続的に観測しています。2023 年に Mandiant が観測した脆弱性で最も多かったのは、「MOVEit Transfer」の SQL インジェクションの脆弱性 CVE-2023-34362 [1] で、Mandiant はこれを高リスクと評価しました[2]。2 番目に多かった脆弱性は CVE-2022-21587 で、Oracle E-Business Suite に潜む未認証のファイル アップロードという重大な脆弱性でした。2023 年に 3 番目に蔓延した脆弱性は CVE-2023-2868 でした。CVE-2023-2868 は、Barracuda Email Security Gateway（物理アプライアンス）のコマンド インジェクションという重大な脆弱性です。これらの脆弱性は攻撃者に頻繁に悪用されており、特に最も狙われやすい脆弱性の 1 位と 3 位はエッジデバイスに関連するものでした。こうしたデバイスが継続的に標的となる背景の詳細については、「可視性のギャップを狙った中国のスパイ活動」をご覧ください。

ただし、Mandiant の専門家は、攻撃者が攻撃ライフサイクルを通じて脆弱性利用型不正プログラムを継続的に使用し、アクセスを維持しているほか、ラテラル ムーブメントを展開して、ミッションを完了していることも観測しています。Mandiant は、Microsoft Access 2003（CVE-2008-2463）[3]、Microsoft Windows Server 2016（CVE-2017-0144）[4]、Telerik（CVE-2019-18935）[5] のような古い技術に関連する脆弱性も若干ながら継続的に観測しています。

特に頻繁に確認された脆弱性



侵害後のアクティビティ

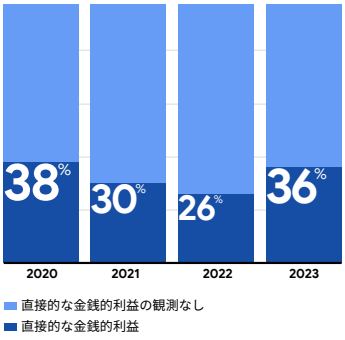
金銭目的

Mandiant が対応した侵入のうち、金銭目的の侵入の割合は、2022 年は全調査の 4 分の 1 を超える 26% でしたが、2023 年には 3 分の 1 を超える 36% に増加しました。ランサムウェア関連の侵入は、金銭目的の侵入のほぼ 3 分の 2 を占め、2023 年の侵入全体の 23% でした。

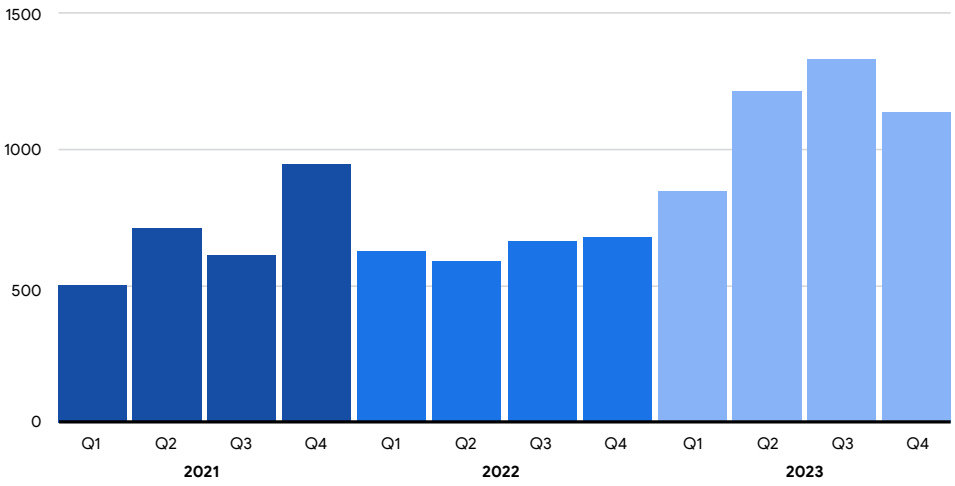
金銭目的の侵入にはこのほか、ランサムウェアによる暗号化を行わずにデータを盗難したうえでの恐喝、攻撃者が他の操作を容易にするための初期アクセスの確立、ビジネスメール詐欺（BEC）、暗号通貨窃盗などがありました。Mandiant は、暗号通貨の窃盗や IT 従業員の賃金窃盗など、金銭目的で侵入した攻撃のいくつかは、北朝鮮[6] が支援する攻撃者によるものである可能性が高いと発表しています。Mandiant は、運用コストの調達と国家に収入をもたらすことを目的としたより大規模なアクティビティの両方を実現するための金銭目的のアクティビティを行う北朝鮮の脅威グループを引き続き追跡しています[7]。

2023 年のランサムウェアやその他の恐喝関連の調査件数の増加傾向は、データ漏洩サイト（DLS）への掲載件数の著しい増加や恐喝の推定被害額に関する Mandiant やオープンソースの観測と一致しています[8]。DLS は、身代金の支払いを拒否した企業から不正に取得したデータが公開されるウェブサイトです。このデータは、攻撃者の身代金要求を拒否した標的に偏っていますが、それでも恐喝行為の大まかな傾向を把握するうえで有用です。「フィッシングの進化」のセクションで説明した FIN11 MOVEit エクスプロイト キャンペーンと UNC3944[9] アクティビティは、ランサムウェアによる暗号化を伴わない恐喝侵入の蔓延を示しています。

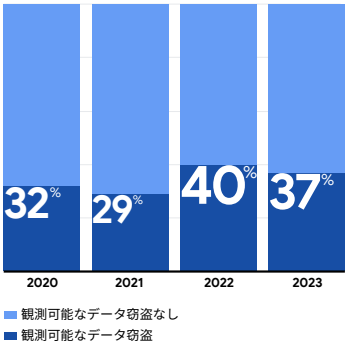
金銭目的（2020～2023 年）



四半期あたりの DLS 掲載件数（2021～2023 年）

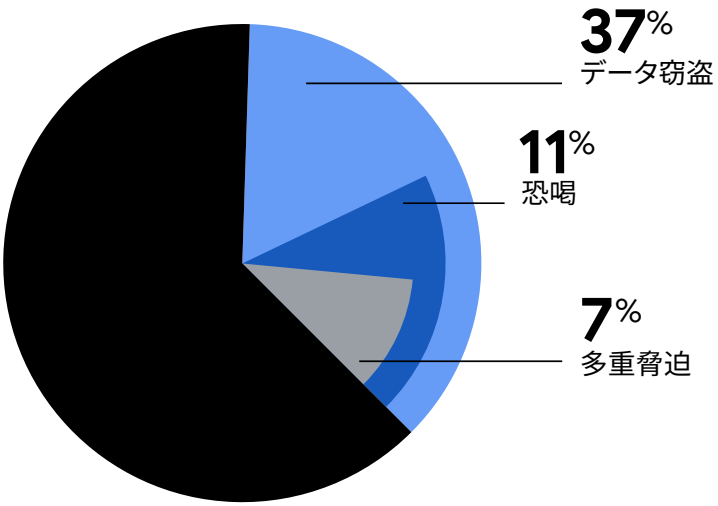


データ窃盗（2020～2023 年）

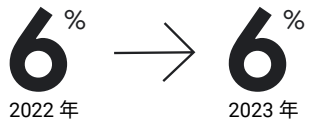


データ窃盗

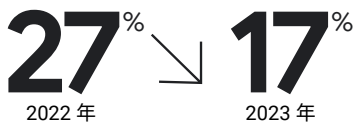
Mandiant は、2023 年の侵入の 37% でデータ窃盗を確認しましたが、これは 2022 年に報告された侵入の 40% よりわずかに低い数値となっています。侵入の 11% において、攻撃者は恐喝によって盗んだデータを直接収益化しています。さらに 7% において、データ窃盗、ランサムウェア、恐喝（別名: 多重脅迫）を組み合わせています。また、Mandiant は攻撃者が認証情報をはじめ標的ネットワークの偵察を容易にすると見られるデータを盗み出したことも観測しました。知的財産を含む大規模なデータが盗まれたケースもいくつかありました。Mandiant は、ロシアのサイバー エスピオナージ グループ APT29[10] や、中国のサイバー エスピオナージ クラスタの疑いがある UNC4841 などのグループによる標的型または選択的なデータ窃盗の事例も特定しました[11]。



侵害されたアーキテクチャ



特定された複数の脅威グループ（環境ごと）

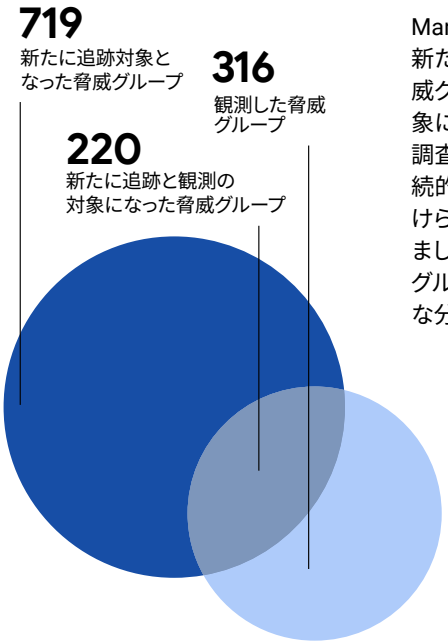


環境

2023 年、Mandiant の専門家は、侵害済みのアーキテクチャを使用して攻撃者が迷惑メールを送信したり、ボットネットを配信したり、ある種のクリプトマイニング アクティビティを行ったりしていることを引き続き観測しました。この 3 年間、脆弱性が大規模に悪用された後、侵害済みのアーキテクチャに関連する侵入が大幅に自動化されています。新たな脆弱性利用型不正プログラムの概念実証（PoC）コードが一般公開されることで、攻撃の自動化が容易になり、侵害済みのインフラストラクチャを悪用する攻撃者の攻撃サイクルが加速します。また、脆弱性を狙った PoC コードが一般公開されると、攻撃者がスキャンツールを使って脆弱性利用型不正プログラムを自動化するのが簡単になります。

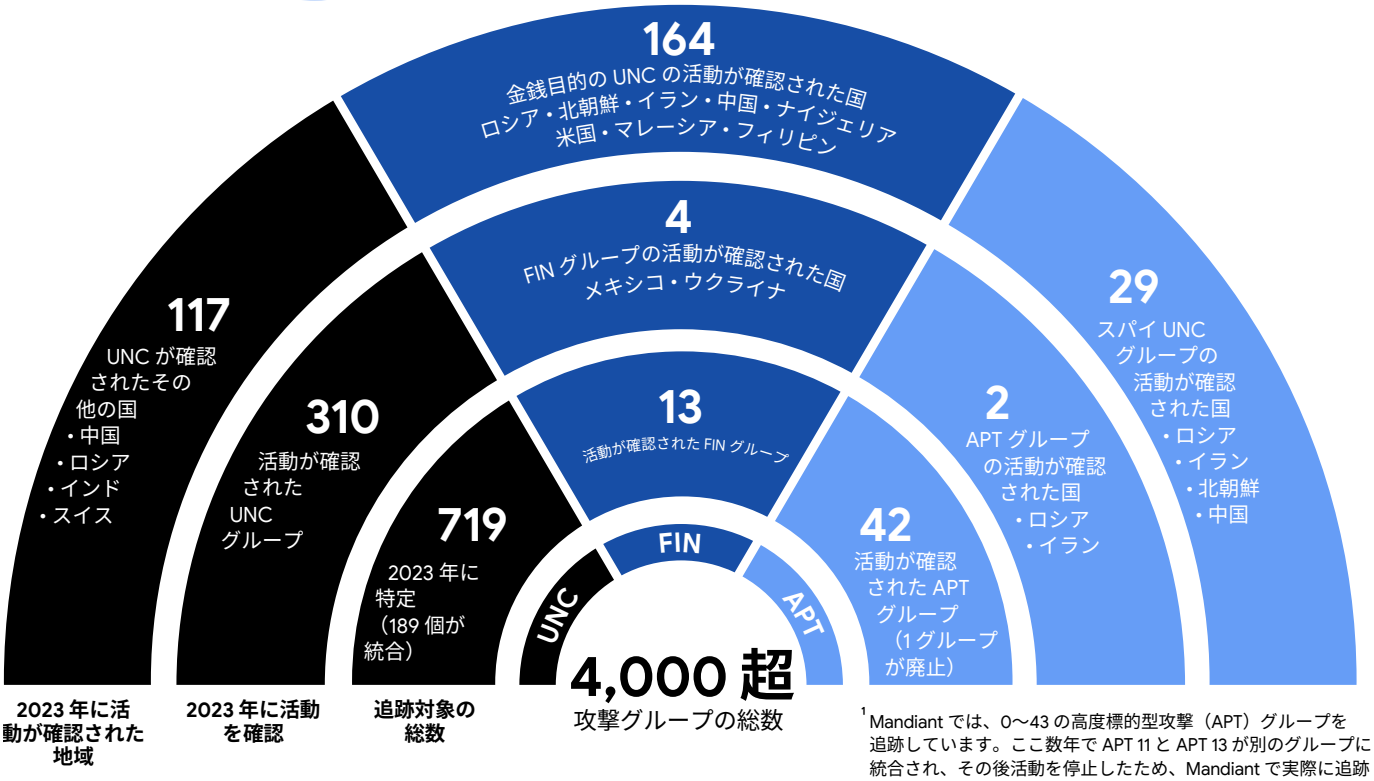
2023 年、Mandiant は単一の環境で複数の脅威グループを特定した調査の件数が減少していることを指摘しました。Mandiant の専門家は、調査の 17% において、複数の脅威グループが標的環境で活動していることを明らかにしました。これはおそらく、Mandiant が調査した標的型ゼロデイの量に関連していると思われます。2022 年（27%）からの 10 ポイントの減少は好ましい傾向であり、これは攻撃者が新たに環境に侵入しにくくなるよう防御側が努力した成果である可能性があります。

脅威グループ



Mandiant は 4,000 を超える脅威グループを追跡しており、そのうちの 719 グループは 2023 年に新たに追跡対象となったものです。Mandiant は、2023 年に侵入に対応する際に 316 の異なる脅威グループに遭遇し、同じ年の Mandiant の調査では 220 のグループが新たに追跡と観測の対象になりました。これらの数字は 2022 年の観測とほぼ一致しています。たとえば、Mandiant の調査で、2022 年には 265 のグループが新たに追跡と観測の対象になりました。2023 年、高度持続的脅威（APT）と名付けられたロシアとイランの 2 つのグループのほか、金融脅威（FIN）と名付けられた 4 つのグループや、310 の未分類（UNC）グループによる侵入に直面した組織が複数ありました。これらの UNC グループのうち 253 は新たに特定されたものでしたが、残りの 57 の UNC グループは、Mandiant がすでに 1〜10 年にわたって追跡していました。脅威グループのこのような分布は、組織が定期的に既存の脅威と新しい脅威の両方と戦っていることを示しています。

観測した脅威グループとは、Mandiant の調査担当者がインシデント対応の調査中に遭遇した脅威グループです。

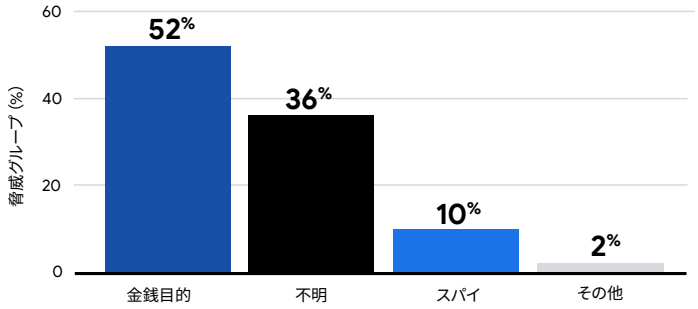


[1] Mandiant では、0〜43 の高度標的型攻撃（APT）グループを追跡しています。ここ数年で APT 11 と APT 13 が別のグループに統合され、その後活動を停止したため、Mandiant で実際に追跡している APT は 42 グループとなっています。

UNC グループ Mandiant は、既存のグループに確実にリンクできない新たな脅威アクティビティに遭遇した場合、UNC グループの正式名称を作成し、そのアクティビティ クラスタに関連する観測可能なアーティファクトを結び付けます。同じアクティビティ クラスタに関連付けることができる新たな情報やアーティファクトが見つかると、Mandiant のアナリストは攻撃者について最初の理解を深め、追跡した他の脅威クラスタと統合し、最終的に UNC を APT または FIN グループに移行する可能性があります。

2023 年に観測された攻撃者の半数超（52%）は、金銭的な利益を主な動機としており、10% はスパイ活動を主な目的としていました。ハクティビズムを動機として活動していると Mandiant が判断した脅威クラスタと、混乱や破壊を目的とした攻撃者、そしてペンテスターはわずか 2% と非常に少数でした。脅威クラスタの残りの 36% については、特定の動機を高い信頼度で判断するには十分な証拠がありませんでした。2022 年と比較して、スパイ活動、混乱や破壊、ハクティビズム、影響力行使を目的とする攻撃者の割合が緩やかに減少していることを Mandiant は観測しています。2023 年に観測された攻撃者のうち、金銭目的のグループが占める割合は 52% と、2022 年の 48% より多くなっており、この変化は、少なくとも部分的には、2023 年のランサムウェアや恐喝に関連するアクティビティの増加によって説明がつきます。

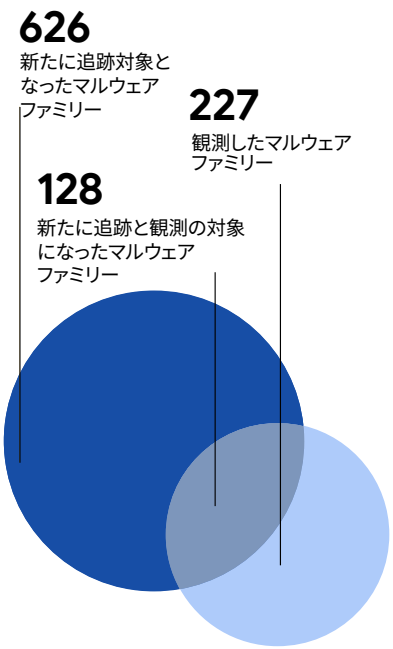
観測した脅威グループ（目標別）（2023 年）



昇格

2023 年、Mandiant は新たに命名した脅威グループの一つである APT43 へと昇格させ、アクティビティの重複に関する広範な調査に基づき、189 のアクティビティ クラスタを他の脅威グループに統合しました。Mandiant が UNC グループと統合を定義および参照する方法の詳細については、「How Mandiant Tracks Uncategorized Threat Actors」をご覧ください[12]。

APT43 は北朝鮮政府の利益に貢献している活発なサイバー活動グループです。このグループは、ある程度洗練された技術力と攻撃的なソーシャル エンジニアリング戦術を組み合わせ、特に朝鮮半島を巡る地政学的問題に熱心に対処している韓国や米国の政府機関、学者、シンクタンクを標的としています。APT43 はスパイ キャンペーンに加え、戦略的インテリジェンスの収集という主要なミッションを実現するために、サイバー犯罪活動を通じて資金を調達していると Mandiant は確信しています。このグループは、ソーシャル エンジニアリングで使用するための多数のなりすましペルソナや不正なペルソナを作成しているほか、運用ツールやインフラストラクチャを購入するための偽装 ID も作成しています。APT43 は北朝鮮の他のスパイ活動家と複数の攻撃活動で協力しており、北朝鮮のサイバー組織において大きな役割を果たしていることが明らかになっています。詳しくは、APT43 の詳細レポートをご覧ください[13]。



マルウェア

2023 年、Mandiant は 626 の新しいマルウェア ファミリーの追跡を開始しました。そのうち 128 はインシデント対応調査で確認したものでした。これは、Mandiant が 1 年間に確認したマルウェア ファミリーの純新規数としては最多です。しかし、この数字は、2022 年に新たに追跡対象となった 588 のマルウェア ファミリーを大幅に上回っているわけではなく、攻撃者が同様のペースでツールセットを増やしている可能性を示しています。

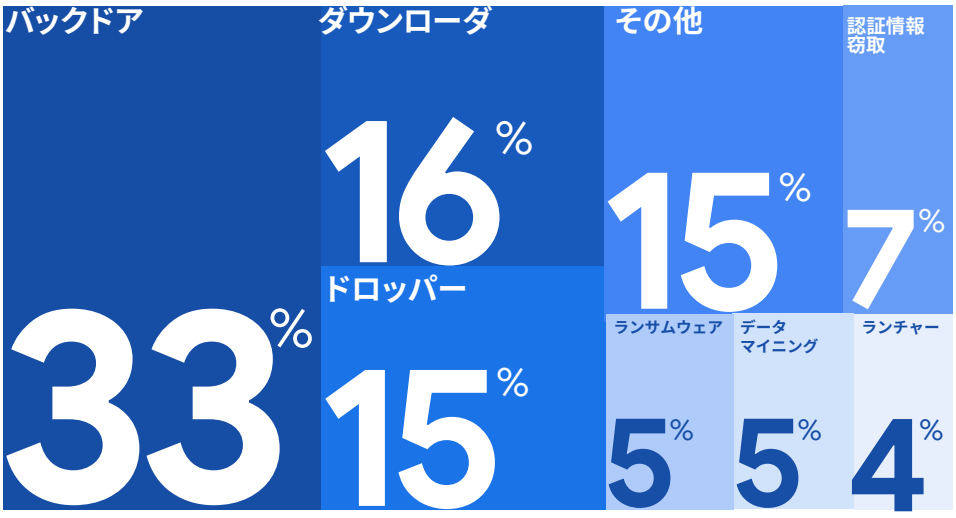
Mandiant が 2023 年に新たに追跡対象としたマルウェア ファミリーの数の増加を観測した一方で、観測したファミリーの総数は 321 から 277 に減少しました。この減少は、以前に確立されたツールの使用の増加や、マルウェアをまったく使用しない侵害の数の増加を反映している可能性があります。侵入で観測した全 277 のマルウェア ファミリーのうち、2023 年に新たに追跡対象としたものは 128 でした。

マルウェア カテゴリとは、マルウェア ファミリーの主な目的を説明したものです。各マルウェア ファミリーは、複数のカテゴリに属する機能を有していたとしても、その主な目的を最もよく表す 1 つのカテゴリにのみ割り当てられます。

新しいマルウェア ファミリー（カテゴリ別）

上位 5 つのマルウェアのカテゴリは、前年比でほぼ一致しています。新たに追跡対象とした 626 のマルウェア ファミリーのうち、上位 5 つのカテゴリには、バックドア（33%）、ダウンローダ（16%）、ドロッパー（15%）、認証情報窃取（7%）、ランサムウェア（5%）が含まれています。新たに追跡対象とした認証情報窃取は、2022 年に一度順位を下げた後、2023 年には再び上位 5 つのカテゴリに返り咲きました。もう一つの注目すべき順位の変化は、新たに追跡対象としたランサムウェア ファミリーの減少です。2023 年に新たに追跡対象としたマルウェア ファミリーは 7% から 5% に減少しています。Mandiant は、2023 年も 2021 年と同様の割合のランサムウェア侵入に対応しましたが、ランサムウェア ファミリーの純新規数の減少は、LOCKBIT、ALPHV、BASTA、ROYALLOCKER など、2023 年より前に存在したランサムウェア系統の普及を反映している可能性があります。

新たに追跡対象となったマルウェア ファミリー（カテゴリ別）（2023 年）



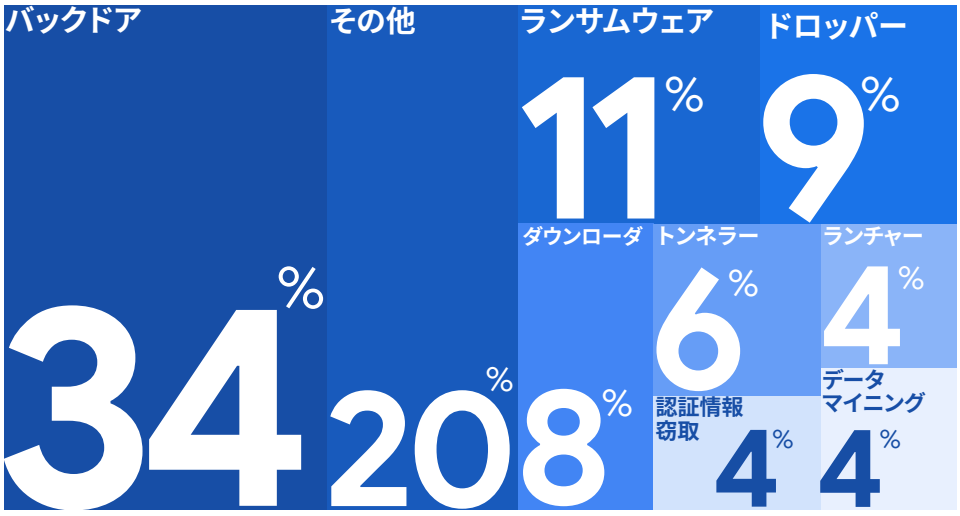
観測したマルウェア ファミリーとは、Mandiant の専門家による調査中に特定されたマルウェア ファミリーです。

観測したマルウェア ファミリー（カテゴリ別）

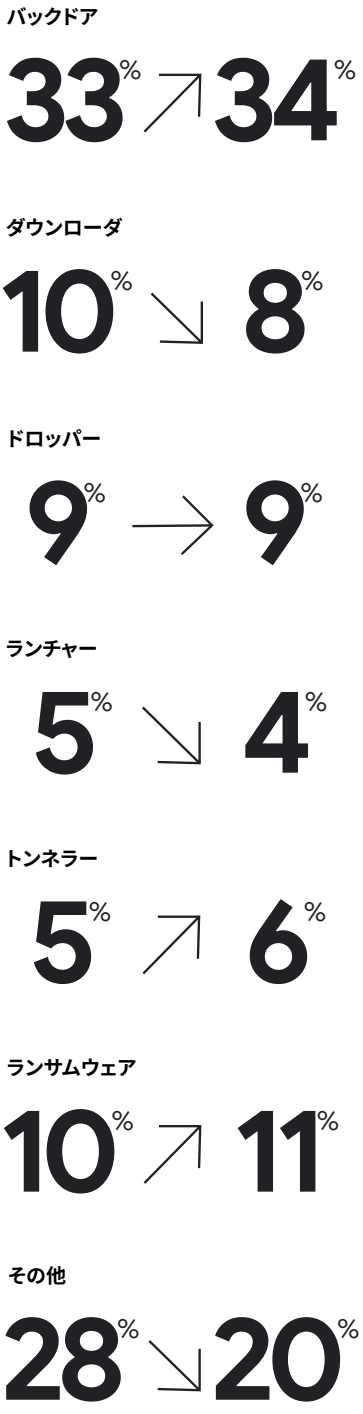
観測したマルウェア ファミリーのカテゴリも、例年の調査結果と比較的一致していました。Mandiant の専門家は、2023 年に実施した調査で 277 のマルウェア ファミリーを観測しています。バックドアは依然として攻撃者によく使用され、観測したマルウェア データセットの 34% を占めています。これは 2022 年から 1 ポイント上昇しています。その他の観測したマルウェア ファミリーのカテゴリを見ると、ランサムウェア（11%）、ドロッパー（9%）、ダウンローダ（9%）、トンネラー（6%）が上位 5 つを占めています。

Mandiant では、リモート管理ツールやその他のユーティリティを使用して攻撃活動を遂行する攻撃者の増加を引き続き確認しており、「その他」のカテゴリが前年比で増加し続けています。このカテゴリに属するマルウェア ファミリーの 20% のうち、8% は正規のユーティリティまたはリモート管理ツールです。これらのツールは本来悪意のあるものではなくても、攻撃者が検出を逃れる手段として頻繁に侵入時に活用しており、利用されやすい状況が継続しています。検出を回避して攻撃活動をさらに進めるために、攻撃者はすでに環境にあるシステムツールを導入することで環境寄生型（LotL）手法を使用しているほか、エンドポイント検出対応ツールのようなセキュリティ技術でデフォルトでフラグが立てられにくいリモート管理者ツールを悪用しています。

観測したマルウェア ファミリー（カテゴリ別）（2023 年）



観測したマルウェア ファミリー（2022〜2023 年）



マルウェアのカテゴリ	主な目的
バックドア	インストール先のシステムに対して攻撃者が対話型コマンドを発行できるようにすることを主な目的とするプログラム。
認証情報窃取	認証情報へのアクセスや、認証情報のコピーまたは窃盗を主な目的とするユーティリティ。
データマイニング	通常、窃盗のためにデータを収集することを主な目的とするユーティリティ。ただし、権限をエスカレーションするために使用される認証情報や、システムまたはネットワークの偵察に使用される情報などのデータを収集するユーティリティは除く。
ダウンローダ	指定されたアドレスからファイルをダウンロード（および、場合によっては起動）することだけを目的とし、それ以外の機能を提供することや、他の対話的コマンドに対応することがないプログラム。
ドロッパー	1 つまたは複数のファイルを抽出、インストールし、場合によっては起動または実行することを主な目的とするプログラム。
ランチャー	1 つまたは複数のファイルを起動することを主な目的とするプログラム。ドロッパーやインストーラと異なる点は、ファイルの格納や構成を行うことがなく、単にファイルの実行や読み込みを行うことである。
ランサムウェア	悪意のあるアクション（データの暗号化など）を実施することを主な目的とし、その悪意のあるアクションを回避または取り消すことを条件に標的に金銭を支払わせることを目的としたプログラム。
トンネラー	ネットワーク トラフィックをプロキシまたはトンネリングするプログラム。
その他	ユーティリティ、リモート管理テクノロジー、キーロガー、POS のような他のカテゴリが含まれる。

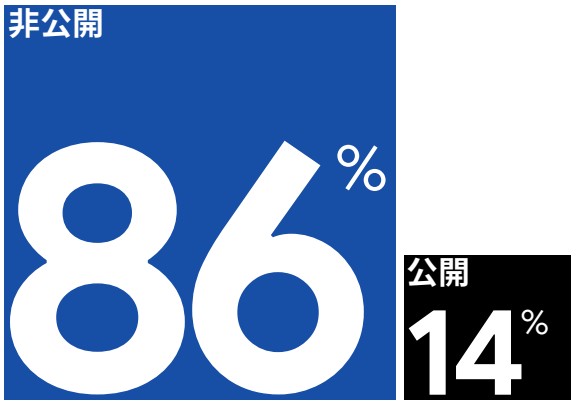
一般に入手可能なツールやマルウェア ファミリーは、制限なく容易に取得できます。これには、インターネットで自由に入手できるツールだけでなく、購入可能な市販されているツールも含まれています。

非公開のツールやマルウェア ファミリーは、Mandiant が知りうる限り（無料、販売のいずれも）一般に入手できません。これには、個人的に開発、保有、使用されるツール、限定された顧客の間で共有されるツール、限定された顧客に販売されるツールなどがあります。

マルウェアの利用可能性

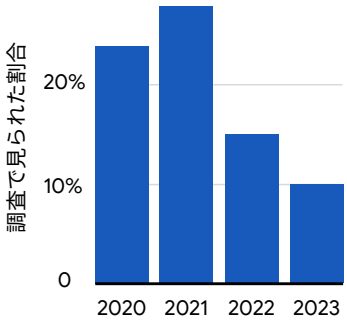
2023 年も、これまでの M-Trends レポートと同様に、新たに追跡と観測の両方の対象になったマルウェア ファミリーの利用可能性は非公開に偏っています。どちらのカテゴリでも、マルウェア ファミリーは非公開で開発されたものや、利用が制限されたものが多くなっています。攻撃者は従来、さまざまな非公開マルウェアを使って攻撃活動を行ってきました。しかし、調査で観測した、一般公開されているマルウェア ファミリーの割合は、2021 年から 2022 年、2022 年から 2023 年でそれぞれ 1 ポイントずつ増加し、30% に達しました。一般公開されているマルウェアの使用が増加しているのは、長期的なステルス性よりもスピードと効率性を優先する、金銭目的の攻撃者が増加していることを反映している可能性があります。

新たに追跡対象となったマルウェア ファミリーの公開状況（2023 年）



観測したマルウェア ファミリーの公開状況（2023 年）

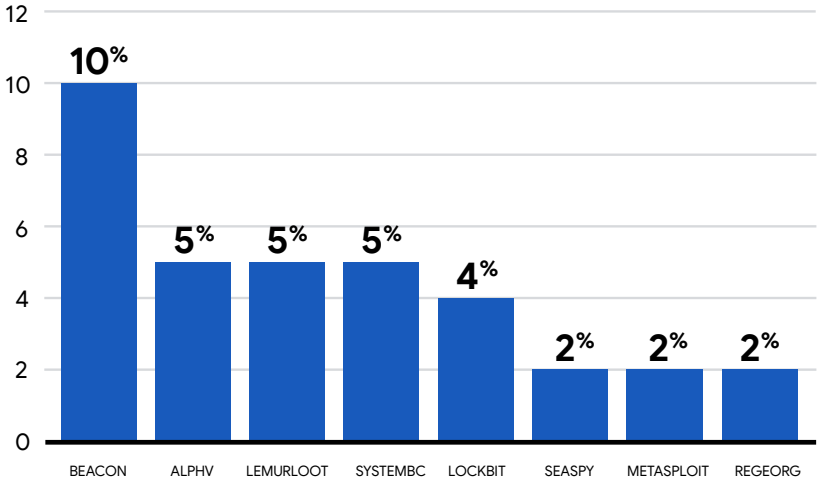
BEACON の利用状況（2020〜2023 年）



特に頻繁に確認したマルウェア

BEACON は、Mandiant の調査において世界的に最も頻繁に観測され続けているマルウェア ファミリーであり、全侵入の 10% において特定されています。BEACON は依然として攻撃者によく使用されていますが、過去 3 年間、Mandiant では BEACON の利用が減少していることを確認しています。2021 年には、侵入の 28% において、少なくとも 1 つの BEACON バックドアが使用されていました。当時、ランサムウェア グループは世界中の組織を積極的に侵害し、BEACON を頻繁に使用して攻撃活動を遂行していました。2022 年、ランサムウェア関連の侵入は世界的に減少し、BEACON の使用率もその減少を反映していました。しかし、2023 年には、ランサムウェアの侵入が増加したにもかかわらず、BEACON の使用率は過去最低であったと Mandiant は指摘しました。

特に頻繁に確認したマルウェア ファミリー（2023 年）

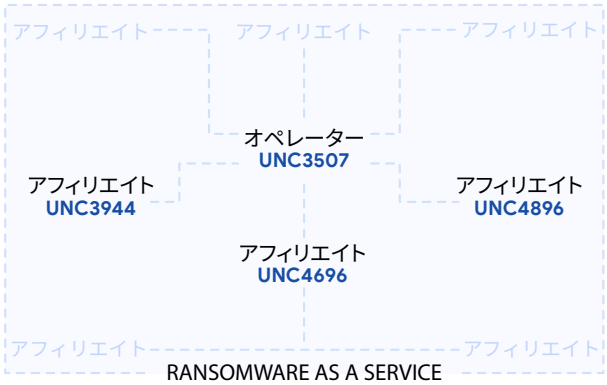


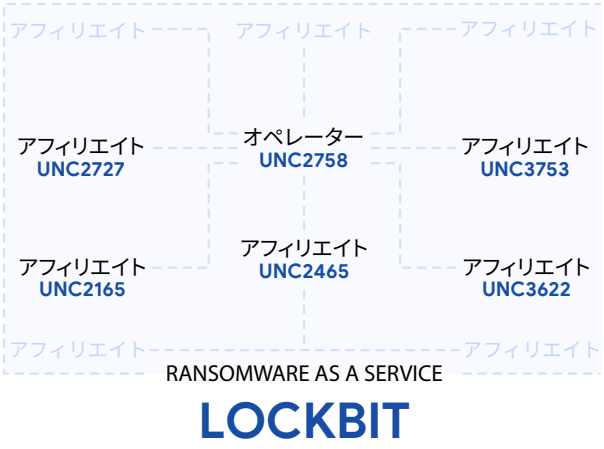
この減少は、攻撃者がメモリ常駐型マルウェアでエンドポイント セキュリティ技術を回避し、サードパーティのリモート管理ツールを利用して、より多くの LotL 手法を採用していることや、システム上のネイティブなツールやプロセスを悪用していることと一致している可能性があります。もう一つの可能性として、攻撃者がコマンド アンド コントロール（C2）フレームワークである Cobalt Strike から移行し、主要なバックドアとして BEACON を使用していることが挙げられます。堅牢なセキュリティ コミュニティ主導の検出により、Cobalt Strike フレームワークに対する軽減措置が増加したため、攻撃者はますます SLIVER、Brute Ratel、Mythic といった他の C2 手段を利用して攻撃活動を支援するようになるでしょう。

2023 年において、ALPHV と LOCKBIT がそれぞれ、頻繁に観測したマルウェア ファミリーの第 2 位と第 5 位でした。Mandiant が主導した調査では、Mandiant が ALPHV ランサムウェアに遭遇したのは 2022 年は 2% だったのに対し、2023 年は 5% でした。

Mandiant が観測したマルウェア ファミリーのうち、多く蔓延しているマルウェア ファミリーの第 3 位と第 6 位は、多く悪用されている脆弱性の第 1 位と第 3 位に関連したものでした。LEMURLOOT（5%）と SEASPY（2%）は、それぞれ MOVEit と Barracuda の技術を悪用した攻撃者が使用するバックドアです。頻繁に観測した残りのマルウェア ファミリーは、複数の攻撃者によって使用されており、ALPHV、LOCKBIT、LEMURLOOT、SEASPY と組み合わせて使用されているものもあります。

BEACON	Cobalt Strike フレームワークの一部である、C/C++ で記述されたバックドア。対応しているバックドア コマンドには、Shell コマンドの実行、ファイル転送、ファイル実行、ファイル管理などがあります。BEACON は、キー操作やスクリーンショットをキャプチャしたり、プロキシ サーバーとして動作したりすることもできます。また、BEACON は、システム認証情報の収集、ポートのスキャン、ネットワーク上のシステムの列挙というタスクも可能です。BEACON は、HTTP または DNS を介して C2 サーバーと通信します。Mandiant は、BEACON が APT19、APT32、APT40、APT41、FIN6、FIN7、FIN9、FIN11、FIN12、FIN13 や 800 を超える UNC グループをはじめ、名前が付いた広範な脅威グループによって使用されていることを確認しています。
ALPHV	Rust で記述されたランサムウェア。このランサムウェアには、その機能を指定する平文の JSON 構成が含まれている場合があります。ALPHV は、権限を昇格させて UAC をバイパスしたり、AES と ChaCha20（または Salsa）の暗号化機能が含まれていたり、攻撃活動の一環として Restart Manager を使用したり、ボリューム シャドーコピーを削除したり、ディスク ボリュームとネットワーク共有を列挙したり、プロセスとサービスを強制終了したりする可能性があります。Mandiant は、金銭目的の 20 を超える UNC グループが ALPHV を使用していることを確認しています。
LEMURLOOT	LEMURLOOT は C# で記述されたウェブシェルで、MOVEit Transfer プラットフォームを操作できるように作られています。このマルウェアは、ハードコードされたパスワードによって受信接続を認証します。また、MOVEit Transfer システムからファイルをダウンロードしたり、Azure システム設定を抽出したり、詳細な記録情報を入手したり、特定のユーザーを作成して挿入したり、そのユーザーを削除したりするコマンドを実行できます。LEMURLOOT とやり取りするシステムに返されるデータは、Gzip で圧縮されています。Mandiant による観測に基づくと FIN11 が LEMURLOOT の主要ユーザーになります。
SYSTEMBC	TCP 上のカスタム バイナリ プロトコルを使って C2 サーバーからプロキシ関連のコマンドを取得する、C で記述されたトンネラー。C2 サーバーは、SYSTEMBC に C2 サーバーとリモート システム間のプロキシとして動作するよう指示します。SYSTEMBC は、HTTP 経由で追加のペイロードを取得することもできます。この目的のために Tor ネットワークを使用する亜種もあります。ダウンロードされたペイロードは、実行前にディスクに書き込まれるか、メモリに直接マッピングされます。SYSTEMBC は多くの場合、他のマルウェア ファミリーに関連するネットワーク トラフィックを隠すために使用されます。観測したファミリーには、DANABOT、SMOKELOADER、URSNIF などがあります。Mandiant は、FIN12 および 40 を超える金銭目的の UNC グループが SYSTEMBC を使用していることを確認しました。
LOCKBIT	C で記述されたランサムウェアであり、ローカルおよび共有ネットワークに保存されているファイルを暗号化します。LOCKBIT はまた、ネットワーク上にある別のシステムを識別し、SMB 経由で増殖することもできます。ファイルを暗号化する前に、LOCKBIT はイベントログを消去し、ボリューム シャドーコピーを削除して、ファイルを暗号化する機能に影響を与える可能性のあるプロセスやサービスを終了します。LOCKBIT は、暗号化したファイルにファイル拡張子「.lockbit」を使用することが観測されています。Mandiant は、金銭目的の 30 を超える UNC グループが LOCKBIT を使用していることを確認しています。
SEASPY	SEASPY は、ポート 25（SMTP）に PCAP フィルタを確立するバックドアで、「マジック パケット」を受信すると起動します。SEASPY は、正規の Barracuda ネットワーク サービスになりすまし、さらに検出を回避するためにメモリ内のプロセスを変更します。Mandiant が SEASPY の使用を確認したのは UNC4841 のみです。
METASPLOIT	ペネトレーション テストのフレームワークで、脆弱性テスト、ネットワーク列挙、ペイロードの生成と実行、 防御回避などの機能があります。 このフレームワークには、多数のアプリケーションのほか、 Windows、Linux、macOS といった一般的なオペレーティング システム向けの脆弱性利用型不正プログラムが含まれています。 METASPLOIT は一般的に、 フレームワークの METERPRETER バックドアをダウンロードして実行する役割を担う、 ステージャー ペイロードを生成するために使用されます。 Mandiant は、 APT32、APT41、APT43、FIN6、FIN7、FIN11、FIN13、さらに 160 を超える UNC グループが Metasploit を 使用していることを確認しています。
REGEORG	ウェブシェルのトラフィックをトンネリングするために使用されるオープンソースのユーティリティ。Mandiant は、APT28、APT29、APT41 および 30 の UNC グループが REGEORG を使用していることを確認しています。





不正行為に対する注目すべき法的措置

2023 年 12 月のプレスリリースで、米国連邦捜査局（FBI）は、BlackCat としても知られる ALPHV が 1,000 を超える組織を標的にしていたと報告しました[14]。FBI のプレスリリースでは、破壊型キャンペーンと復号ツールの開発についても概説しています。これらのキャンペーンと開発により、FBI は被害を受けた多くの組織を支援することができました。Mandiant は、ALPHV ランサムウェアの運営者を UNC3507 として追跡しており、その他にもアクティビティの複数のクラスタ（特に UNC3944、UNC4696、UNC4896）をアフィリエイトとして追跡しています。

2023 年の Mandiant の調査で多く観測したマルウェア ファミリーの第 5 位は LOCKBIT でした。LOCKBIT ランサムウェアは調査の 4% において出現し、2022 年の 2% から増加しています。LOCKBIT のデータ漏洩サイトは、2023 年に他のどの恐喝グループよりも遥かに多くの標的をリストアップしています。2023 年 6 月、米国司法省（DOJ）は LOCKBIT の関連者を被告人とする刑事告発を発表しました[15]。これは、LOCKBIT ランサムウェアの世界的な攻撃活動に関与したとして DOJ が起訴した 3 人目の個人でした。LOCKBIT が 2020 年初頭に初めて登場して以来、DOJ は LOCKBIT の Ransomware-as-a-service（RaaS）関連者による攻撃件数が 1,400 超であったと指摘しています。国際的な法執行機関は LOCKBIT のアクティビティを継続的に追求しており、2024 年 2 月には「Operation Cronos」で LOCKBIT のデータ漏洩サイトとバックエンドのインフラストラクチャを押収したと発表しました[16]。Mandiant は、LOCKBIT ランサムウェアの運営者を UNC2758 として追跡しているほか、注目すべきその他の 5 つの関連グループも追跡しています。

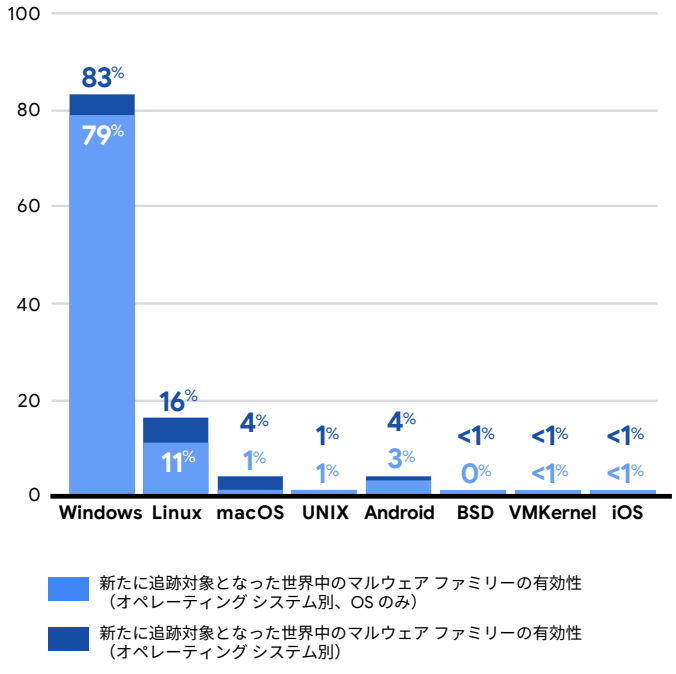
ALPHV や LOCKBIT のようなランサムウェア ファミリーは、独自の犯罪エコシステム内で活動しています。2023 年 12 月の法執行機関による ALPHV の取り締まりの後、LOCKBIT ランサムウェア サービスの運営者は、ALPHV の関連者にアピールし、ALPHV の標的がすでに行っていた交渉プロセスの妨害を試みることで、その状況を利用しようとしました。法執行機関によるこのような取り締まりや逮捕にもかかわらず、ランサムウェア グループは弾力性を維持し、迅速に適応することで、攻撃活動への影響を軽減しています。法執行機関の努力により、暗号化の解除や一時的な減速は見られたものの、ランサムウェアの収益性は、金銭目的の攻撃者が攻撃を継続する際の動機となり、組織が強固なセキュリティ対策を維持する必要性を浮き彫りにしています。

マルウェア ファミリーの**オペレーティング システムに対する有効性**とは、マルウェアの標的として使用できるオペレーティング システムを指します。

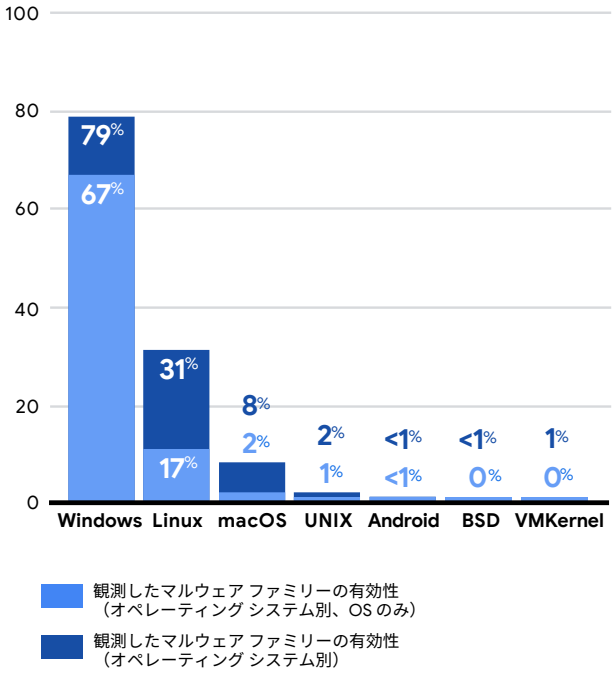
オペレーティング システムに対する有効性

2023 年、Mandiant は新たに追跡対象となった、Linux システムに対して有効なマルウェアの割合が、2022 年の 12% から 16% へとわずかに増加していることを指摘しています。特に、観測したすべてのマルウェアのうち、Linux に対して有効なものは、2022 年の 15% に対し、2023 年は 31% にまで増加しています。これまでの M-Trends レポートの対象期間と同様に、新たに追跡と観測の対象になったマルウェア ファミリーのほとんどは、依然として Windows に対して有効です。2022 年から 2023 年にかけて、Windows に関連するマルウェアの割合が明らかに減少しているのは、Windows に対して有効なマルウェアが実際に減少しているのではなく、Linux に関連するマルウェアの割合が増加していることを反映していると考えられます。

新たに追跡対象となったマルウェア ファミリーのオペレーティング システムに対する有効性（2023 年）



観測したマルウェア ファミリーのオペレーティング システムに対する有効性（2023 年）

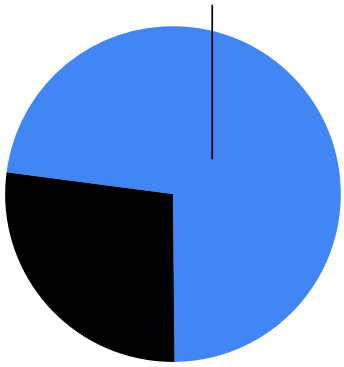


MITRE ATT&CK® は実世界での観測に基づく敵対戦術と敵対手法のナレッジベースで、どの国や地域からもアクセスできます。ATT&CK のナレッジベースは、民間部門、行政機関、サイバー セキュリティのプロダクトやサービスのコミュニティで特定の脅威モデルや手法を開発するための基盤として使用されています。

最も頻繁に使用された MITRE ATT&CK 手法（2023 年）

74%

Mandiant の調査で観測



脅威の手法

M-Trends 2020 以降、Mandiant は M-Trends で発表された知見を MITRE ATT&CK フレームワークにマッピングすることで、コミュニティをサポートしてきました。組織は、自組織のセキュリティ対策を継続的に強化する際に、侵入時に使用される手法やサブ手法に基づいて、検出機能の実装に優先順位を付けることができます。Mandiant は、組織がセキュリティ能力をさらに高める方法について意思決定する際のリソースとして使用できるよう、攻撃者によって使用された手法のうち、最も頻繁に観測した手法の指標を提供しています。

Mandiant はさらに 1,200 以上の Mandiant の手法を最新の MITRE ATT&CK フレームワークにマッピングし、合計 3,500 以上の Mandiant 手法と ATT&CK フレームワークに関連する後続の知見を提供しました。2023 年に、MITRE ATT&CK フレームワークはバージョン 14.1 に更新され、ATT&CK for Enterprise には 201 の手法と 427 のサブ手法が含まれるようになりました。

最も頻繁に使用された MITRE ATT&CK 手法（2023 年）

Mandiant の専門家は、攻撃者が、2023 年の侵入時に MITRE ATT&CK の手法の 74%、サブ手法の 44% を使用したことを観測しました。マッピングされた ATT&CK 手法のほぼ 4 分の 3 とサブ手法のほぼ半分が、2023 年に Mandiant が調査した侵入においてよく観測されました。この手法やサブ手法の幅広さは、Mandiant が 2022 年に観測したときと同規模です。

2023 年に攻撃者が使用した手法は 2022 年に観測したものと一致し、最も頻繁に見受けた手法の上位 10 個は過去数年間ほとんど変化していません。Mandiant の調査担当者は、調査の過半数において、攻撃者がコマンドまたはスクリプトのインタープリタ（T1059）を使用していることを指摘しています。2023 年のデータセットでの顕著な違いは、観測した手法の上位 10 個に、システム オーナーまたはユーザーの検出（T1033）と、公開アプリケーションに対する脆弱性利用型不正プログラムの使用（T1190）が含まれていることです。これら 2 つの手法は、ランサムウェア関連の侵入の増加や脆弱性利用型不正プログラムの利用の増加、特に 2023 年に観測した大規模なエクスプロイト キャンペーンと相関しています。

観測した上位 5 つのサブ手法は、PowerShell（T1059.001）、ウェブ プロトコル（T1071.001）、Remote Desktop Protocol（T1021.001）、サービス実行（T1569.002）、ファイル削除（T1070.004）であり、4 年連続でこれらのサブ手法がチャートを独占しているのは当然のことかもしれません。攻撃者がこれらのサブ手法を好むのは、システム内ですぐに使用できるツールを利用するため、悪用しやすいからだと考えられます。侵害の実績があり、セキュリティ対策を回避する機能が組み合わさっている場合もあるため、攻撃者のツールキットとして非常に効果的です。この長く続く傾向から、攻撃者が目的を達成するために採用する標準的な戦術が明らかになっています。組織は、これらのサブ手法をまだ検出していないのであれば、優先的に検出する必要があります。

特に頻繁に確認した手法の上位 10 個

1	T1059: コマンドとスクリプトのインタープリタ	52.3%
2	T1027: ファイルまたは情報の難読化	46.5%
3	T1083: ファイルとディレクトリの探索	38.6%
4	T1021: リモート サービス	37.3%
5	T1082: システム情報の探索	37.1%
6	T1070: インジケーターの削除	35.1%
7	T1071: アプリケーション レイヤ プロトコル	34.0%
8	T1033: システム オーナー / ユーザーの探索	31.7%
9	T1140: ファイルまたは情報の難読化解除 / デコード	31.5%
10	T1190: 一般公開されているアプリケーションの悪用	28.7%

最も頻繁に確認した MITRE ATT&CK のサブ手法の上位 5 個

1	T1059.001: PowerShell	32.3%
2	T1071.001: ウェブ プロトコル	29.6%
3	T1021.001: Remote Desktop Protocol	28.3%
4	T1569.002: サービス実行	26.8%
5	T1070.004: ファイルの削除	26.6%

Mandiant 標的型攻撃ライフサイクルにマッピングされた観測済みの MITRE ATT&CK 手法については、本レポートの付録をご覧ください。

キャンペーンおよびグローバルイベント

キャンペーンとは、1 人の攻撃者または複数の攻撃者が、時系列内で複数の標的に対して単一の目的を達成するために連携して実施する、インパクトのある一連の侵入を指します[17]。

グローバル イベントとは、複数の無関係な攻撃者が、類似のテーマ、標的、またはリソースを含むキャンペーンを並行して実施することで、インパクトのある一連の侵入を行うことです。

複数の組織が同様の脅威アクティビティによって何回も被害を受けていることを Mandiant の専門家が観測すると、キャンペーンまたはグローバル イベントが作成されます。キャンペーンは、1 つまたは複数の脅威グループが単一の目的を達成するために連携する一連のアクティビティです。より大規模なグローバル イベントでは、複数の脅威グループが関与し、複数の異なる目的を追求しますが、多くの場合、脆弱性を悪用し、類似した戦術を使用します。キャンペーンおよびグローバル イベント（CGE）は、新たな脅威アクティビティや積極的な脅威アクティビティをクライアントに通知します。各キャンペーンおよびグローバル イベントの期間中、Mandiant は、より多くの情報を受信し、分析するにつれて、新しいデータを使用して潜在的な標的を動的に更新します。このインテリジェンスには、Mandiant の調査やその他の Mandiant のリサーチから直接収集したデータに基づく、セキュリティ侵害インジケーター、主要イベントを取り巻く状況、防御策、予防策が含まれます。

キャンペーンおよびグローバル イベントにより、Mandiant のクライアントに、現在の最も危険な脅威から身を守るために必要な重要なインテリジェンスが提供されます。使用されている脆弱性利用型不正プログラムを早期に特定することは、攻撃を迅速に阻止し、被害を最小限に抑えることを意味します。CGE はチーム間の迅速な連携を促進し、迅速な対応を確実にします。Mandiant が新たな脅威データを発見すると、CGE ユーザーは即座に最新情報を受け取るため、防御を洗練させ、攻撃の最大インパクトをピンポイントで特定できます。Mandiant は、2023 年に Mandiant Consulting による調査に関連する 25 のキャンペーンおよびグローバル イベントを追跡し、報告しました。これらのキャンペーンは、南北アメリカ、EMEA、JAPAC の 21 の業種の組織に影響を与えました。

CVE-2023-34362 回顧的タイムライン

* MOVEit Cloud と MOVEit Transfer のオンプレミス バージョン

FIN11 MOVEit エクスプロイト キャンペーンは、この種のイベントの顕著な例です。CVE-2023-34362 回顧的タイムラインは、FIN11 による[18]この脆弱性の悪用に関する観測結果を示しています[19]。

Mandiant は、FIN11 が 2023 年 5 月 15 日からインターネットをスキャンし、その後 MOVEit のゼロデイ脆弱性を悪用するために使用されたインフラストラクチャを使用していることを観測しました。Mandiant のインシデント対応エンゲージメントを分析したところ、CVE-2023-34362 が悪用されたことを示す最も古い痕跡は、12 日後の 2023 年 5 月 27 日に発生していました。この痕跡は、脆弱性が最初に悪用されてから 16 時間以内に FIN11 が MOVEit テクノロジーを介して多数の組織からデータを盗み始めたことも示しています。2023 年 5 月 31 日、Progress はこの脆弱性を公表し、クラウドベースのサービスにパッチを適用して、オンプレミスの実装用パッチをリリースしました。FIN11 が CL0P^_- LEAKS DLS でのキャンペーンの責任を主張したのは、脆弱性の悪用に初めて成功した日から 10 日後の 2023 年 6 月 6 日でした。最初の PoC は、3 日後の 2023 年 6 月 9 日に公開されました。

注目すべきは、2020 年後半から 2023 年にかけて[20]、FIN11 が 4 つの異なるファイル転送アプリケーションの脆弱性を悪用するパターンを示したことです。その理由は、この種のキャンペーンが FIN11 にいくつかのメリットをもたらすからだと考えられます。この悪用を利用することで、FIN11 は一度に多くの標的を侵害することができます。特定のファイル転送ソフトを標的にすることで戦術的に有利になり、FIN11 のデータ窃盗恐喝のビジネスモデルがサポートされます。FIN11 は、標的環境にラテラル ムーブメントをさらに加えることなく、ファイル転送アプライアンスから標的のファイルを直接入手できます（ラテラル ムーブメントは、攻撃者にとっては時間と労力が必要になり、防御者にとっては侵入検出の機会が増えることになります）。

Mandiant のインシデント対応調査に関連するキャンペーンおよびグローバル イベント（2023 年）

影響を受けた業種

製造
法律および専門サービス
金融サービス
医療
テクノロジー
メディア、エンターテイメント
化学薬品、材料
教育
エネルギー、公共事業
小売
保険
医薬品
通信
自動車
市民社会、非営利団体
建設、エンジニアリング
行政機関
石油、ガス
交通
その他

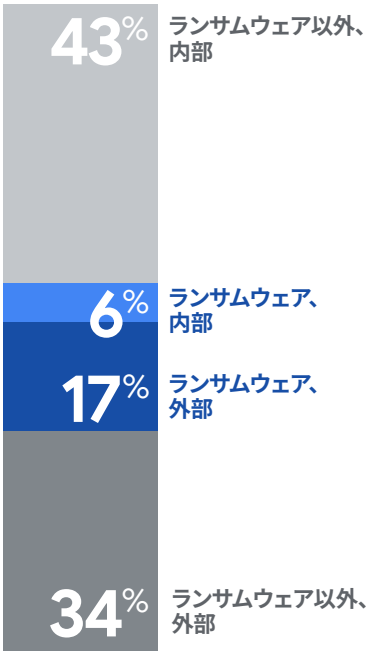
地域の動向

南北アメリカ

このセクションで報告している指標は、北米、中米、南米に所在する組織に影響する Mandiant Consulting の調査に基づいています。

検出元

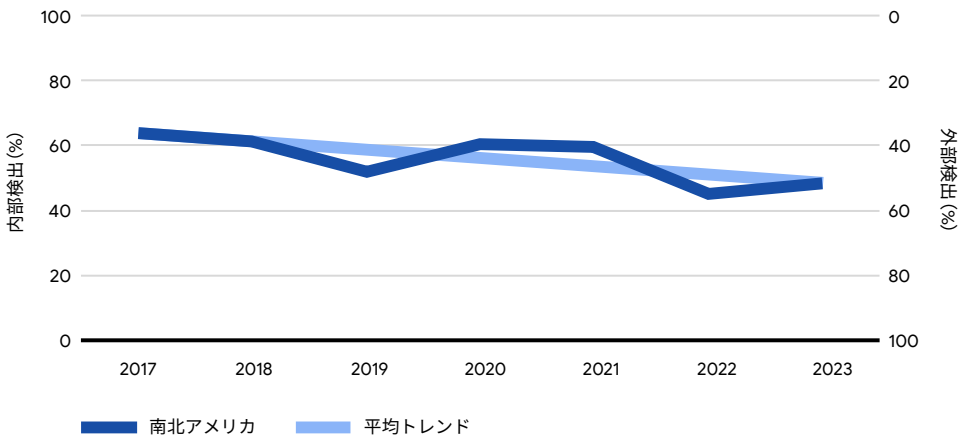
検出元 - 南北アメリカ（2023 年）



2023 年の南北アメリカでは、組織の 51% が最初に外部の情報源から侵害を知らされ、49% が内部で侵害の痕跡を確認しました。この二分化は、内部検出と外部検出のバランスに見られる世界の長期的な傾向と一貫性があるように思われます。これは 2022 年の南北アメリカでの観測結果とも一致し、2017～2021 年までと比較して、全体的に外部通知の割合が高くなる傾向が続いています。過去 4 年間にランサムウェア関連の侵入が増加していることが、この通知元の変化に寄与している可能性があります。

ランサムウェアに関連する侵入を他のすべての侵害から切り離すと、ランサムウェア関連の侵入とそうでない侵入とでは、通知元が大きく異なることが明確になります。南北アメリカで発生したランサムウェア関連の侵入の約 3 分の 2 は外部から通知されたものであり、ランサムノートの形で攻撃者自身から通知されたものが最も多くなっています。その一方で、ランサムウェアによる暗号化とは無関係のケースでは、南北アメリカの半数強の企業が最初に社内で侵害の痕跡を発見しています。

検出元 - 南北アメリカ（2017～2023 年）



滞留時間は、攻撃者が標的環境に侵入してから検出されるまでの日数として算出されます。中央値は、大きさで分類されたデータセットの中点の値を表します。

南北アメリカにおける滞留時間の中央値

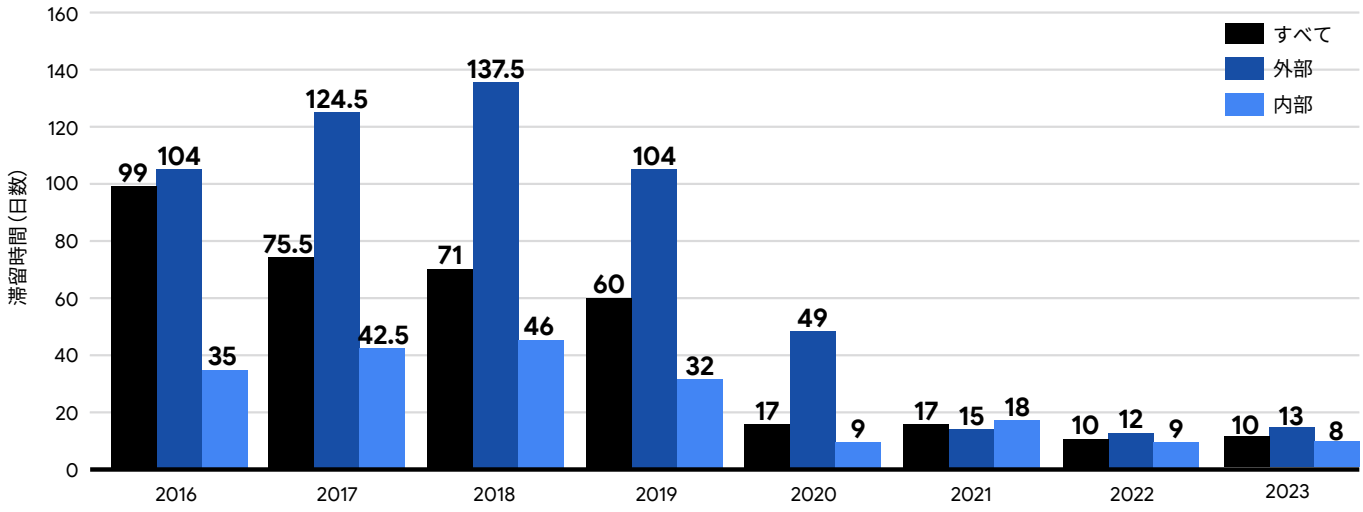
2023 年、南北アメリカの組織は 2022 年と同じペースで侵入を検出しました。南北アメリカにおける滞留時間の中央値は 10 日間でした。外部関係者が侵入を通知するまでの期間は 13 日間で、2022 年の 12 日間と比べて伸びています。しかし、内部で侵入を検出した場合、組織が悪意あるアクティビティを見つけるまでに要した期間は、前年は 9 日間であったのに対し、2023 年は 8 日間でした。

南北アメリカにおける滞留時間の中央値の変化

10 → 10

日間（2022 年） 日間（2023 年）

南北アメリカにおける滞留時間の中央値（2016〜2023 年）

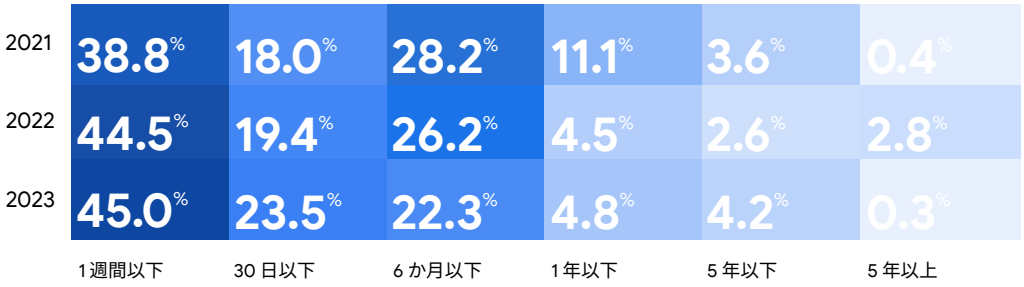


滞留時間の分布

南北アメリカの各組織は、引き続き検出能力を向上させています。組織は 1 週間以内に侵入の 45% を検出しており、この割合は 2022 年とほぼ同じです。Mandiant が実施した調査の 68.5% において、防御側は 30 日以内に侵入を認識しました。これは、2022 年の調査と比較すると 4 ポイント増加しています。

世界的な傾向と同様に、組織はこれまで長期間にわたって検出されないままの侵入を継続的に特定しています。南北アメリカに所在する組織が 5 年以内に検出した侵入にわずかな増加が見られ、5 年が経過しても検出していないままの侵入は減少しました。

南北アメリカにおける滞留時間の分布（2021～2023 年）



南北アメリカのランサムウェアに関する調査からわかった変化

22% → 23%

2022 年　2023 年

南北アメリカにおける滞留時間の中央値の変化 - ランサムウェア

5 → 6

日間 (2022 年)　日間 (2023 年)

南北アメリカにおける滞留時間の中央値の変化 - ランサムウェア以外

12 → 12

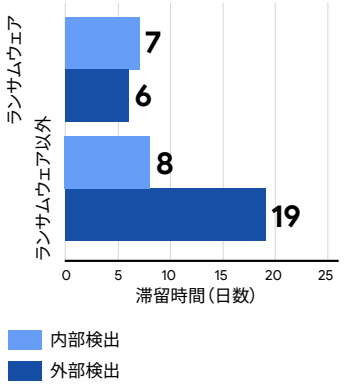
日間 (2022 年)　日間 (2023 年)

ランサムウェアに関する調査

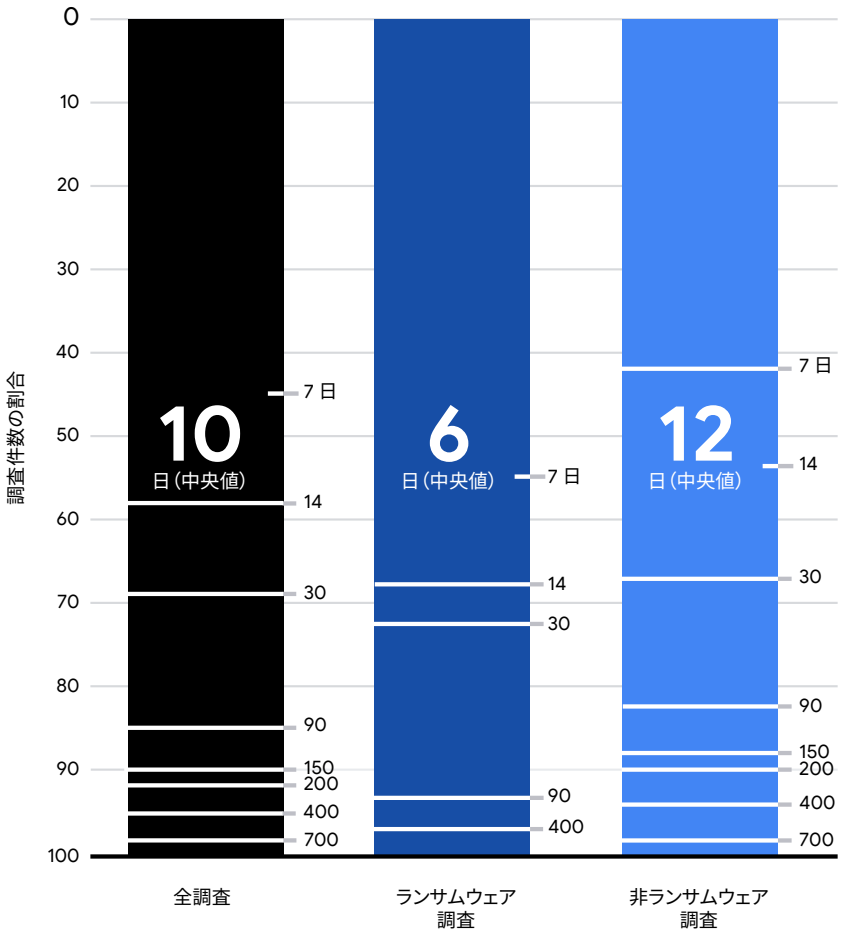
南北アメリカに所在する組織は、ランサムウェアに関連する全体的な侵入を 6 日間で検出し、前回の M-Trends レポート対象期間に確認した 5 日間から伸びています。これは、ランサムウェアに関わる調査がわずかに増加したことや、ランサムウェア攻撃者の攻撃活動遂行能力にわずかな変動があったことに関連している可能性があります。ランサムウェアに関連した侵入の場合、標的組織が内部で悪意のあるアクティビティを検出したのは 7 日後であるのに対し、外部から侵入を知らされたのは 6 日後でした。

ランサムウェアを介さない侵入では、内部検出は依然として組織が侵入を知る最速の方法であり、その滞留時間は 8 日間でした。内部で侵入を検出できなかった場合、南北アメリカの組織は中央値で 19 日以内に外部から侵入を通知されています。

南北アメリカにおける滞留時間の中央値 (検出元別)



南北アメリカにおける滞留時間 (調査タイプ別) (2023 年)



南北アメリカ

脆弱性利用型不正プログラム
41%

フィッシング
18%

過去の侵害
14%

標的型攻撃

初期感染ベクトル

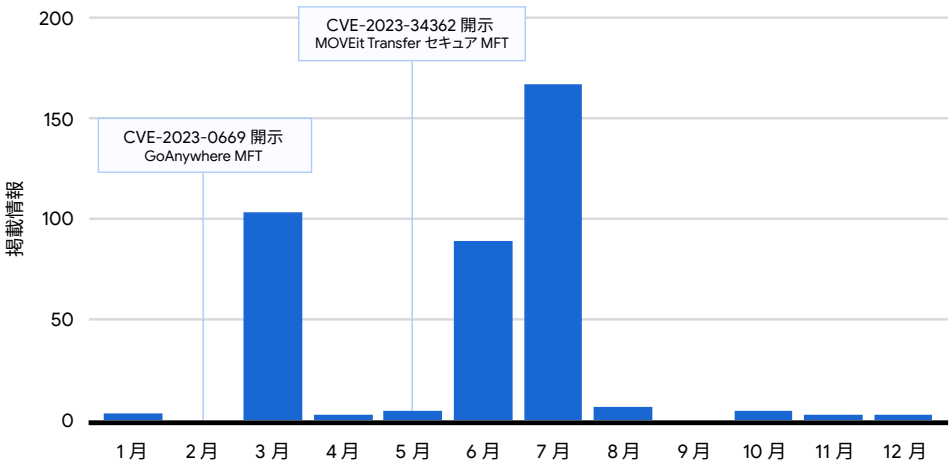
南北アメリカの組織は、世界中の組織が経験したのと同様の脅威に直面しました。初期感染ベクトルが特定された侵入の 41% において、セキュリティ上の脆弱性を利用した不正プログラムがこの地域における攻撃者の活動源でした。フィッシングが侵入の初期ベクトルとして使用された割合は 18% でした。上位 3 つを占めたのは、他の脅威グループやマルウェアから得た過去の不正アクセスを利用した攻撃で、侵入の 14% でした。

脅威グループ

南北アメリカを標的とする脅威グループ

2023 年に南北アメリカで最も頻繁に観測した攻撃者は、金銭目的の脅威グループである FIN11 でした。Mandiant が調査した FIN11 の侵入の大半は、MOVEit Transfer の安全なマネージド ファイル転送（MFT）ソフトウェアの CVE-2023-34362 を悪用した広範なキャンペーンに関連していました[21]。Mandiant は、FIN11 が GoAnywhere MFT の CVE-2023-0669 を悪用した侵入についても調査しました。FIN11 は過去にも CLOP ランサムウェアをデプロイしていますが、これらのキャンペーンでは、攻撃者はランサムウェアによる暗号化を行わず、データ窃盗による恐喝に重点を置いていました。CL0P^_- LEAKS DLS の掲載件数は、Mandiant の調査結果を裏付けるもので、FIN11 がこのような集中的な脆弱性悪用キャンペーンを通じて達成できたスケールの大きさを示しています。

CL0P^_- LEAKS DLS への掲載数（2023 年）



JAPAC

このセクションで報告している指標は、日本およびアジア太平洋（JAPAC）に所在する組織に影響する Mandiant Consulting の調査に基づいています。

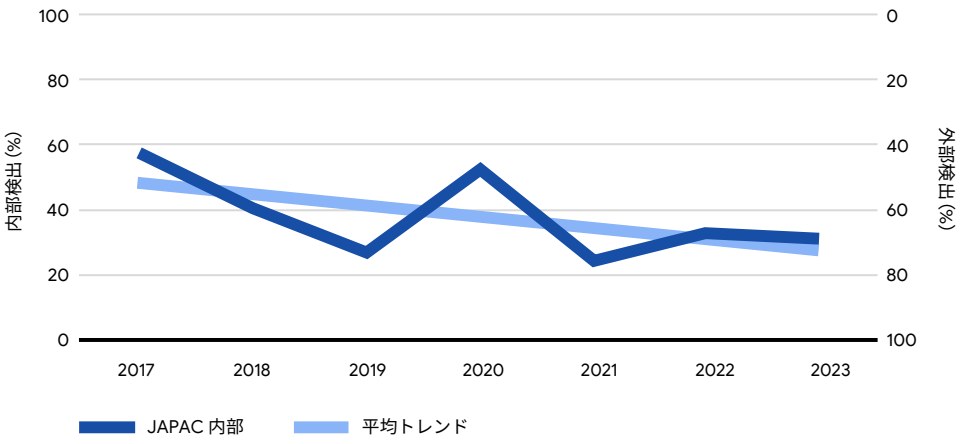
検出元

検出元 - JAPAC（2023 年）

2023 年の JAPAC 地域における侵入において、組織が外部の情報源から侵害を通知されたケースは 69% で、内部で侵入を検出したケースは 31% でした。これは、内部検出の割合が減少傾向にあるという、JAPAC地域における長期的な動向と一致しています。

世界的な数値と同様に、JAPAC に所在する組織では、外部通知によって侵入を把握するケースが多く見られました。2023 年、JAPAC の組織は、ランサムウェア関連の感染の 4 分の 3 を外部の情報源から知らされました。

検出元 - JAPAC（2017～2023 年）



JAPAC における滞留時間の
中央値の変化

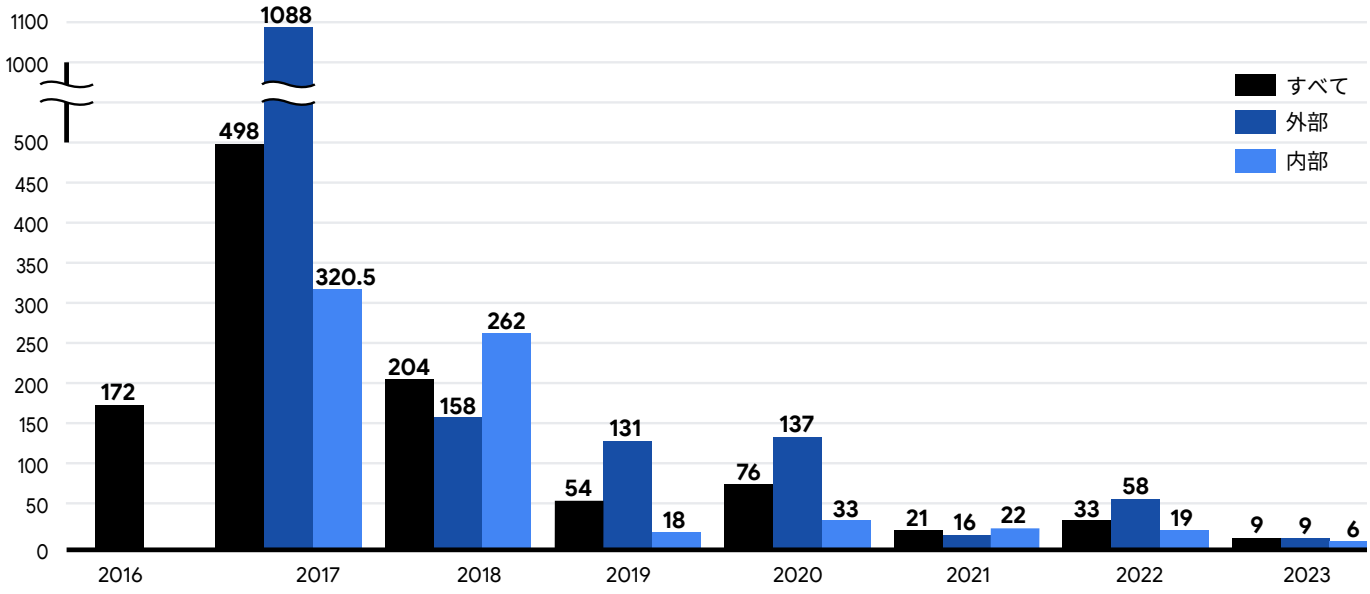
33 ↘ 9

日間（2022 年） 日間（2023 年）

JAPAC における滞留時間の中央値

JAPAC 地域の組織は、継続的に前年よりも早く侵入を検出しています。これはどちらの通知元でも同様でした。JAPAC における滞留時間の中央値は、初期感染から検出までにかかった日数が 2022 年は 33 日間だったのに対し、これまでで最短の 9 日間でした。JAPAC の組織は 6 日間で侵入を内部で特定できました。2022 年の 19 日間と比べて短くなっています。悪意のあるアクティビティに関する外部通知を組織が受け取るまでにかかった時間は 1 週間強の 9 日間で、2022 年の 2 か月近くから大幅に短くなっています。

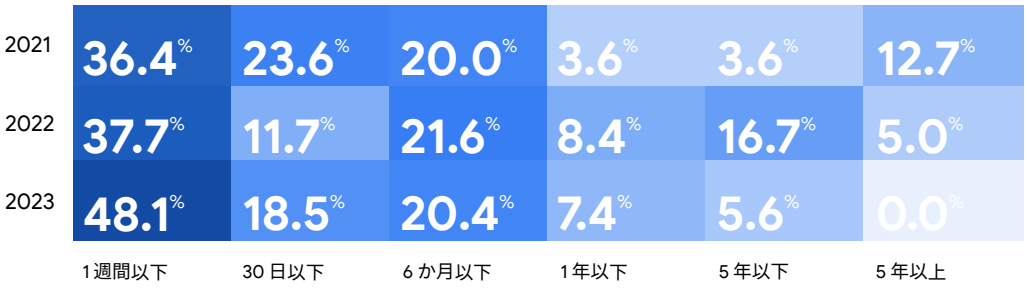
JAPAC における滞留時間の中央値（2016〜2023 年）



滞留時間の分布

2023 年、JAPAC で発生した侵入の 48% において、標的型攻撃者によるアクティビティが 1 週間以内に検出されました。世界での継続的な観測やこの地域の前年比を見ても、侵入の早期検出が継続的に増えており、防御側のレジリエンスが示されています。過去 3 年間、Mandiant は、JAPAC 地域で長期間未検出の侵入が少なくなっていることを確認しています。

JAPAC における滞留時間の分布（2021～2023 年）



JAPAC におけるランサムウェアに関する調査からわかった変化

32% → 33%

2022 年 2023 年

JAPAC における滞留時間の中央値の変化 - ランサムウェア

19 → 3

日間（2022 年） 日間（2023 年）

JAPAC における滞留時間の変化 - ランサムウェア以外

60 → 26

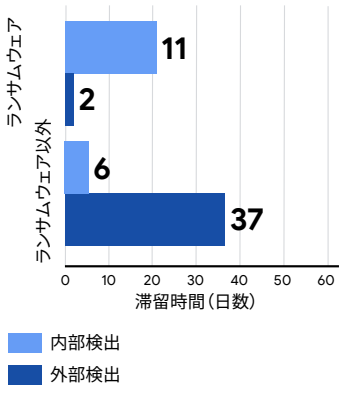
日間（2022 年） 日間（2023 年）

ランサムウェアに関する調査

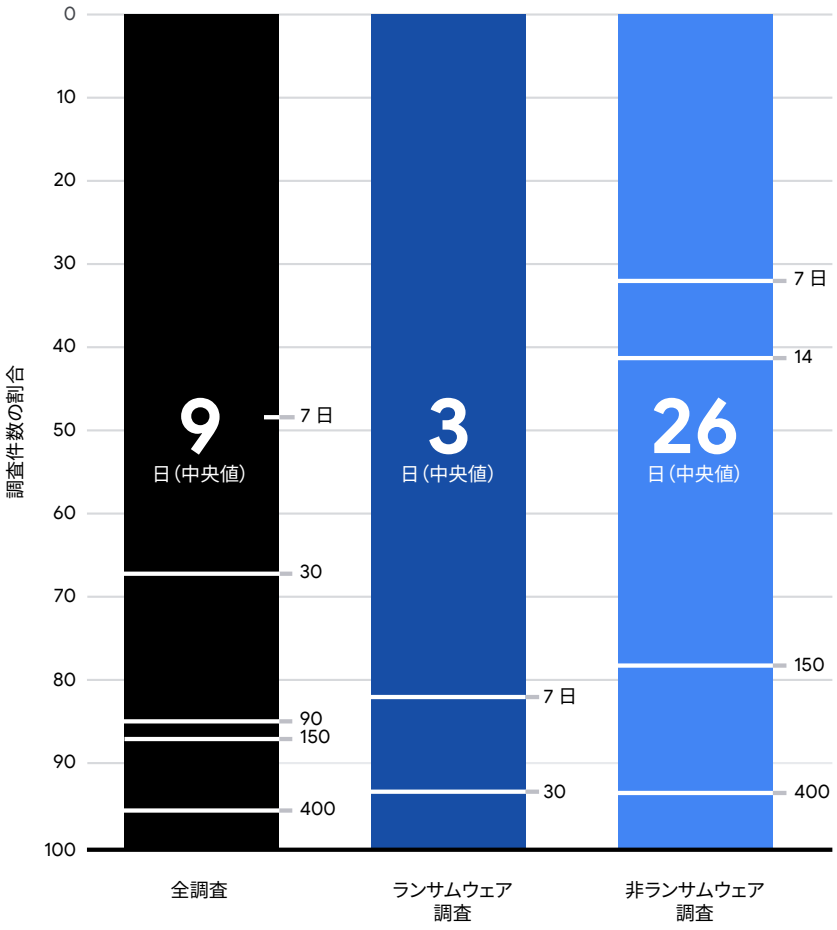
JAPAC では、ランサムウェア関連の侵入の件数にほとんど動きはなく、2023 年に同地域で実施された調査の 33% とわずかに増加しました。しかし、ランサムウェア関連の侵入の滞留時間は、2022 年の 19 日間から 3 日間に短縮しました。この急激な短縮は、ここ数年、侵入に使われるランサムウェア ファミリーが迅速に移り変わっていることが原因と思われます。Mandiant は、ランサムウェア関連の侵入では侵害の速度と徹底度のバランスが取られていることを観測しています。ランサムウェアをデプロイする攻撃者は、検出されにくいように迅速に行動しようとするとともに、最高額の身代金が支払われる可能性を高めるのに十分な潜在的な損害を確保することに細心の注意を払います。

組織は、2023 年にランサムウェアに関連しない侵入を 2022 年に観測された半分強の時間で迅速に検出しました。JAPAC 地域におけるランサムウェアに関連しない侵入の滞留時間の中央値は、2023 年は 26 日間でした。組織は、6 日以内に内部のセキュリティ プロダクトかチームメンバーから侵入を通知されました。しかし、外部からの侵入の通知は、悪意のあるアクティビティが始まってから 37 日後となっています。

JAPAC における滞留時間の中央値（検出元別）



JAPAC における滞留時間（調査タイプ別）（2023 年）



JAPAC

脆弱性利用型不正プログラム
39%

フィッシング
18%

過去の侵害
15%

標的型攻撃

初期感染ベクトル

Mandiant は、JAPAC の組織について、初期感染ベクトルが特定された際、調査の 39% において、脆弱性利用型不正プログラムの影響を受けていることを確認しました。調査のほぼ 5 分の 1（18%）において、攻撃者はこの地域で初期アクセスを獲得するためにブルートフォース手法を利用していました。この地域の初期感染ベクトルで特に多く見られた上位 3 番目は、過去の侵害で獲得したアクセスを使用することでした。侵入の 15% において、Mandiant は攻撃者が元々別の攻撃者によって獲得されたアクセスや、セキュリティで保護されていないバックドア アクセスによって獲得されたアクセスを利用した痕跡を確認しました。過去の侵害の利用が増加しているのは、犯罪的ランサムウェアのエコシステムの内情を表していると考えられます。

脅威グループ

JAPAC を標的とする脅威グループ

2023 年の日本およびアジア太平洋地域で Mandiant が最も多く遭遇したのは、中国のサイバー エスピオナージ クラスタと疑われる UNC4841 でした。

UNC4841 は、遅くとも 2022 年 10 月以来、Barracuda Email Security Gateway（ESG）アプライアンスのゼロデイ脆弱性 CVE-2023-2868 を悪用して、世界中の公的組織および民間組織を標的としたキャンペーンを展開しました[22]。Mandiant は、いくつかのケースで UNC4841 が中国の政治的または戦略的利益に関連するデータを検索し、流出させている痕跡を観測しました。Mandiant は、UNC4841 がデータ窃盗の重点的な対象として選択した一連の機関に、ASEAN 加盟国の外務省のメールドメインとユーザーのほかに、台湾と香港の外国貿易事務所と学術研究機関にいる個人を標的としたシェル スクリプトがあることを発見しました。

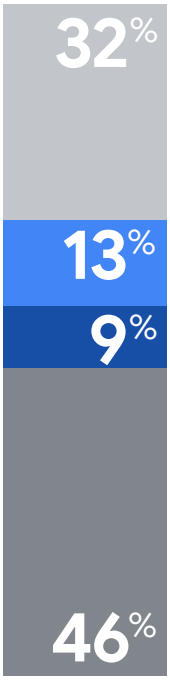
このキャンペーンで、UNC4841 はアクティビティを偽装するために多くの手段を講じていました。たとえば、正規の Barracuda モジュールの名前を使用したり、そうしたモジュールやフィッシング メッセージにマルウェアを挿入したりしていました。迷惑メールフィルタで検出されて、セキュリティ チームによって詳しく調査されないようにすることが目的です。その顕著な例が、最初の脆弱性の開示とその修復作業を受けて、UNC4841 が積極的に反応したことです。すぐにマルウェアを変更し、追加で永続化メカニズムをデプロイしたほか、ラテラル ムーブメントを展開して標的環境へのアクセスを維持しました。この点に関する詳細な分析については、「さまざまな動機に基づくゼロデイ攻撃」をご覧ください。

EMEA

このセクションで報告している指標は、欧州、中東、アフリカ（EMEA）に所在する組織に影響する Mandiant Consulting の調査に基づいています。

検出元

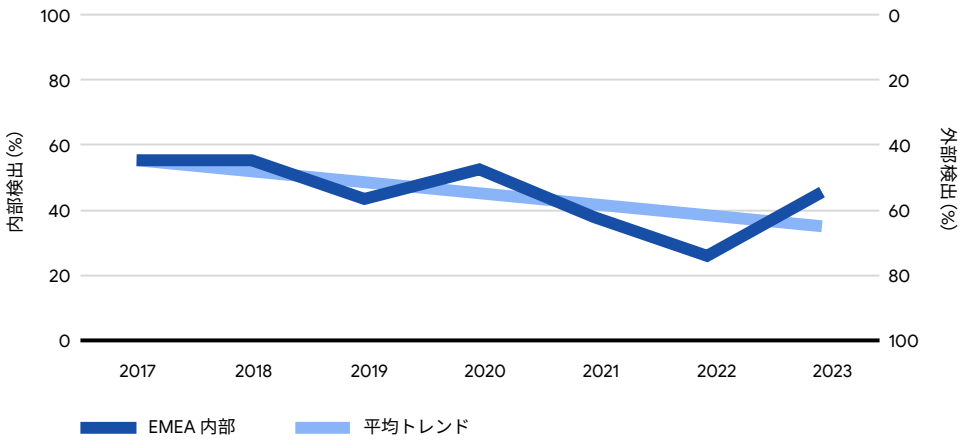
検出元 - EMEA（2023 年）



Mandiant が 2023 年に EMEA で調査したケースでは、組織が最初に侵害の痕跡を内部で発見したのは 46% で、侵入の 54% においては、侵害が外部から通知されていました。この二分化は、2023 年の世界全体の数字と一致し、この地域で長く続く内部通知の減少とは逆の傾向を示しています。

EMEA の組織では、ランサムウェア関連の侵入を内部で確認する頻度が、ランサムノートなどの外部通知で確認する頻度よりも若干高くなっています。ランサムウェアに関連しない侵入の大半は、外部のセキュリティ パートナーによって特定されていました。

検出元 - EMEA（2017〜2023 年）



EMEA における滞留時間の中央値の変化

20 ↗ 22

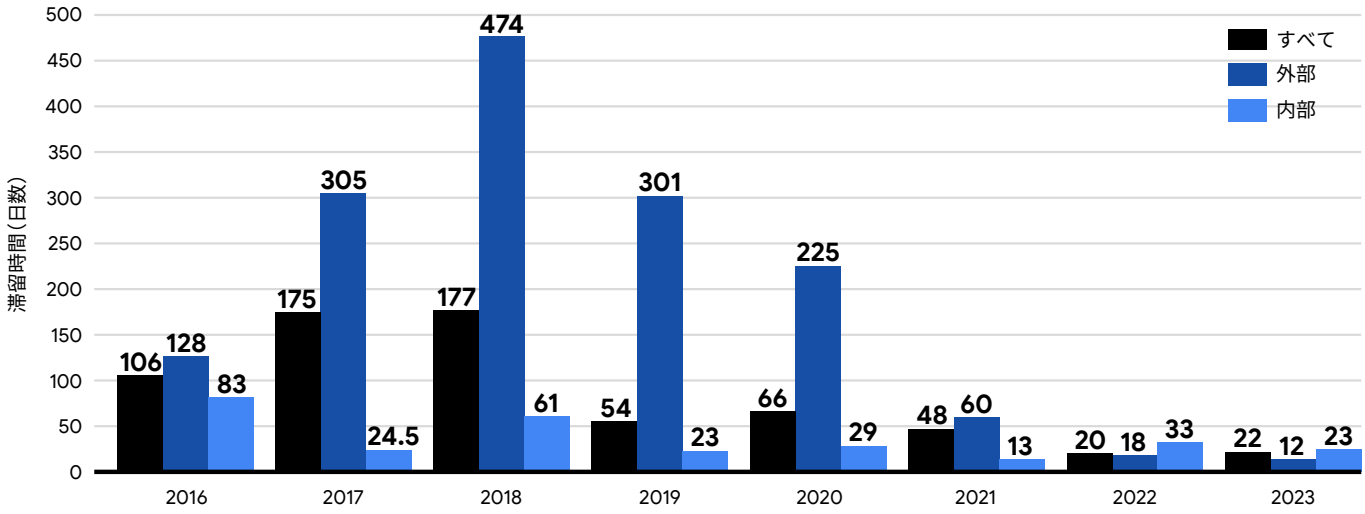
日間（2022 年） 日間（2023 年）

EMEA における滞留時間の中央値

EMEA の組織が侵入を検出するまでの期間は 2023 年は 22 日間で、2022 年の 20 日間から伸びています。外部関係者が侵入を検出した場合の滞留時間は、2022 年の 18 日間に対し、2023 年は 12 日間と、2 週間弱に短縮されました。組織が内部で侵入を検出するまでの期間は 2023 年は 23 日間で、2022 年の 33 日間から短くなっています。

長年にわたり、滞留時間は EMEA の検出元によって異なってきました。一般的な傾向として、滞留時間の中央値は年々減少し続けており、2022 年の滞留時間の中央値はこの地域で最も短くなりました。2023 年にわずかに変動が見られたのは、地域データが正規化したためと考えられます。Mandiant が 2022 年にウクライナで行った作業の注目すべき部分です。

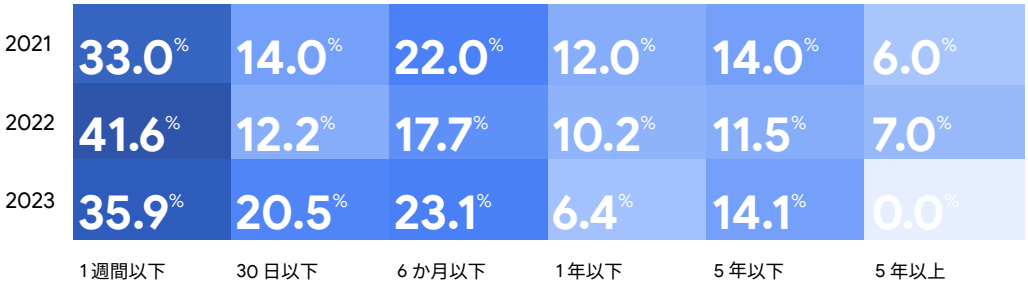
EMEA における滞留時間の中央値（2016〜2023 年）



滞留時間の分布

EMEA では今年、例年に比べて組織によって侵入が検出されない期間が長くなりました。この地域で実施された調査の 14% においては、最長で 5 年間も未検出のままでした。しかし、2023 年、5 年が経過しても侵入が検出されていないのは、調査の 1% 未満にとどまりました。

EMEA における滞留時間の分布（2021〜2023 年）



EMEA のランサムウェアに関する調査からわかった変化

7% → 22%

2022 年 2023 年

EMEA における滞留時間の中央値の変化 - ランサムウェア

33 → 8

日間 (2022 年) 日間 (2023 年)

EMEA における滞留時間の変化 - ランサムウェア以外

19 → 31

日間 (2022 年) 日間 (2023 年)

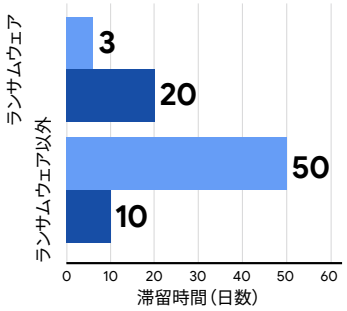
ランサムウェアに関する調査

EMEA で Mandiant と提携している組織では、ランサムウェアに関連する侵入が 2021 年に見られた件数に戻っています。同地域で実施された調査のほぼ 4 分の 1 がランサムウェアに関連するもので、2022 年の 7% に対し、2023 年は 22% となりました。

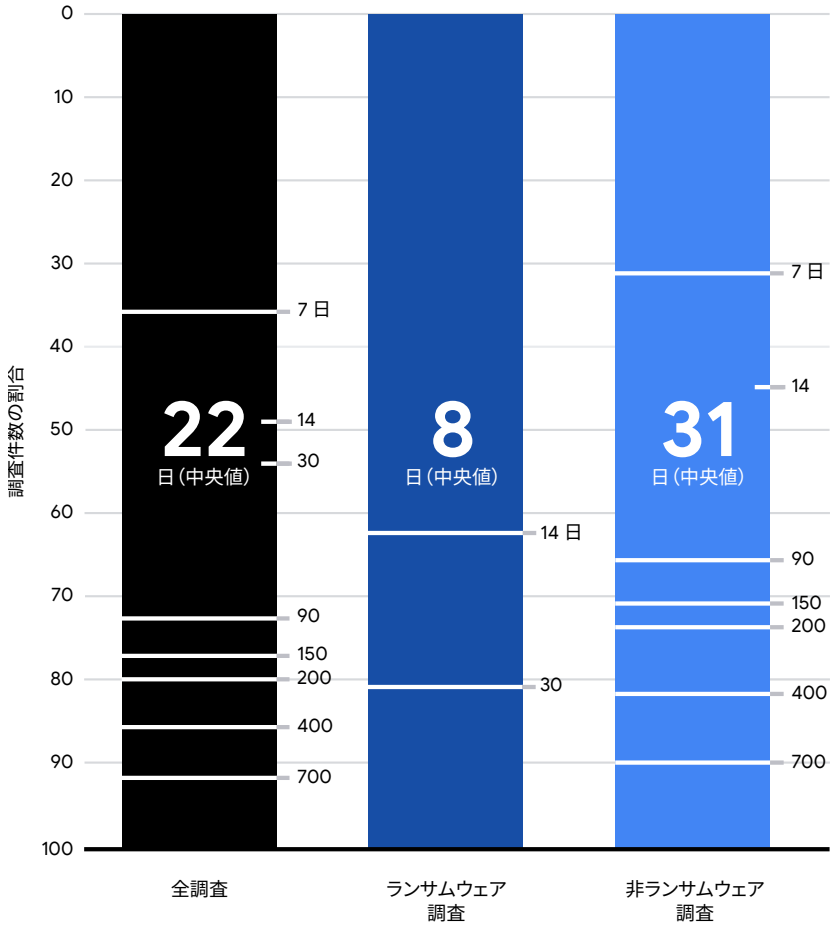
この地域では、ランサムウェア関連の侵入の滞留時間の中央値が減少しました。ランサムウェアの侵入を検出するまでの期間は 1 週間強の 8 日間で、2022 年の 33 日間に比べて短くなっています。EMEA では、ランサムウェアの侵入を検出するまでに内部検出では 3 日間、外部通知では 20 日間かかっています。

ランサムウェアに関連しない侵入を検出するまでの期間は、2022 年は 19 日間、2023 年は 31 日間でした。ランサムウェアに関連しない侵入が内部で検出された場合、検出されないままの期間が長くなっています。

EMEA における滞留時間の中央値 (検出元別)



EMEA における滞留時間 (調査タイプ別) (2023 年)



EMEA

Exploit
37%

Prior Compromise
21%

Phishing
16%

標的型攻撃

初期感染ベクトル

EMEA では、初期感染ベクトルが特定された際、侵入の 36% が脆弱性利用型不正プログラムから始まったと Mandiant は指摘しています。EMEA の組織への侵入の 21% が以前に獲得したアクセスを悪用したもので、16% がフィッシングによるものでした。

脅威グループ

EMEA を標的とする脅威グループ

Mandiant は 2023 年、EMEA で UNC4393 に起因する侵害を含むさまざまな侵入を調査しました。UNC4393 は、金銭目的の脅威クラスタであり、BASTA ランサムウェアをデプロイすることでアクセスを収益化しています。このクラスタは単独では機能せず、標的環境への初期アクセスを獲得するために他の攻撃者に依存しています。2023 年の大半を通じて、Mandiant は UNC2500 と UNC2633 の QAKBOT 感染が、標的環境において一貫して UNC4393 のアクティビティに先行していることを確認しました。2023 年 8 月、国際的な法執行機関の取り組みにより、QAKBOT ボットネットが解体されました[23]。これにより、UNC2500 は活動を継続するために代替のマルウェアのペイロードに移行せざるを得なくなりました。2023 年 9 月中旬から UNC2500 が DARKGATE ペイロードを配布し始め、UNC4393 がこのペイロードを利用して最終的に BASTA ランサムウェアをデプロイしたことをたことを Mandiant は観測しました。

Mandiant は、複数の攻撃者が侵害のさまざまな段階に関与している痕跡を定期的に観測しており、過去のセキュリティ侵害は、2023 年の Mandiant のインシデント対応で 3 番目に多い初期アクセス ベクトルでした。複数の攻撃者による侵入の複雑さと、攻撃者の戦術、手法、手順（TTP）の進化の速さは、攻撃者が環境に足場を築くことによる影響を最小化するために、多層防御戦略を実装することの重要性を裏付けています。

MITRE ATT&CK

Mandiant の標的型攻撃ライフサイクルに関連する手法（2023 年）

Mandiant の標的型攻撃ライフサイクルとは、サイバー攻撃者が攻撃を実行するために使用するイベントの予測可能なシーケンスのことです。

初期偵察

偵察

T1595: アクティブ スキャン	1.1%	T1595.001: IP ブロックのスキャン	0.6%
		T1595.002: 脆弱性スキャン	0.6%

リソース開発

T1608: ステージ機能	12.8%	T1608.003: デジタル証明書のインストール	6.6%
		T1608.005: リンク ターゲット	2.6%
		T1608.001: マルウェアのアップロード	2.1%
		T1608.002: ツールのアップロード	0.9%
		T1608.006: SEO ポイズニング	0.9%
T1583: インフラストラクチャ取得	5.4%	T1583.003: 限定公開の仮想サーバー	5.4%
T1584: インフラストラクチャの侵害	3.2%		
T1587: 機能の開発	2.3%	T1587.002: コード署名証明書	1.3%
		T1587.003: デジタル証明書	0.9%
T1588: 機能の入手	1.5%	T1588.004: デジタル証明書	1.1%
		T1588.003: コード署名証明書	0.4%
T1585: アカウント開設	0.2%	T1585.002: メール アカウント	0.2%

初期侵害

初期アクセス

T1190: 一般公開されているアプリケーションの悪用	28.7%		
T1133: 外部リモート サービス	20.3%		
T1566: フィッシング	16.3%	T1566.001: 添付ファイルのスピアフィッシング	5.1%
		T1566.002: リンクのスピアフィッシング	3.2%
		T1566.004: 音声のスピアフィッシング	1.9%
		T1566.003: サービスを介したスピアフィッシング	0.8%
T1078: 有効なアカウント	11.3%	T1078.004: クラウド アカウント	2.1%
		T1078.001: デフォルトのアカウント	0.2%
T1189: ドライブバイ侵害	3.4%		
T1195: サプライ チェーンの侵害	0.8%	T1195.002: ソフトウェア サプライ チェーンの侵害	0.6%
T1199: 信頼関係	0.8%		
T1091: リムーバブル メディアを介したレプリケーション	0.6%		
T1200: ハードウェアの追加	0.2%		

足場確立

永続性

T1543: システム プロセスの作成または変更	28.3%	T1543.003: Windows サービス	16.7%
		T1543.002: Systemd サービス	0.9%
		T1543.004: デーモンの起動	0.4%
		T1543.001: エージェントの起動	0.2%
T1098: アカウント操作	18.6%	T1098.005: デバイスの登録	2.1%
		T1098.004: SSH 認証鍵	1.7%
		T1098.001: 追加のクラウド認証情報	0.4%
T1053: 計画的タスク / ジョブ	18.0%	T1053.005: 計画的タスク	14.8%
		T1053.003: cron	1.7%
T1003: OS 認証情報のダンプ	16.9%	T1003.003: NTDS	7.1%
		T1003.001: LSASS メモリ	5.4%
		T1003.002: セキュリティ アカウント マネージャー	3.0%
		T1003.008: /etc/passwd と /etc/shadow	2.4%
		T1003.006: DCSync	0.4%
		T1003.004: LSA シークレット	0.2%
T1505: サーバー ソフトウェアのコンポーネント	14.4%	T1505.003: ウェブシェル	14.3%
		T1505.001: SQL ストアド プロシージャ	0.2%
		T1505.004: IIS コンポーネント	0.2%
T1136: アカウントの作成	11.8%	T1136.001: ローカル アカウント	5.4%
		T1136.002: ドメイン アカウント	1.1%
		T1136.003: クラウド アカウント	0.6%
T1574: ハイジャックの実行フロー	10.3%	T1574.011: サービス レジストリの権限弱点	8.6%
		T1574.002: DLL サイド ローディング	1.1%
		T1574.001: DLL 検索順序のハイジャック	0.4%
		T1574.008: 検索順序のハイジャックによるパスの傍受	0.4%
		T1574.006: 動的リンカーのハイジャック	0.2%
T1547: 自動起動実行の起動またはログオン	9.6%	T1547.001: レジストリ実行キー / スタートアップ フォルダ	7.1%
		T1547.009: ショートカット修正	2.6%
		T1547.004: Winlogon ヘルパー DLL	0.4%
		T1547.011: Plist 変更	0.2%
T1552: セキュリティが確保されていない認証情報	8.8%	T1552.002: レジストリ内の認証情報	2.4%
		T1552.004: 秘密鍵	1.7%
		T1552.001: ファイル内の認証情報	1.3%
		T1552.003: Bash 履歴	0.9%
		T1552.006: グループ ポリシーの設定	0.8%
		T1555.005: パスワード マネージャー	0.8%
T1056: 入力キャプチャ	8.1%	T1056.001: キーロギング	7.5%
		T1056.002: GUI 入力キャプチャ	0.6%
		T1056.003: ウェブポータル キャプチャ	0.2%

T1110: ブルート フォース	7.3%	T1110.001: パスワード推測	2.8%
		T1110.003: パスワード スプレー	1.1%
		T1110.004: クレデンシャル スタッフィング	0.8%
T1555: パスワード ストアにある認証情報	5.4%	T1555.003: ウェブブラウザにある認証情報	3.2%
		T1555.004: Windows Credential Manager	2.8%
		T1555.006: クラウド シークレット管理ストア	0.9%
		T1555.005: パスワード マネージャー	0.8%
		T1555.001: キーチェーン	0.2%
T1546: イベント トリガーによる実行	3.4%	T1546.003: Windows Management Instrumentation イベントの登録	2.8%
		T1546.008: ユーザー補助機能	0.4%
		T1546.010: AppInit DLL	0.2%
		T1546.015: コンポーネント オブジェクト モデルの ハイジャック	0.2%
T1111: 多要素認証の傍受	3.2%		
T1558: Kerberos チケットの窃盗または偽造	3.2%	T1558.003: Kerberoasting	1.7%
T1556: 認証プロセスの修正	1.7%	T1556.006: 多要素認証	1.1%
		T1556.002: パスワード フィルタ DLL	0.2%
		T1556.003: プラグ可能な認証モジュール	0.2%
T1037: 初期化スクリプトの起動またはログオン	0.9%	T1037.004: RC スクリプト	0.6%
T1187: 強制認証	0.8%		
T1539: ウェブ セッション Cookie の窃盗	0.8%		
T1649: 認証証明書の窃盗または偽造	0.4%		
T1557: 中間者攻撃	0.2%	T1557.00: LLMNR/NBT-NS ポイズニングと SMB リレー	0.2%
T1621: 多要素認証リクエスト生成	0.2%		

権限の昇格

権限昇格

T1543: システム プロセスの作成または変更	28.3%	T1543.003: Windows サービス	16.7%
		T1543.005: 計画的タスク	14.8%
		T1543.002: Systemd サービス	0.9%
		T1543.004: デーモンの起動	0.4%
		T1543.001: エージェントの起動	0.2%
T1055: プロセス インジェクション	25.1%	T1055.003: スレッド実行のハイジャック	1.3%
		T1055.004: 非同期プロシージャ コール	0.9%
		T1055.001: ダイナミック リンク ライブラリ インジェクション	0.8%
		T1055.002: ポータブル実行可能インジェクション	0.4%
		T1055.012: 空洞化の処理	0.4%
T1053 計画的タスク / ジョブ	18%	T1053.003: cron	1.7%
T1134: アクセス トークンの操作	13.7%	T1134.001: トークンの偽装 / 窃盗	4.9%
		T1134.004: 親 PID なりすまし	0.6%
T1547: 自動起動実行の起動またはログオン	9.6%	T1547.001: レジストリ実行キー / スタートアップ フォルダ	7.1%
		T1547.009: ショートカット修正	2.6%
		T1547.004: Winlogon ヘルパー DLL	0.4%
		T1547.011: Plist 変更	0.2%
T1546: イベント トリガーによる実行	3.4%	T1546.003: Windows Management Instrumentation イベントの登録	2.8%
		T1546.008: ユーザー補助機能	0.4%
		T1546.010: AppInit DLL	0.2%
		T1546.015: コンポーネント オブジェクト モデルのハイジャック	0.2%
T1484: ドメイン ポリシーの修正	1.5%	T1484.001: グループ ポリシーの修正	1.5%
T1037: 初期化スクリプトの起動またはログオン	0.9%	T1037.004: RC スクリプト	0.6%
T1548: 昇格管理メカニズムの乱用	0.8%	T1548.002: ユーザー アカウント管理のバイパス	0.8%
T1068: 権限昇格用の脆弱性利用型不正プログラム	0.6%		

内部偵察

発見

T1083: ファイルとディレクトリの探索	38.6%		
T1082: システム情報の探索	37.1%		
T1033: システム オーナー / ユーザーの探索	31.7%		
T1087: アカウントの探索	28.1%	T1087.002: ドメイン アカウント	15.0%
		T1087.001: ローカル アカウント	10.5%
		T1087.004: クラウド アカウント	0.8%
T1012: クエリ レジストリ	24.8%		
T1016: システム ネットワーク構成の検出	23.5%	T1016.001: インターネット接続の検出	5.3%
T1622: デバッガ回避	21.8%		
T1057: プロセスの探索	18.9%		
T1003: OS 認証情報のダンプ	16.9%	T1003.003: NTDS	7.1%
		T1003.001: LSASS メモリ	5.4%
		T1003.002: セキュリティ アカウント マネージャー	3.0%
		T1003.008: /etc/passwd と /etc/shadow	2.4%
		T1003.006: DCSync	0.4%
		T1003.004: LSA シークレット	0.2%
T1518: ソフトウェアの探索	16.3%	T1518.001: セキュリティ ソフトウェアの探索	1.3%
T1614: システムの位置の探索	15.9%	T1614.001: システム言語の探索	9.6%
T1069: 権限グループの探索	14.8%	T1069.002: ドメイン グループ	11.1%
		T1069.001: ローカル グループ	1.3%
		T1069.003: クラウド グループ	1.1%
T1482: ドメイン信頼の探索	12.6%		
T1497: 仮想化 / サンドボックス化の回避	12.2%	T1497.001: システム確認	10.1%
T1007: システム サービスの探索	11.4%		
T1552: セキュリティが確保されていない認証情報	8.8%	T1552.002: レジストリ内の認証情報	2.4%
		T1552.004: 秘密鍵	1.7%
		T1552.001: ファイル内の認証情報	1.3%
		T1552.003: Bash 履歴	0.9%
		T1552.006: グループ ポリシーの設定	0.8%
T1049: システム ネットワーク接続の探索	8.1%		
T1056: 入力キャプチャ	8.1%	T1056.001: キーロギング	7.5%
		T1056.002: GUI 入力キャプチャ	0.6%
		T1056.003: ウェブポータル キャプチャ	0.2%
T1110: ブルート フォース	7.3%	T1110.001: パスワード推測	2.8%
		T1110.003: パスワード スプレー	1.1%
		T1110.004: クレデンシャル スタッフィング	0.8%
T1010: アプリケーション ウィンドウの探索	7.1%		

T1135: ネットワーク共有の探索	6.8%		
T1555: パスワード ストアにある認証情報	5.4%	T1555.003: ウェブブラウザにある認証情報	3.2%
		T1555.004: Windows Credential Manager	2.8%
		T1555.006: クラウド シークレット管理ストア	0.9%
		T1555.005: パスワード マネージャー	0.8%
		T1555.001: キーチェーン	0.2%
T1046: ネットワーク サービスの探索	3.4%		
T1111: 多要素認証の傍受	3.2%		
T1558: Kerberos チケットの窃盗または偽造	3.2%	T1558.003: Kerberoasting	1.7%
T1018: リモート システムの探索	2.8%		
T1556: 認証プロセスの修正	1.7%	T1556.006: 多要素認証	1.1%
		T1556.002: パスワード フィルタ DLL	0.2%
		T1556.003: プラグ可能な認証モジュール	0.2%
T1580: クラウド インフラストラクチャの探索	1.5%		
T1124: システム時間の探索	1.3%		
T1619: クラウド ストレージ オブジェクトの探索	1.3%		
T1040: ネットワーク スニッフィング	0.8%		
T1615: グループ ポリシーの探索	0.8%		
T1187: 強制認証	0.8%		
T1539: ウェブ セッション Cookie の窃盗	0.8%		
T1526: クラウド サービスの探索	0.6%		
T1120: 周辺機器の探索	0.4%		
T1201: パスワード ポリシーの探索	0.4%		
T1538: クラウド サービス ダッシュボード	0.4%		
T1649: 認証証明書の窃盗または偽造	0.4%		
T1217: ブラウザ ブックマークの探索	0.2%		
T1557: 中間者攻撃	0.2%	T1557.001: LLMNR/NBT-NS ポイズニングと SMB リレー	0.2%
T1621: 多要素認証リクエスト生成	0.2%		

ラテラル ムーブメント

ラテラル ムーブメント

T1021: リモート サービス	37.3%	T1021.001: Remote Desktop Protocol	28.3%
		T1021.004: SSH	10.3%
		T1021.002: SMB / Windows 管理者共有	10.1%
		T1021.006: Windows リモート管理	1.3%
		T1021.005: VNC	0.8%
T1570: ラテラルツール移行	2.3%		
T1563: リモート サービス セッション ハイジャック	2.1%	T1563.002: RDP ハイジャック	0.4%
T1550: 代替認証マテリアルの使用	1.7%	T1550.001: アプリケーションのアクセス トークン	1.1%
		T1550.002: ハッシュを渡す	0.6%
		T1550.004: ウェブ セッション Cookie	0.2%
T1534: 内部スピアフィッシング	0.6%		
T1091: リムーバブル メディアを介したレプリケーション	0.6%		
T1072: ソフトウェア デプロイツール	0.2%		
T1080: Taint 共有コンテンツ	0.2%		

プレゼンス維持

永続性

T1027: ファイルまたは情報の難読化	46.5%	T1027.009: 埋め込みペイロード	9.6%
		T1027.002: ソフトウェア パッキング	8.6%
		T1027.010: コマンド難読化	3.9%
		T1027.004: 配信後のコンパイル	1.3%
		T1027.005: ツールからのインジケーターの削除	0.4%
		T1027.001: バイナリ パディング	0.2%
		T1027.003: Steganography	0.2%
		T1027.008: 削除されたペイロード	0.2%
T1070: インジケーターの削除	35.1%	T1070.004: ファイルの削除	26.6%
		T1070.009: 永続性をクリア	9.0%
		T1070.006: Timestomp	7.1%
		T1070.001: Windows イベントログの消去	5.6%
		T1070.007: ネットワーク接続履歴と構成の消去	3.4%
		T1070.005: ネットワーク共有接続の削除	1.1%
		T1070.003: コマンド履歴の消去	0.6%
		T1070.002: Linux または Mac のシステムログの消去	0.4%
		T1070.008: メールボックス データの消去	0.2%
T1140: ファイルまたは情報の難読化解除 / デコード	31.5%		
T1543: システム プロセスの作成または変更	28.3%	T1543.003: Windows サービス	16.7%
		T1543.002: Systemd サービス	0.9%
		T1543.004: デーモンの起動	0.4%
		T1543.001: エージェントの起動	0.2%
T1112: レジストリの修正	26.5%		
T1564: アーティファクトの非表示	19.5%	T1564.003: ウィンドウの非表示	14.8%
		T1564.001: ファイルとディレクトリの非表	4.7%
		T1564.008: メール非表示ルール	2.1%
		T1546.008: ユーザー補助機能	0.4%
		T1564.011: プロセス中断を無視	0.2%
T1562: 防御の侵害	18.6%	T1562.001: ツールの無効化または変更	13.3%
		T1562.004: システム ファイアウォールの無効化または変更	7.9%
		T1562.002: Windows イベント ロギングの無効化	4.3%
		T1562.010: 攻撃のダウングレード	0.9%
		T1562.003: コマンド履歴ロギングの侵害	0.9%
		T1562.009: セーフモード起動	0.2%
T1053: 計画的タスク / ジョブ	18.0%		

T1218: システム バイナリ プロキシ実行	16.1%	T1218.011: Rundll32	12.9%
		T1218.010: Regsvr32	1.7%
		T1218.005: Mshta	1.3%
		T1218.007: Msiexec	0.9%
		T1218.014: MMC	0.4%
		T1218.001: コンパイル済み HTML ファイル	0.2%
T1036: マスカレード	11.8%	T1036.001: 無効なコード署名	6.8%
		T1036.008: ファイル形式のマスカレード	0.8%
		T1036.005: 正規の名前または位置の照合	0.8%
		T1036.003: システム ユーティリティ名の変更	0.2%
T1547: 自動起動実行の起動またはログオン	9.6%	T1547.001: レジストリ実行キー / スタートアップ フォルダ	7.1%
		T1547.009: ショートカット修正	2.6%
		T1547.004: Winlogon ヘルパー DLL	0.4%
		T1547.011: Plist 変更	0.2%
T1202: 間接的コマンド実行	8.6%		
T1620: リフレクト コード読み込み	8.6%		
T1222: ファイルとフォルダの権限の修正	7.9%	T1222.002: Linux と Mac のファイルとディレクトリの権限の修正	4.1%
		T1222.001: Windows のファイルとディレクトリの権限の修正	1.1%
T1546: イベント トリガーによる実行	3.4%	T1546.003: Windows Management Instrumentation イベントの登録	2.8%
		T1564.010: 処理引数のなりすまし	0.2%
		T1546.010: AppInit DLL	0.2%
		T1546.015: コンポーネント オブジェクト モデルのハイジャック	0.2%
T1556: 認証プロセスの修正	1.7%	T1556.006: 多要素認証	1.1%
		T1556.002: パスワード フィルタ DLL	0.2%
		T1556.003: プラグ可能な認証モジュール	0.2%
T1037: 初期化スクリプトの起動またはログオン	0.9%	T1037.004: RC スクリプト	0.6%
T1006: 直接ボリューム アクセス	0.8%		
T1553: トラスト管理の無効化	0.8%	T1553.002: コード署名	0.6%
		T1553.005: Mark of the Web バイパス	0.2%
T1578: クラウド コンピューティング インフラストラクチャの変更	0.6%	T1578.002: クラウド インスタンスの作成	0.6%
		T1578.005: クラウド コンピューティング構成の修正	0.2%
T1207: 不正ドメイン コントローラ	0.4%		
T1014: ルートキット	0.4%		
T1480: 実行ガードレール	0.2%		
T1601: システム イメージの変更	0.2%	T1601.001: パッチシステム イメージ	0.2%
T1647: Plist ファイル変更	0.2%		
T1127: 信頼できるデベロッパー ユーティリティ プロキシ実行	0.2%	T1127.001: MSBuild	0.2%
T1220: XSL スクリプト処理	0.2%		

目的の達成

コレクション

T1213: 情報リポジトリにあるデータ	16.7%	T1213.002: SharePoint	8.4%
		T1213.001: Confluence	0.4%
		T1213.003: コード リポジトリ	0.2%
T1560: アーカイブ収集データ	14.6%	T1560.001: ユーティリティ経由のアーカイブ	7.5%
		T1560.002: ライブラリ経由のアーカイブ	0.8%
T1056: 入力キャプチャ	8.1%	T1056.001: キーロギング	7.5%
		T1056.002: GUI 入力キャプチャ	0.6%
		T1056.003: ウェブポータル キャプチャ	0.2%
T1074: データのステージング	5.4%	T1074.001: ローカルデータのステージング	4.7%
		T1074.002: リモートデータのステージング	0.4%
T1115: クリップボードのデータ	5.3%		
T1113: スクリーン キャプチャ	4.7%		
T1125: 動画キャプチャ	3.9%		
T1114: メール収集	2.4%	T1114.002: リモートメール収集	0.6%
		T1114.001: ローカルメール収集	0.2%
T1039: ネットワーク共有デバイスにあるデータ	1.7%		
T1005: ローカル システムにあるデータ	0.8%		
T1530: クラウド ストレージにあるデータ	0.6%		
T1602: 構成リポジトリにあるデータ	0.4%	T1602.002: ネットワーク デバイス構成のダンプ	0.4%
T1119: 自動収集	0.2%		
T1123: 音声キャプチャ	0.2%		
T1557: 中間者攻撃	0.2%	T1557.001: LLMNR/NBT-NS ポイズニングと SMB リレー	0.2%

データの抽出

T1567: ウェブサービスの抽出	5.6%	T1567.002: クラウド ストレージへの抽出	2.4%
		T1567.003: テキスト ストレージ サイトへの抽出	0.2%
T1041: C2 チャネルの抽出	3.6%		
T1020: 自動抽出	1.1%		
T1052: 物理メディアへの抽出	0.2%	T1052.001: USB による抽出	0.2%

影響

T1486: 影響のためのデータ暗号化	25.5%		
T1489: サービス ストップ	15.9%		
T1657: 金融窃盗	7.9%		
T1529: システム シャットダウン / 再起動	6.9%		
T1490: システム復旧の抑制	5.8%		
T1485: データの破壊	2.8%		
T1496: リソース ハイジャック	2.3%		
T1565: データの操作	2.3%	T1565.001: 保存されたデータの操作	2.3%
T1531: アカウントへのアクセスの解除	1.7%		
T1491: 改変	1.1%	T1491.002: 外部改変	0.2%
T1561: ディスクのワイプ	0.6%	T1561.001: ディスクのコンテンツのワイプ	0.4%
T1498: ネットワーク サービス拒否攻撃	0.2%	T1498.001: 直接ネットワーク フラッド	0.2%
T1499: エンドポイント サービス拒否攻撃	0.2%		

コラム

可視性のギャップを狙った中国のスパイ活動

エンドポイント検出対応（EDR）プラットフォームは、セキュリティ モニタリングのベースラインを提供するために必要なエンドポイントのアクティビティに対する可視性の拡大を求める企業の間で一般的になりました。このように可視性が高まったことで、攻撃者は攻撃活動の有効性を維持するために進化することを余儀なくされています。EDR をバイパスする手法に投資する攻撃者もいれば、徹底した可視化がまだ一般的でない企業環境の領域に焦点を当てる攻撃者もいます。EDR エージェントはセキュリティ デプロイの標準機能となりましたが、組織にとって重要なアセットを分割またはホストする多くの専用アプライアンスでは、同様のレベルの可視性が欠如していることがよくあります。そのようなシステムは、その可視性のギャップがゆえに攻撃が検出される危険性が低く、長期的な持続性を維持できるため、攻撃者にとって新たな安住の地となっています。

EDR のデプロイにほとんど対応していないデバイスの一般的な例としては、ファイアウォール メールフィルタリング プロダクト、仮想化プラットフォーム、バーチャル プライベート ネットワーク（VPN）ソリューションなどがあります。さらに問題を複雑にしているのは、これらのアプライアンスが構築されているプラットフォームです。独占的なテクノロジーなどでロックされていて、フォレンジック分析作業の妨げとなっています。これらのデバイス用の脆弱性利用型不正プログラムは、攻撃者にとって非常に貴重です。なぜなら、通常、ユーザーの操作がなくても攻撃を仕掛けられるため、検出される可能性を最小化できるからです。攻撃者がこれらのデバイス上にゼロデイ脆弱性を狙った脆弱性利用型不正プログラムを保有している場合、標的環境にアクセスし、長期間検出されないままになる可能性が高くなります。さらに、攻撃者はこの脆弱性利用型不正プログラムを利用して、さらに別の標的にアクセスすることや、同じ標的へのアクセスが中断された場合に再びアクセスすることもできます。

ゼロデイ: パッチが入手可能になる前に開示された脆弱性。

N デイ: パッチが入手可能になった後で最初に悪用された脆弱性。

Mandiant は、2023 年にこのプロファイルに一致するデバイスを標的とするさまざまな攻撃者を観測しました。Sandworm[24] は、ウクライナでの戦時攻撃活動を実現するために、侵害済みのネットワーク エッジ インフラストラクチャを介したアクセスを継続的に利用しています。金銭目的のグループ FIN11[25]は、データ窃盗恐喝攻撃活動の一環として、MOVEit Transfer ソフトウェアのゼロデイを悪用して、データを盗み出しています。この 1 年だけでも、Mandiant は、ゼロデイや n-day の脆弱性を利用して可視化を計測するのが困難なシステムを標的にした、中国のスパイ攻撃活動と疑われる重大な事例を数件調査してきました。

エッジデバイスを狙ったカスタム マルウェア

ネットワークの論理境界に位置し、インターネット上のサービスをホストするセキュリティ デバイスやネットワーキング デバイスは、一般に「エッジデバイス」と呼ばれます。Mandiant は、中国が関与する攻撃者が脆弱性（特にゼロデイ）を悪用してエッジデバイスにアクセスし、カスタム マルウェアのエコシステムをデプロイする動向を観測しています。このようなマルウェアのエコシステムは、通常、攻撃者が一斉に操作する複数の異なるコード ファミリーで構成され、通常はカスタム開発されるか、標的となるエッジデバイスや基盤となるオペレーティング システムに合わせて調整されます。こうしたマネージド アプライアンス用のマルウェアの開発は容易ではありません。ベンダーは通常、アプライアンス デバイスの所有者やユーザーがオペレーティング システムやファイル システムに直接アクセスできないようにしています。このクラスのプラットフォーム内で攻撃を実施できるようにするには、攻撃者はリソースを大量に消費するマルウェア開発ライフサイクルを維持しなければなりません。これには柔軟性と高度な技術的見識を維持することが必要になります。このプロセスには多額の投資が必要になりますが、攻撃者が利用に成功すれば結果は明らかです。

検出を回避する

一般に、カスタム マルウェアを検出できる具体的な機能が導入されていないことが多いため、そうしたマルウェアが長期間検出されないままになる可能性があります。これは、特にエッジデバイスに当てはまります。ネットワークの防御担当者が、マルウェア アクティビティをモニタリングして検出する手段をほとんど持っていない場合があります。また、マルウェア作成者は、デバイスに導入されているロギング システムを回避またはクリアすることでフォレンジック調査の妨げになるよう、特別な注意を払ってマルウェアを作成します。マルウェアが発見されてセキュリティ コミュニティが公開した後でも、多くの場合、デバイスの所有者が影響を受けたかどうかを特定することは容易ではありません。なぜなら、既製のセキュリティ プロダクトは通常、エッジデバイスに対応していないからです。また、ゼロデイ脆弱性の悪用が試みられても、確かな痕跡がほとんど、あるいはまったく残らないケースもあります。さらに、実はその攻撃が検出の数か月前あるいは数年前に発生していた可能性があると判明し、問題が悪化することも多々あります。そのうえ、このような侵害の調査は本質的に複雑であり、対象となるデバイスは通常メーカーによって厳重に管理されているため、従来のフォレンジック手法では困難を伴うことが少なくありません。

例: BOLDMOVE

BOLDMOVE は、中国のスパイグループと疑われている集団が使用しているバックドアで、Windows 版と Linux 版の両方があり、コアとなる一連の機能が含まれています。Mandiant は、Linux 版の BOLDMOVE をカスタマイズした亜種を特定しました。この亜種には、Fortinet のデバイスで検出されないようにするための一連の巧妙な機能が含まれていました。この BOLDMOVE の亜種は、アプライアンス上の「miglogd」と「syslogd」のロギング デーモンを無効にし、これらのロギング機能のためのメモリアドレス空間にパッチを適用するコマンドを含んでいました。これらの BOLDMOVE のバックドアのカスタマイズにより、従来の手段では不可能だったであろうほど長い期間、攻撃者は検出されずにいることができたと見られています。

複雑さの軽減、信頼性の向上

メール セキュリティ ゲートウェイ アプライアンスや VPN などのエッジデバイスは通常、再起動することなく数か月から数年間稼働する高可用性デバイスです。そのため、これらのデバイスの多くについて、その安定性を確保するために、開発中にメーカーによる厳格な試験レジームが実施されます。中国と関連するマルウェア デベロッパーは、これらのシステムに組み込まれた機能を利用することで、いくつかのメリットが得られます。一般に、ネイティブ機能を利用した場合、攻撃者は組織が厳密にテストした既存の機能を逆に武器にすることで、マルウェアの全体的な複雑さを軽減できるようになります。たとえば、カスタム ファイル形式や構成ファイルのような独自のソフトウェア コンポーネントを使用しているデバイスの場合、攻撃者は独自の実装を開発するのではなく、組み込まれた機能を利用してこれらのファイルを解析または処理できる可能性があります。これは環境寄生型に似たコンセプトであり、エッジデバイスでは特に効果的です。こうしたネイティブ デバイスのオペレーションは、ネットワークの防御担当者にモニタリングされず、気付かれない可能性があるからです。

> **環境寄生型:** 攻撃者が特に検出を逃れる目的で標的環境内にプリインストールされた正規のツールとソフトウェアを使用すること。

例: THINCRUST

UNC3886 による侵害では、Mandiant は、FortiAnalyzer と FortiManager のデバイスにデプロイされた THINCRUST というバックドアを発見しました。このバックドアは、デバイスへの正規の API 呼び出しとしてそのコマンド&コントロール（C2）通信を偽装していました。中国のスパイグループと疑われる UNC3886 は、Python ベースのバックドア コードを、アプライアンスの API インターフェースを提供する正規のウェブ フレームワーク ファイルに追加しました。これにより、UNC3886 はネイティブ API の実装を利用し、前に追加しておいた新しいエンドポイント URL を操作するだけで、THINCRUST にアクセスしてコマンドを送信できるようになります。アプライアンスに組み込まれている既存の機能を活用することで、UNC3886 は継続的な活動に必要な信頼性を維持しながら、マルウェアを簡素化できました。

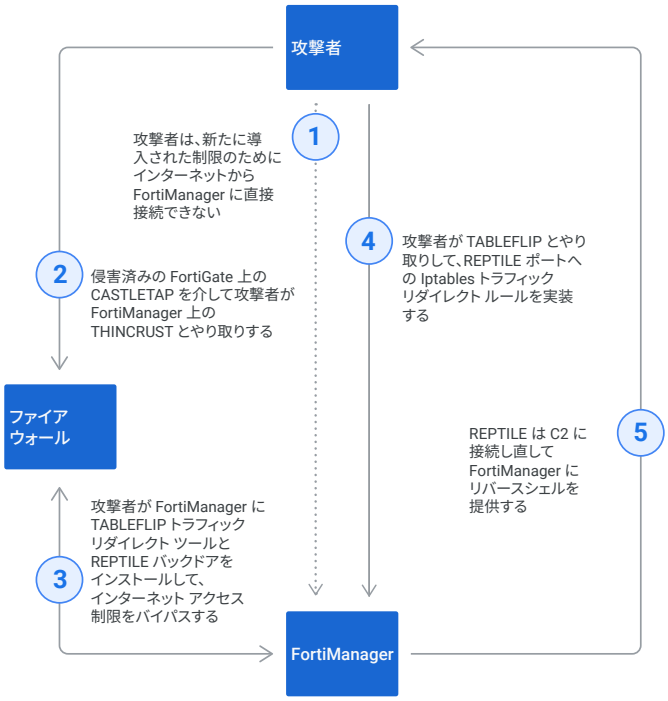
カスタマイズされた機能と小規模なフットプリント

エッジデバイス向けにカスタマイズされたマルウェアには、攻撃者のミッション目標を達成するために必要な機能しか含まれていない可能性があります。脆弱性を悪用するために使用されたマルウェアは、コードを維持して再利用するコストがメリットを上回る場合が多いため、脆弱性が発見され、パッチが適用されると、二度と使用されない可能性があります。標的のデバイス上で攻撃者が望む機能を提供するだけの比較的単純なマルウェアを開発することで、攻撃者は全体のフットプリントを最小限に抑えながら目的を達成できます。同様に、攻撃者の主な目的は、マルウェアが発見された後の分析を妨げることではなく、完全に発見されないようにすることであるため、複雑な難読化の必要性は低くなると考えられます。マルウェアが発見される頃には、脆弱性とキャンペーンはすでに表面化し、攻撃者の攻撃活動は通常終了しています。

例: TABLEFLIP

UNC3886 は、アクセス制御リストの変更により FortiManager デバイスへのアクセスを失った後、TABLEFLIP というネットワーク トラフィックのリダイレクト ユーティリティをデプロイして、この状況に対応しました。TABLEFLIP は、iptables コマンドを使用してトラフィックをリダイレクトするために、XOR エンコードされた IP アドレスとポートを含む特殊なコマンドパケットを、すべてのアクティブ インターフェース上で受動的にリッスンします。UNC3886 は、一般に公開されている REPTILE ルートキットとともに TABLEFLIP をデプロイし、リバースシェルとして動作させ、FortiManager デバイスへの再アクセスに成功しました。進行中の攻撃活動の変化に応じて目的に応じたマルウェアを作成できるため、国家を後ろ盾して高い能力とアジリティを備えた攻撃者がこれを使用すると、防御側にとって不利となります。

FortiManager にインターネット アクセスの制限を導入した後のアクティビティ



使用者の特定に関する課題

エッジデバイス用に開発されたカスタム マルウェアは、サイバー脅威インテリジェンス アナリストのアトリビューションを阻害する可能性があります。これらのマルウェア ファミリーと、場合によってはエコシステム全体は、標的となるオペレーティング システムとその調整された機能により、既存のマルウェアと比べてほぼまったく他に類を見ないものである可能性があります。そのため、関連するマルウェア ファミリー間に、技術的なアトリビューション分析に寄与するようなコードやその他の重複が見られない可能性があります。

例: SEASPRAY と WHIRLPOOL

SEASPRAY は、UNC4841 が正規の Barracuda Email Security Gateway (ESG) モジュールに挿入する Lua で記述されたランチャーです。SEASPRAY は、受信メールのイベント ハンドラを登録し、特定のマーカーが存在する場合、Mandiant が WHIRLPOOL として追跡する外部バイナリを起動します。WHIRLPOOL はシンプルな TLS リバースシェル ユーティリティで、実行時に SEASPRAY から接続先の C2 IP アドレスとポートを受け取ります。SEASPRAY は、Barracuda ESG アプライアンス固有の数行のコードで構成される比較的単純な実装であったため、アトリビューションの観点ではあまり価値がありません。同様に、WHIRLPOOL はシンプルで汎用的な TLS リバースシェルであり、分析可能な C2 サーバー情報は埋め込まれていません。そのようなマルウェアがエッジデバイス上で使用されることは、アトリビューション分析を行うアナリストにとって大きな課題となりました。

エッジデバイスに対する詳しい知識

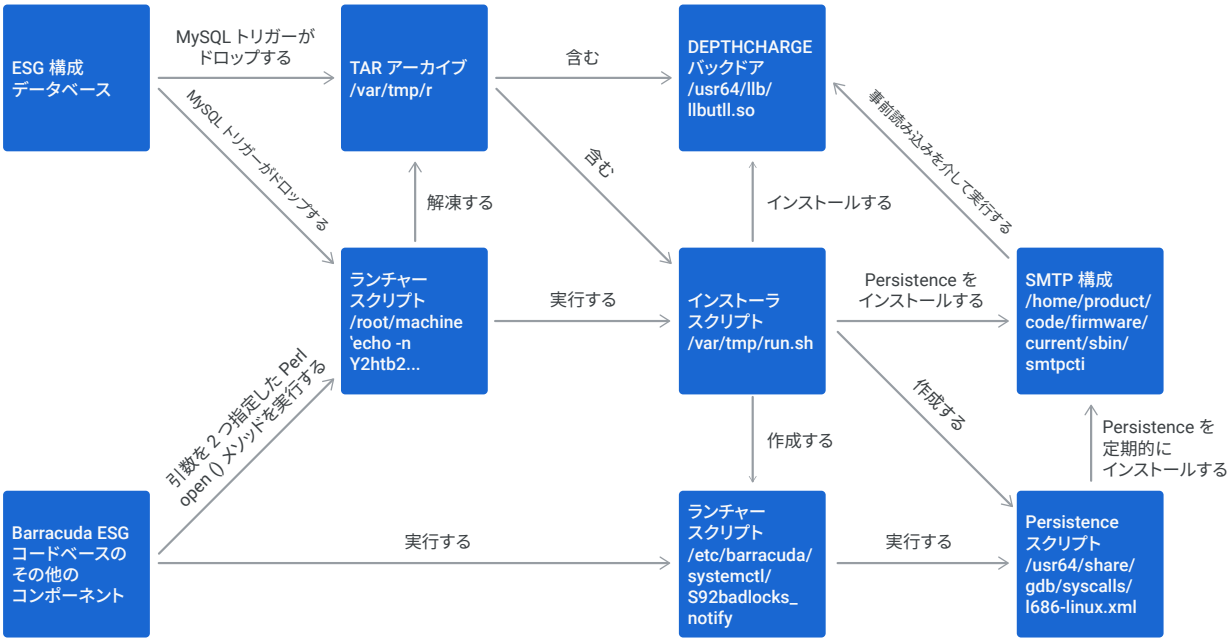
Mandiant は、中国の関与する攻撃者がエッジデバイスを標的とする際に高度で詳細な知識を示す事例をいくつか観測しています。その知識は、攻撃時に使用されたマルウェアだけでなく、これらのデバイスにアクセスするために使用されたゼロデイ脆弱性にも及んでいます。

例: DEPTHCHARGE

DEPTHCHARGE はパッシブ バックドアで、これを UNC4841 が Barracuda による ESG ゼロデイ キャンペーンの最初の公開通知から約 1 週間後にデプロイを開始したことを Mandiant が観測しています。これは、Barracuda が影響を受けたデバイスの交換計画を発表した後、Mandiant が保護対象として優先度の高い対象者により迅速にデプロイされました。デプロイが加速されたタイミングは、UNC4841 がこれを予期していた可能性を示唆しており、標的とするネットワークへのアクセスを妨害しようとする試みに直面しても攻撃活動を継続できるように設計されたツールや戦術、手法、手順 (TTP) を利用して、修復作業に備えていたことを示しています。

DEPTHCHARGE とその実行チェーンのいくつかの側面は、Barracuda ESG デバイスとそのソフトウェア コンポーネントを熟知していることを示していました。最も注目すべき点は、攻撃者がアプライアンスの構成データベース内にマルウェアを常に存在させる方法を特定したことです。その結果、エクスポートされたバックアップ構成にマルウェアが存在するようになりました。つまり、デバイス所有者はクリーンなデバイスをセットアップしようとして、知らないうちに DEPTHCHARGE 永続性が含まれるバックアップ構成をエクスポートし、構成を復元しようとすると、クリーンなアプライアンスが感染する結果となります。

おそらく、UNC4841 がアプライアンスの内部構造についてさらに複雑な知識を持っていることが示されたのは、DEPTHCHARGE が MySQL 構成データベースをインポートした後、内部のトリガーからコマンド実行を実施できたときでした。UNC4841 は、ESG のコードベースの完全に独立したコンポーネントが、Perl の open() 関数の、引数が 2 つの形式を使ってファイルにアクセスし、アプライアンス上でコマンドが実行されるような特殊なファイル名を作成できることを把握していました。MySQL トリガーがこのコマンド実行を誘発するファイルをドロップすることで、UNC4841 はこれらの手法を連鎖させ、新しいアプライアンスでバックアップ構成をインポートする際に DEPTHCHARGE をドロップして実行できるようにしました。これにより、件数は少ないものの、デバイスが完全に交換された後も、UNC4841 が存続していたケースが見られました。

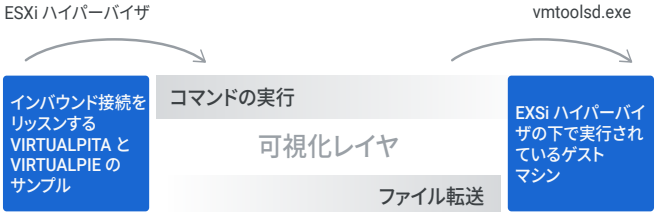


ハイパーバイザ向けカスタム マルウェア

クラウド コンピューティングが年々普及してきたことに伴い、ハイパーバイザは最新のインフラストラクチャでよく使用されるようになりました。ただし、ゲスト仮想マシンでエンドポイントの可視性を計測するのは比較的簡単ですが、ハイパーバイザ自体で可視性を計測するのはかなりの困難を伴います。ネットワーク エッジ デバイスと同様に、タイプ 1 のハイパーバイザは、EDR ベンダーがほとんどサポートしていないオペレーティング システムのバージョンで実行されるのが一般的です。当然のことながら、ハイパーバイザの可視性が低いにもかかわらず、その標的の価値が非常に高いことから、中国が関与する攻撃者がハイパーバイザを標的にしていることを Mandiant は観測しています。

VMware の ESXi のようなハイパーバイザ技術は、Virtual Machine Communication Interface (VMCI) ソケットを使用して、ベアメタル ホストとゲスト オペレーティング システム間の通信を容易にしています。Mandiantは、攻撃者がVMCIソケットを利用して標的環境内でラテラルムーブメントを行い、永続性を維持していることを確認しています。UNC3886 は、VIRTUALPITA などのバックドアを利用し、ESXi ホストからゲスト仮想マシン (VM) への通信に VMCI ベースのチャネルを利用しています。仮想化レイヤ上のトラフィックはベアメタル マシンにローカライズされるため、ゲスト VM や ESXi ホストが他方との接続を開始することを制限するセキュリティ メカニズムは存在せず、基本的にあらゆるネットワーク セグメンテーションをバイパスします。さらに、仮想化環境に存在するゲスト VM と ESXi ホストの外部でトラフィックをモニタリングすることはできません。クライアント / サーバー通信ソケットには、TCP や UDP によく似た接続指向と非接続バリアントがありますが、異なるソケット アドレス ファミリーに属するため、カスタム構成なしでは、tcpdump、netstat、nmap、Wireshark などのよく使用されるネットワーキング ツールからは見えません。

UNC3886 は、新しい永続化手法により、vSphere Installation Bundles (「VIB」) を利用して VIRTUALPITA バックドアをデプロイしています。Mandiant は、これまでこの手法を使用してマルウェアや永続性がデプロイされたことを観測していません。このことから、UNC3886 は多大なリソースが費やして VMware の技術、特にセキュリティ制限を回避する VMCI ソケットの内部構造を理解していたと考えられます。また、VIRTUALPITA を使用して、ホストにログオンすることなくゲスト VM に任意のコマンドを渡しています。これらのコマンドは、vmtoolsd.exe プロセスでゲスト VM 上で実行され、Windows のイベントログに記録されます。また、VIRTUALPITA は、HISTFILE を 0 に設定します。これにより、ホストシステム上のターミナル履歴がすべて削除され、フォレンジックの痕跡はほとんど残りません。



推奨事項

このような攻撃から身を守るための最も重要な戦略は、既知の脆弱性を悪用されるリスクを軽減できるよう、適切なパッチ管理を維持することです。最新のパッチを適用することは、アプライアンスの予期せぬ改ざんや変更を制限する最善の方法です。エクスプロイトが検出される可能性が低いゼロデイ脆弱性の場合、多層防御アプローチは攻撃ライフサイクルのさらに先にある悪意のあるアクティビティの痕跡を表面化させる最良の機会となります。

脆弱なデバイスを運用している組織が侵害された可能性があることを特定した場合、Mandiant はネットワーク内で調査とハンティング アクティビティを行うことを推奨しています。調査項目には、以下のものがあります。

- IOC スキャナなどの一般に入手可能なツールを使用して、影響を受ける可能性のあるデバイスをスキャンし、侵害の痕跡を特定する。
- 既知の IOC について環境全体を調査する。
- ネットワーク ログを確認し、データ窃盗やラテラル ムーブメントの兆候を確認する。
- 異常なログインやエッジデバイスからの内部トラフィックがないか、ネットワーク ログを確認する。
- 影響を受けたアプライアンスのフォレンジック イメージをキャプチャし、フォレンジック分析を行う。
- フォレンジック調査をサポートするために、アプライアンスのイメージにマルウェア署名（YARA ルールなど）を適用する。

セキュリティ ベンダーが提供するアーキテクチャ強化ガイダンスに詳しく説明されているセキュリティ管理の実装も検討することをおすすめします。Mandiant は以前、Barracuda ESG イベントでそのようなドキュメントを提供したことがあります[26]。

今後の展望

多くのリソースを必要とするにもかかわらず、中国のスパイグループがゼロデイの脆弱性利用型不正プログラムやプラットフォーム固有のツールの獲得に投資を続けることはほぼ間違いありません。Mandiant は、侵害の発見と調査に関連する課題があることから EDR やその他のセキュリティ ソリューションが以前より欠如していたエッジデバイスやプラットフォームが今後も標的になると予想しています。これらのデバイスの悪用は、中国のスパイグループにとって、発見されずに標的環境に継続的に侵入するための魅力的な初期アクセス ベクトルであり続けるでしょう。

また、当面のデバイスや攻撃活動に合わせてカスタマイズされたマルウェアのエコシステムが、中国のスパイグループによって引き続きデプロイされる可能性があります。このアプローチには、検出されずにとどまる能力の向上、複雑さの軽減と信頼性の向上、マルウェアのフットプリントの軽減など、いくつかの利点があります。さらに、脅威インテリジェンス アナリストが行っている技術的なアトリビューションにも課題があります。

組織は警戒を怠らず、オペレーティング システム層でネットワークをモニタリングするだけでなく、ネットワークの基盤となるインフラストラクチャを稼働させているアプライアンスにパッチを適用し、保守して、可能であればモニタリングを続ける必要があります。

さまざまな動機に基づくゼロデイ攻撃

サイバーセキュリティを取り巻く状況が絶え間なく進化する中で、ゼロデイ エクスプロイトは攻撃者の強力な武器であり続けています。この種の脆弱性は、ソフトウェア ベンダーに知られていないため、ステルス型攻撃の標的となって攻撃者にシステムとセンシティブ データに不正にアクセスされる可能性があります。

ゼロデイ: パッチが入手可能になる前に開示された脆弱性。

2023 年には、合計 97 種類のゼロデイ脆弱性が実際の環境で悪用されたことを確認しています。2022 年に追跡した件数を 56% 近く上回る結果となっています。2023 年にゼロデイを悪用した攻撃者の中でも特に目立ったのは中華人民共和国 (PRC) のサイバー エスピオナージ グループで、そのゼロデイ エクスプロイト キャンペーンではステルス性が重視されていました。同グループは中国政府の支援を受けており、Mandiant で追跡したところ、主としてインテリジェンスを収集し、戦略的に優位に立つことを目的にゼロデイを利用しています。

ターンキーやオフザシェルフとよく言われるすぐに使用可能な機能を販売する商用監視ベンダーが増えてきたことも、サイバー エスピオナージ活動を一貫して支える要素となっています。多くの場合、こうしたベンダーはエクスプロイト チェーンの構築に必要な技術専門知識だけでなく、標的とした被害組織を特定してデータを密かに盗み出すために必要な後続のツールも提供します。こうした機能の発達は、内部的な専門知識がなくてもゼロデイ脆弱性を悪用できるようになったことを示唆しています。攻撃者にとっては、ゼロデイを調査できるだけの高度な技術知識がなくても、ゼロデイ エクスプロイトにアクセスできる可能性が広がるわけです。

それと同時に、金銭目的の攻撃者は、引き続きシステムに侵入し、貴重なデータを盗み出して金銭を受け取るためにゼロデイを導入します。2023 年に金銭目的の攻撃者とエスピオナージ グループが悪用したゼロデイの総数は、過去 2 年間とほぼ変わりません。少なくとも 2016 年以降活動を続ける金銭目的のグループ FIN11 は、2023 年に広域にわたるキャンペーンで 2 件のゼロデイを悪用しました。FIN11 はゼロデイの開発に投資して、継続的にグループの洗練化を図っています。ゼロデイ脆弱性の調査は多大な時間とリソースを要するプロセスであり、FIN11 が複数のゼロデイ脆弱性を悪用していることから、グループは時間もリソースも着実に活用できるようです。特に、FIN11 はファイル転送アプリケーションを頻繁に標的にしています。この種のアプリケーションでは、被害組織のネットワーク内でラテラル ムーブメントを加える必要なく、大量のセンシティブ データに迅速かつ効率的にアクセスできます。

攻撃者の動機はさまざまであり、したがってゼロデイ エクスプロイトの利用に向けたアプローチもさまざまに異なります。ステルス性と長期的なアクセスを優先するエスピオナージ グループは、ゼロデイの使用には慎重になり、できる限り検出されないようにエクスプロイトを巧みに作成する可能性があります。その一方で、金銭目的の攻撃者は速度と効率を優先し、ステルス性を犠牲しても見返りをより迅速に得てより広範にエクスプロイトを行おうとする傾向があります。

最前線の Mandiant エンゲージメントから導き出されたケーススタディを 2 つ紹介します。これらの例を見ると、攻撃者の取る行動が目的によってさまざまに異なることがよくわかります。Progress Software の MOVEit Transfer を悪用した金銭目的のキャンペーンを見ると、金銭目的の攻撃者の順応性とすばやさがわかります。その一方で、Barracuda Email Security Gateway (ESG) を標的としたスパイ主導のキャンペーンを見ると、政府の支援を受けたグループの永続性と巧妙化が浮き彫りになります。これらのケーススタディから、目的が明確に異なる 2 つのグループでは戦術、手法、手順 (TTP) がさまざまに異なるものの、いずれの目的も同じような創意工夫と順応性で遂行されていることがよくわかります。

サイバー犯罪キャンペーンのケーススタディ: MOVEit

2023 年 5 月に、Mandiant は CVE-2023-34362[27]のエクスプロイトを観測しました。これは、Progress のマネージド ファイル転送ソリューション MOVEit Transfer のゼロデイ脆弱性です。2023 年 5 月 31 日より前のすべての MOVEit Transfer バージョンがこの脆弱性の影響を受け、攻撃者は MOVEit Transfer のデータベースに不正にアクセスできたため、データが侵害され、金銭を失う可能性がありました。CVE-2023-34362 を悪用するには、攻撃者は巧妙に細工したリクエストを脆弱なサーバーに送りつけることで、脆弱なシステム上のアプリケーション クエリに悪意ある SQL ステートメントを挿入する必要があります。脆弱なアプリケーションのデータベースへのアクセスを獲得すると、攻撃者はさらに権限昇格を獲得して任意のコードを実行するためのアクションを実行できるようになります。データベース内のデータへのアクセス、変更、削除などです。Mandiant は、この脆弱性に関連する 31 件の攻撃を調査して、FIN11 が採用した TTP に関して有益な分析情報を得ることができました。このいずれの攻撃も、エクスプロイトに原因があると考えられます。Mandiant の分析から、自動攻撃のパターンが明らかになりました。自動攻撃の間、FIN11 はエクスプロイトのスピードと効率性に注力していたと見られます。キャンペーンに対する FIN11 のアプローチは巧妙化が進み、標的組織にもたらされるリスクが大きくなっています。

FIN11 の攻撃キャンペーン

MOVEit Transfer ゼロデイを悪用するキープレーヤーとして、FIN11 が浮上してきました。Mandiant の調査から、FIN11 が早ければ 2022 年 4 月にはこの脆弱性のテストを開始していたことが明らかになっています。ただし、公表された報告書を見ると、もっと早い段階で開始された可能性があります。その後、信頼性の高いエクスプロイトとデータの抽出手段が開発されるまで継続されていたようです。

2023 年 5 月以来、FIN11 の攻撃手法は主にウェブベースのバックドアのデプロイ、データの列挙、データの盗難に関わるものとなっています。初期アクセスを獲得すると、FIN11 は侵害したシステムにウェブベースのバックドア（Mandiant ではこれを LEMURLOOT として追跡）をデプロイします。こうしたバックドアは、正規のソフトウェア コンポーネントを装って、データの列挙と盗難に必要な機能を提供します。FIN11 は、LEMURLOOT を介して各種コマンドを実行します。ファイルとフォルダを列挙する、構成情報を取得する、名前がハードコードされたユーザーを作成または削除するといったコマンドです。

影響と修復

このキャンペーンでは、さまざまなセクターと業種全体で 2,600 近くの組織が FIN11 の標的となりました。攻撃のスケールから、FIN11 はこうした広範なスケールでハンズオン キーボード侵入を展開することは実用的でないと考えて自動化手法を利用していたと考えられます。FIN11 データ漏洩サイトに投稿されたデータによると、センシティブ データを含む可能性 がある、数テラバイトものデータがこのキャンペーンによって盗まれました。

Mandiant は、FIN11 が MOVEit Transfer 脆弱性を利用したことについて何度か調査しましたが、ラテラル ムーブメントの痕跡を特定するには至りませんでした。FIN11 の主な目的が、長期的な永続性を確立することや標的のネットワーク内でさらに別のシステムを侵害することではなく、データをすぐに盗み出すことにあった可能性があります。ファイル転送アプライアンスにアクセスしたことで、FIN11 はセンシティブ データへの十分なアクセス権を得て、ネットワーク内でラテラル ムーブメントを行わなくても被害者を恐喝できたと考えられます。

MOVEit Transfer アプライアンスを標的とした FIN11 の活動を巡る修復作業には、Progress Software からリリースされた一連のパッチを適用する作業が伴います。組織は、パッチの適用を優先し、堅牢なサイバーセキュリティ対策を導入して、同じような攻撃から保護することを早急に求められました。

エスピオナージ キャンペーンのケーススタディ: Barracuda

PRC サイバー エスピオナージ グループは、2023 年にゼロデイ エクスプロイト キャンペーンを何度か実施して注目を集めました。その中でも、Barracuda ESG アプライアンスを標的としたキャンペーンは影響範囲が最も大きかったと考えられ、特に有名です[28]。UNC4841 は、リモート コマンド インジェクション脆弱性（CVE-2023-2868）を利用して Barracuda ESG を標的とした中国による一群のサイバー エスピオナージ アクティビティです。これは 2023 年 5 月に開示されました。ただし、Mandiant の調査から、少なくとも 2022 年 10 月まで遡ってエクスプロイトの痕跡が明らかになっています。UNC4841 は、TAR ファイルを処理する解析ロジックの欠陥を利用することで、ESG アプライアンスを悪用しました。UNC4841 は、ある特殊な方法で TAR ファイルをフォーマットすることで、リモート コマンド インジェクション攻撃をトリガーし、システム コマンドを実行できました。UNC4841 の攻撃戦略は入念に策定され、低品質の迷惑メールに見えるよう巧妙に設計されたメールを使用して、悪意のある TAR アーカイブ ファイルを添付します。TAR アーカイブのメール添付ファイルにはファイル名が含まれていて、そこには悪意あるコマンドが混入されていました。それを利用して、脆弱なアプライアンスに足がかりが築かれました。アクセスを獲得すると、UNC4841 は Barracuda ESG に合わせて特に調整した幅広い第 2 段階のバックドアをデプロイしました。長期的なアクセスを確立してスパイ活動を行うことが目的で、実際その活動は 8 か月もの間検出されませんでした。

センシティブ データを的確に盗み出す

長期的なアクセスを着実に確立した後、UNC4841 は標的組織からセンシティブ データを密かに盗み出すことに焦点を当てました。その戦術では、ESG の一時的なメール ストレージ コンポーネントからメールを獲得することに重点が置かれ、これにより、侵害したアプライアンスで幅広いメール収集を実施できるようになりました。UNC4841 ではこのほか、シェル スクリプトによるメール収集も標的としました。対象となったのは、中国にとって戦略的に重要であると見なされた特定のメールドメインとユーザーです。また、Mandiant は収集目的で UNC4841 ターゲティング メールが Barracuda アプライアンス（送信元が特定のインテリジェンス値のソースである可能性がある）に送信されていることを観測しました。キャンペーン全体を通して UNC4841 で使用されていたステージング ファイルの命名規則を見ると、大規模なスパイ活動が行われていたと考えられます。UNC4841 は、主に /mail/tmp/ ディレクトリ内のデータをステージングし、先頭が被害組織に対応する 3 文字、その後に番号が続くという一貫性のあるファイル命名規則を使用しています。

標的の傾向

UNC4841 の標的パターンは、キャンペーンが続く間進化し、8 か月以上も存続しました。当初は行政機関に焦点を当てていましたが、キャンペーンが進むにつれて、UNC4841 は情報技術セクターの組織、そしてさらに幅広く他のセクターへと攻撃対象を広げていきました。脆弱性が一般に広く知られるようになると、UNC4841 は行政機関とハイテク組織に優先して特定のマルウェア ファミリーをデプロイし始めました。UNC4841 は、アクセスを維持して攻撃活動を続行するために、通知後期間内に組織全体に一連のバックドアをデプロイします。

脅威の軽減

2023 年 5 月 31 日に、Barracuda は侵害されたすべての ESG をパッチレベルに関係なく直ちに交換するように組織に強く勧告しました。このインシデントは、プロアクティブなサイバーセキュリティ対策の重要性を物語っています。エッジ アプライアンスからラテラル ムーブメントや不審なアクティビティが試行されることがあるため、脆弱性に速やかにパッチを適用する、定期的にセキュリティを監査する、ネットワークを継続的にモニタリングするといった対策が必要です。防御側がゼロデイを予想することはできませんが、こうした対策は、攻撃者がネットワーク全体をより簡単に移動したり、権限をエスカレーションしたりするために利用できる他のセキュリティ欠陥を明らかにするために有用です。非開示の脆弱性を利用した攻撃の損傷と拡大を抑えると、攻撃者の進化とともに組織が直面するリスクを減らすために役立ちます。

比較分析: 得られる教訓と進化し続ける脅威の状況

MOVEit Transfer と Barracuda ESG の脆弱性を標的としたキャンペーンを見ると、進化し続ける脅威の状況がはっきりと表れ、ゼロデイ エクスプロイトをどのように実施するかという点で金銭目的の攻撃者とスパイ主体の攻撃者との間に明確な違いがあることがわかります。FIN11 は、MOVEit を悪用するにあたって迅速かつ効率的なアプローチを優先し、多数の組織を標的に簡素ながら効率的な方法でセンシティブ データにアクセスします。

比較項目	金銭目的	スパイ
被害組織の数と質	大量の被害組織 (2,600 を超えるとの報告あり)	比較的少ない被害組織 (脆弱なアプライアンスの 5% ほど)
CVE の武器化へのアプローチ	すばやく金銭を獲得	持続性のあるインテリジェンス収集
影響	PII の損失、企業秘密を漏洩する可能性、個人のプライバシーと事業運営への影響	国家安全保障への影響、行政機関を標的とした攻撃
対応 / 封じ込め	データの抽出を最小限に抑え、ランサムウェアのデプロイを防ぐ必要がある	セキュリティ侵害、攻撃者の戦術、マルウェアの検出について徹底的に理解する必要がある

その一方で、UNC4841 は、Barracuda ESG を悪用する際にもっと緻密で標的を絞ったアプローチを採用し、インテリジェンス目的でセンシティブ データに長期的かつ密かにアクセスすることを目指します。

ゼロデイ脆弱性利用型不正プログラムを入手して利用するためにさまざまな攻撃者が従来講じてきた手段を調べると、今後標的となる可能性のある組織での意思決定と優先順位付けの参考となる情報が得られます。ゼロデイ脆弱性利用型不正プログラムを確実に防御できる方法はありませんが、重要なシステムの保護と分離に取り組むとともに、不審なアクティビティを継続的にモニタリングするために必要な可視性を確保することで、リスクを軽減できます。

組織は従来、リスクスコアに従ってパッチの適用に優先順位を付けています。リスクスコアの高いもののほうが、低いものよりも先にパッチが適用される傾向にあります。ただし、脆弱性を悪用する動きが活発であるという痕跡があると、パッチ適用の優先順位が上がります[29]。対象となる組織は、すぐに影響調査を開始する必要があります。

すでにインシデント対応計画を策定し、幅広い環境モニタリングを確立している組織は、一般的に、その環境で脆弱性の潜在的な影響を評価する態勢がより充実しています。ネットワーク セグメンテーションをレイヤに分け、ロギングを確保するとともに、高度なエンドポイント検出対応ソリューションを導入すると、組織は効率よく調査を開始し、速やかに事態を終結できます。

同様に、ハードウェアやソフトウェアを環境にデプロイする前に、ベンダーのセキュリティ プラクティスとネットワーク要件を徹底的に評価することで、防御側は何をもって「正常」使用と考えるべきかについて品質のベースラインを築くことができます。また、ベンダーを入念に調べることで、普段とは異なる使用を明確に定義した包括的な検出メカニズムを作成できます。ベンダーのプロダクトのコンテキスト内で何か普段とは異なる使用を検出したら、それを優先して調査し、その検出に対して講じるアクションの正当性を裏付けます。ポリシー、脅威インテリジェンス、アクティブ モニタリングを組み合わせれば、ゼロデイ脆弱性を悪用しようとする攻撃者に対抗する早期警戒システムとして機能します。

まとめ

ゼロデイ エクスプロイトは、もはや一握りの攻撃者だけが利用できるニッチな能力ではなくなっています。Mandiant は、ここ数年見られた増加傾向が今後も続くと予想しています。ランサムウェア グループとデータ盗難恐喝グループによるゼロデイ エクスプロイトが増え、政府の支援を受けたエクスプロイトが今後も続き、ターンキーやオフザシェルフと言われる商用監視ベンダーから購入してすぐに使用できる機能が増加傾向にあることから、引き続きゼロデイ脆弱性とそれを標的とするエクスプロイトの特定を推進していく必要があります。攻撃者の動機と TTP を理解することで、組織は防御戦略を策定するにあたって環境に影響を与える可能性が高いと考えられる脅威のタイプに優先順位を付けることができます。サイバーセキュリティ ポスチャーの強化、堅牢な脆弱性管理プラクティスの導入、セキュリティ意識の文化の育成が、ゼロデイから安全に保護する際の重要なステップとなります。MOVEit と Barracuda へのキャンペーンは、サイバー脅威が単なる迷惑行為ではなく、人々の注目を集め、対策が必要な脅威であることをはっきりと思い出させます。防御側は、サイバーセキュリティに対してプロアクティブなアプローチを導入して、ゼロデイ脆弱性が現実であることと、しっかり準備すればその影響が軽減されることを認識する必要があります。

セキュリティ対策が変化する中でのフィッシングの進化

2022 年に、Microsoft は Office ドキュメントでのマクロの実行をデフォルトではブロックする方針にしました。この変更は、攻撃者が初期アクセスに続いてこの手法を利用してコードを実行することを事実上阻止するものです。Mandiant はそれ以来、攻撃者が新しい方法で初期アクセスを獲得し始めたことを観測しています。ペイロードの選択の幅を広げ、ソーシャル エンジニアリングで非常に効果的な戦術を取っています。攻撃者は、セキュリティ管理をすり抜けるために、LNK ファイルや兵器化された Microsoft Office ドキュメントなどさまざまなペイロード タイプを試し始めました。さらに、従来の標的範囲から抜け出す道を模索し、ソーシャル メディア、SMS メッセージング、その他のよく使用されるコミュニケーション プラットフォームなど、メールを超えたプラットフォームに積極的に関わり始めました。Mandiant では、攻撃者が会話を乗っ取る、単に内部ユーザーを装うといった手法で信頼された関係やコミュニケーションを悪用していることも観測しています。こうした時代に応じたフィッシング手法は、ユーザー教育、メール ゲートウェイ フィルタリング、多要素認証 (MFA) に焦点を当ててきた従来のセキュリティ パラダイムに疑問を投げかけます。2023 年に、攻撃者はユーザーを標的とする際に、これまでの規範から外れた複数のタイプのフィッシング ペイロードと手法を利用しています。Mandiant は、攻撃者がコードの難読化、リモート ペイロードのホスティング、アーカイブ ファイル内へのドロッパー スクリプトの配置、メール フィルタリング制御のバイパスを行っていることを観測しました。

マルウェアの配信: 古い、借りものの、新しい手法

2023 年に、攻撃者はユーザーを標的とする際に、これまでの規範から外れた複数のタイプのフィッシング ペイロードと手法を利用しています。Mandiant は、攻撃者がコードの難読化、リモート ペイロードのホスティング、アーカイブ ファイル内へのドロッパー スクリプトの配置、メール フィルタリング制御のバイパスを行っていることを観測しました。

圧縮アーカイブ ファイル

ZIP や RAR ファイル形式などの圧縮アーカイブは、悪意あるドロッパー ファイルのコンテナとして使用できるほか、パスワードベースの暗号化機能を利用して自動検出をすり抜けることも可能です。メール セキュリティとファイアウォール テクノロジーは、特定のアーカイブ ファイル形式を解凍して、ファイル転送の際にコンテンツを検査し、ポリシーを適用できます。ただし、暗号化されていないアーカイブの場合、サンドボックス分析に時間がかかって悪意あるファイルがエンドユーザーに配信されるのを阻止できないことがあります。同様に、パスワード保護を使用して暗号化されたアーカイブ ファイルは、実際に自動ファイル スキャンをバイパスします。Microsoft が 2022 年にデフォルトでマクロを無効化することに踏み切った後、複数の脅威グループが初期検出をバイパスする手段として圧縮アーカイブを含める方向へ転換したことを Mandiant は観測しました。

UNC2500 は、マクロが有効な Office ドキュメントではなく、OneNote や LNK ファイルなど他のファイル形式をパスワードで保護された ZIP アーカイブ内に含めるようになりました。こうしたファイルは、メールへの添付ファイルとしてよく利用されるほか、OneDrive リンク、Google ドライブ URL、侵害したウェブサイトからダウンロードすることも可能です。UNC2500 フィッシング拡散キャンペーンでは、初期侵害に続いて複数のバックドア タイプをデプロイし、ランサムウェアの攻撃活動の前段階として複数の攻撃者にアクセスを提供します。2023 年 9 月以来、UNC2500 は LNK ファイルにコマンドを含めて兵器化しています。コマンドは、組み込みの cURL ユーティリティを利用して、悪意ある URL にホストされている Visual Basic スクリプトをダウンロードして実行し、さまざまなバックドアをデプロイします。

UNC4814 という別の脅威グループは、2023 年の 4 月から 5 月にかけてウクライナの行政機関と重要なインフラストラクチャを標的にスピア フィッシング メールを送信しました。これらのメールにはファイルが添付されていて、難読化した JavaScript ダウンローダが含まれています。UNC4814 は、オランダを拠点とする PAX 組織が主催する会議をおとりに組織を標的としました。この難読化した JavaScript ダウンローダを起動すると、PowerShell コマンドが実行されてダウンローダがインストールされます。

Microsoft Office ドキュメント

Microsoft が今後 VBA マクロをブロックすることになると発表したことを受け、マルウェアの配布方法が Microsoft アプリケーションのエコシステム内の新しい配信メカニズムへと転換したことを Mandiant は観測しました。2023 年 1 月の後半以来、UNC2633 は悪意ある OneNote ファイルを利用して QAKBOT マルウェアを配布しています。こうした OneNote ファイルは、Windows スクリプト ファイルをドロップし実行して、さらに別の悪意あるコマンドを実行します。Mandiant は 2 月に、FIN6 が CV をテーマにした OneNote をおとりにして、LNK ファイルに埋め込まれたダウンローダで構成されるペイロードを配布していることも観測しました。

Microsoft がデフォルトで Office マクロをブロックしているにもかかわらず、2023 年も依然として攻撃者が Office ドキュメントを利用してユーザーを標的にしていることを Mandiant は観測しています。相変わらず悪意あるマクロを使用しているのは、正規のビジネス目的でマクロを利用するためにマクロを有効にしておくという方針を維持している組織が存在していることの表れかもしれません。少なくとも 2023 年 2 月以降、ロシアとつながりのある攻撃者 Turla (Mandiant では UNC638 として追跡) は、Excel ドキュメント

を添付したスピア フィッシング メールを使用してウクライナの軍関係者を標的にしていると見られます。メールに添付されたスプレッドシートには、標的のマシンに .net バックドアをインストールするマクロが埋め込まれています。2023 年 4 月に、UNC1151 は埋め込みの .net ダウンローダ ペイロードをドロップする悪意あるマクロを Excel スプレッドシートに含めた RAR アーカイブを使用して、ウクライナの行政機関を標的としました。

メール本文内のハイパーリンクと添付ファイル

Mandiant は、攻撃者がメール セキュリティ ソリューションをバイパスしようとした試みの中で注目すべき手法を利用していることを観測しています。悪意ある添付ファイルを含めてもスキャンで阻止される可能性があることから、攻撃者は第 2 段階のペイロードへのハイパーリンクを含める試みを始めています。問題がなさそうな添付ファイルにハイパーリンクが含まれていることもあれば、メール本文にリンクが含まれていることもあります。メール セキュリティ ソリューションでは、どの程度までハイパーリンクをたどるか、どの深さまでスキャンを実行するかがさまざまに異なります。

2023 年 2 月以来、APT29 が第 2 段階のペイロードをホストするハイパーリンクを使用して外交機関に対してフィッシング キャンペーンを何度か実施していることを Mandiant は観測しました。ある特定のフィッシング キャンペーンでは、APT29 はワインテイスティング イベントへの招待を装う PDF を添付して、悪意ある埋め込み URL を含めていました。外交機関を標的とした別の事例では、APT29 はメール本文に直接 URL を埋め込んでいました。標的となったユーザーがフィッシング メールや PDF 内の URL をクリックすると、HTML ドロッパー添付ファイル（Mandiant では ROOTSAW として追跡）がディスクにダウンロードされます。ROOTSAW は、HTML スマグリングを利用して、JavaScript を起動して添付ファイルをデコードし、埋め込まれたマルウェアを実行します。2023 年 10 月以来、FIN6 もソーシャル メディア フィッシング メッセージにレジュメや職務をテーマにした PDF を含めることで、この手法を利用していることを Mandiant は観測しました。標的となったユーザーが PDF を開くと、偽のエラー メッセージが表示され、そこに攻撃者が管理するドメインへの URL が記載されていました。

ソーシャル エンジニアリング: 代替プラットフォームの利用

メールベースのフィッシングから防御する新しいテクノロジーが登場してデプロイされると、攻撃者はおとりを標的にばらまくためのプラットフォームを新たに見つけて試し、最終的に利用するというごく当たり前のプロセスを実施します。攻撃者は、さまざまな方法を使用して、メールと境界ネットワークのモニタリングでは目の届かないところでユーザーとやり取りして悪用しようとします。こうしたモニタリングが、検出に最も力を入れているからです。特に重点を置いているのが、標的環境のコミュニケーション プラットフォームとメッセージング プラットフォームへの侵入、ソーシャル メディアを利用したつながり、モバイル デバイスのフィッシングなど可視性が大幅に低いと見られている領域です。

コミュニケーション プラットフォームとメッセージング プラットフォーム

複数の攻撃者が侵害した内部アカウントと外部アカウントを利用して、Microsoft Teams ユーザーにフィッシング メッセージを送信しようとしたことを Mandiant は観測しました。2023 年 4 月に、UNC3944 は侵害した内部 O365 アカウントを使用して、Microsoft Teams を利用する他の内部ユーザーを標的としました。攻撃者は、組織の人事部門に所属する社員を装い、組織名が含まれているドメインに開設したなりすましの O365 ログインページにアクセスするように標的のユーザーを言葉巧みに誘導します。攻撃者は、ログイン フォームにアクセスするようユーザーを導き、MFA コードを提供します。侵害したユーザーとして認証されると、攻撃者は新しい MFA 手法を登録するか、MFA SMS コードの受信に使用されるユーザーの電話番号を更新します。

2023 年 9 月に、UNC5051 は外部 O365 テナント アカウントを使用して、Microsoft Teams チャット リクエストに悪意ある URL を含め、リクエストを行うユーザーを標的としました。アクセスすると、ユーザーは攻撃者が管理する SharePoint サイトに保存されている ZIP アーカイブをダウンロードするように求められます。ZIP アーカイブには、PDF ファイルを装う LNK ドロッパーが含まれていて、実行すると Visual Basic スクリプト ダウンローダが起動します。ダウンローダは、組み込みの Windows cURL ユーティリティを使用して、コンパイル済みの AutoIT スクリプトをダウンロードして実行し、DARKGATE バックドアをインストールします。Mandiant は、DARKGATE バックドアを攻撃活動に組み込んでいる脅威クラスタをいくつか特定しました。その中には、ランサムウェアを侵入させる目的で初期アクセスを提供するものがあります。

ソーシャル メディア

ソーシャル メディア プラットフォームは、攻撃者から見ると、データを追加で収集し、標的組織のユーザーをフィッシングする絶好の場です。中でも、特定の企業の従業員を標的とする場合によく選ばれるのが LinkedIn です。LinkedIn はビジネス指向のプラットフォームとしてのステータスを確立し、従業員の名前、役職、職務を参照できるようにしているため、攻撃者はフィッシング キャンペーンに合った真実味のあるおとりを仕込むことができました。

2023 年に、Mandiant は複数の攻撃者が偽の LinkedIn ペルソナを作り、個人的なメッセージを送って標的組織のユーザーをおびき寄せる事例を特定しました。2023 年 5 月以来、UNC2970 は LinkedIn プラットフォームを使用して、スピアーフィッシング活動を展開しました。その際、コンテナ ファイルをはじめさまざまなペイロード タイプを使用して、標的組織の従業員を侵害しています。侵害後は、バックドアの実行、標的となった情報の盗難といったアクティビティが見られ、スパイ活動疑惑の裏付けとなっています。2023 年 6 月の後半に、UNC4962 は LinkedIn から社内開発プロジェクトや職種をテーマにした個人的なメッセージを送信することで、ユーザーを標的としました。メッセージの受信者は、クラウド ストレージ サービスにホストされている ZIP アーカイブをダウンロードする

ように誘導されます。アーカイブには、Visual Basic スクリプト ペイロードが含まれていました。そのペイロードは Windows インストーラ（MSI）パッケージを実行し、その結果 DARKGATE バックドアが実行されます。2023 年 10 月に、FIN6 も LinkedIn プラットフォームを使用して、標的組織の人事採用担当者に URL を送信しています。その URL を開くと、偽のレジュメサイトにホストされている PDF ファイルをダウンロードするように求められます。FIN6 は、特定のユーザー エージェント文字列やジオフェンスなどのフィルタリング要件を使用して、URL へのアクセスを制限しました。条件を満たしたユーザーには、ZIP アーカイブが提供されます。そのアーカイブには悪意ある LNK ファイルが含まれていて、ダウンローダとバックドアの両方がインスタンス化されます。

> **ジオフェンス:** 攻撃者がある特定の地域内の個人のみを標的とする場合に使用する、特定の地理的位置を中心とした仮想境界。

QR コード フィッシング（「クイッシング」）

クイック レスポンス コード（QR コード）は、URL などのエンコードされたデータが含まれているバーコードの一種で、モバイル デバイスを使ってスキャンできます。モバイル デバイスでのウェブブラウザの使用状況を収集、モニタリングするのはあまり一般的ではありません。ユーザーがいつフィッシング ウェブサイトを利用するかを簡単には判断できないからです。QR コード画像に悪意ある URL をエンコードしてフィッシング メール内に埋め込むことで、攻撃者はメールのセキュリティ スキャンをすり抜けることができます。メール メッセージ本文内のハイパーリンクを検出することでスキャンしているからです。モバイル デバイスのブラウザで URL やウェブページを表示したときに、ユーザーがその信憑性を確認するのは、パソコンのブラウザ クライアントと比べると容易ではありません。2023 年に、攻撃者がフィッシング メールに QR コードを含める事例が確認されました。添付した PDF ファイルや画像ファイル内に QR コードを埋め込み、メールの受信者にバーコードをスキャンして請求書やドキュメントなどの情報を取得するように求めます。

2023 年 9 月以降、Mandiant は QR コードを利用して中国の State Taxation Administration（STA）を装うウェブサイトにフィッシング メールの受信者を誘導するという UNC5103 を観測しています。攻撃者は、フィッシング メールに Microsoft Word ドキュメントを添付して、受信者が開くと、税還付アプリケーションを開始する手順を組み込んだ悪意ある QR コードが表示されます。ユーザーがモバイル デバイスからなりすましの STA ウェブサイトを閲覧すると、名前、個人識別番号、銀行口座情報などの個人情報を提供するように求められます。

2023 年 9 月から 10 月にかけて、UNC5092 は侵害したサードパーティのメール アカウントを使用して、QR コードが含まれている画像ファイルを添付したフィッシング メールを送信しています。QR コードにはエンコードした URL が含まれ、認証情報を盗み出す目的でユーザーのモバイル デバイスのブラウザをなりすましの Microsoft ログインページに誘導します。Mandiant はその後、UNC5092 が敵対的中間者攻撃を仕掛けて追加的な認証情報を入手し、セッショントークンを盗み出したことを観測しました。UNC5092 は、入手したクラウド アクセスを利用して、多種多様なアクティビティを実施しました。外部デバイスを登録して MFA を有効にする、会社のメール アカウントにアクセスしてデータを精査する、メール受信トレイの新しいルールを作成する、SharePoint からファイルを入手する、内部ユーザーに不正な振込フィッシング メールを送信するといったことです。

SMS フィッシング（「スミッシング」）

攻撃者は SMS フィッシング（スミッシング）を介してユーザーを狙うことができます。これは、インターネットへの常時接続というモバイル デバイスの性質を利用した手法で、認証情報を盗み出す目的でなりすましのログインページなどのウェブ コンテンツを読み込みます。2023 年に、Mandiant は SMS フィッシングに関する複数のインシデントに対応しました。

2023 年 10 月のある事例では、攻撃者は第三者金融機関のヘルプデスク メンバーを装って SMS メッセージを送信し、社内システムからなりすましのウェブページに受信者を誘導しています。この悪意あるウェブページにアクセスしたユーザーは、社内システムに AnyDesk リモート アクセス ソフトウェアをインストールするように求められます。攻撃者は、標的システムへのリモート アクセスを獲得すると、ユーザーの第三者金融機関口座に関連する複数のウェブページに移動しました。新たにモバイルアプリへのアクセスを登録し、振込を利用して金銭を盗み出すのが目的です。

Mandiant は、UNC3944 が標的となった組織の従業員に対して SMS フィッシング キャンペーンを展開して、認証情報を取得したことも観測しています。その目的は標的の環境へのアクセスを獲得してエスカレーションすることです。2023 年半ばから、Mandiant は UNC3944 を特定しています。新しいフィッシング キットを利用して標的組織に属しているかのように見えるフィッシング ページを提供し、標的組織名と「-sso」や「servicenow」とを組み合わせたドメインを登録して使用します。以後見られた UNC3944 によるアクセスでは通常、クラウド リソースを標的としてデータ盗難と金銭獲得の足がかりを確立していましたが、この攻撃者は 2023 年にデータ恐喝とランサムウェアを含めた戦術に転換しました。

検出と緩和

SMS や QR コードといった代替プラットフォーム フィッシングによってユーザーの認証情報が侵害されたときに、侵害が最初に検出されたきっかけがクラウド セキュリティ アラートだったということがよくあります。アラートの内容は、危険なログイン イベント、メールボックス ルールの作成、不審な MFA デバイスの登録、組織内の侵害されたユーザー アカウントを送信元とする不審なメールに関する社内外のユーザーからの報告などです。検出戦略には、前述のアクティビティに関するアラートの生成も含まれることがあります。プラットフォーム ログにはユーザー間で送信されたメッセージや URL も記録されることがあり、それらをプロアクティブに分析して不審なコンテンツがないか確認できます。たとえば、Microsoft 365 監査ログの場合、Microsoft Teams を介して送信された URL を MessageCreatedHasLink オペレーション内の MessageURLs 項

目に記録できます。代替プラットフォーム フィッシングの脅威を軽減するためによく使用される緩和手法には、Microsoft Teams で内部ユーザーとチャットしても問題ない信頼できる Microsoft 365 組織を指定する、フィッシングに耐性のある MFA 手法をデプロイする、Microsoft セキュリティ ガイド内で詳しく説明されている推奨事項を提供するといったことがあります[30]。

検出機会	検出名	擬似コード	説明	MITRE
ファイル ダウンロード - ウェブプロキシ	ファイル ダウンロード - 実行可能ファイル	Logsource = ウェブプロキシ Eventtype = ファイル ダウンロード Filetype = [exe、lnk、vb、…]	実行可能ファイルのダウンロード中に異常な拡張機能が確認されたら、アラートを通知します。	T1566.002
ファイル ダウンロード - ウェブプロキシ	ファイル ダウンロード - コンテナに実行可能ファイルが含まれている	Logsource = ウェブプロキシ Eventtype = ファイル ダウンロード Filetype = [zip、rar…] Archive_Contents = [exe、vb、com、bat、js、…]	パスワードで保護されているとはいえ、多くのアーカイブがその内容をまとめたディレクトリを公開しています。ツールによっては、ログイベントメタデータにアーカイブの内容が含まれていることがあります。アーカイブに実行可能ファイルが含まれていたら、アラートを通知します。	T1566.002
ファイル ダウンロード - ウェブプロキシ	外部のクラウド ストレージからのファイル ダウンロード	Logsource = ウェブプロキシ Eventtype = ファイル ダウンロード Sourcedomain = [*.onedrive.com、drive.google.com、*.sharepoint.com、…]	クラウド ストレージを利用して他の組織とやり取りすることがほとんどない場合、外部組織のクラウド ストレージが使用されたら、アラートを通知します。承認されたドメインから情報を入手するためのダウンロードであるとマークします。	T1566.002
ファイルの書き込み - エンドポイント	不審な LNK ファイルの作成	Logsource = エンドポイント Eventtype = ファイル作成 Filetype = lnk コンテンツの内容（cscript または wscript または cmd または powershell または curl または wget または bitsadmin または …）	スクリプト環境を実行するためか、またはインターネットからコンテンツをダウンロードするツールを起動するために使用される、LNK ファイルの作成を調べます。一部のエンドポイント検出対応ツールと Sysmon から、この分析情報を得ることができます。	T1566.002
ファイルの書き込み - エンドポイント	WSF ファイルの作成	Logsource = エンドポイント Eventtype = ファイル作成 Filetype = wsf	お使いの環境に WSF ファイルが存在することはめったにありません。存在しない環境の場合、そのようなファイルが作成されたら、アラートを通知します。	T1059

続き

検出機会	検出名	擬似コード	説明	MITRE
ファイルの書き込み - エンドポイント	マクロを含めることが可能な Office ファイルの作成	Logsource = エンドポイント Eventtype = ファイル作成 Filetype = [doc、docm、xls、xlsm、…]	組織のほとんどは、旧式の Office ドキュメント形式を使用しなくなっています。こうしたファイル形式がディスクに書き込まれたら、アラートを通知します。また、マクロ固有のドキュメント タイプが書き込まれたら、アラートを通知します。	T1566.001
メール セキュリティ ゲートウェイ	マクロを含めることが可能な Office ファイルをメールに添付	Logsource = メール Eventtype = メール Attachment=true Filetype = [doc、docm、xls、clsm、…]	組織のほとんどは、旧式の Office ドキュメント形式を使用しなくなっています。マクロ指向の添付ファイルはブロックしてください。そうしない場合は、アラートを通知し、調査を始めてください。	T1566.001
エンドポイント実行	パワーユーザー以外のエンドポイントでの cURL の使用	Logsource = エンドポイント Eventtype = プロセス開始 Filename = curl.exe NOT user = [パワーユーザーのリスト…]	組織内の Windows エンドポイントで cURL が異常なほど使用されたら、アラートを通知します。	T1204.002
エンドポイント実行	MSI パッケージの使用	Logsource = エンドポイント Eventtype = プロセス開始 Filename = *.msi	MSI ファイルが実行されたら、アラートを通知します。	T1204.002
Teams メッセージ	Teams ユーザー間で送信された不審なリンク	Logsource = M365 Eventtype = MessageCreatedHasLink MessageURL に [組織のドメインに似た文字列] が含まれている	Teams 経由で URL が送信されたら、アラートを通知します。さらに多くのアカウントをキャプチャする目的で類似のドメインを参照している可能性があります。	T1534
ネットワーク接続	類似のドメインへのネットワーク トラフィック	Logsource = [dns、webproxy] ドメインに [組織のドメインに似た文字列] が含まれている	ドメインへの DNS クエリまたはウェブ トラフィックに不審な文字列があれば、アラートを通知します。たとえば、example.com ではなく ex4mple[.]com。	T1583.001
MFA 変更	ユーザーの MFA に対する変更または追加	Logsource = MFA Eventtype = [電話の変更、電話の追加]	MFA プロファイルに記載のユーザーの電話番号はめったに変更されません。ユーザーにアラートを通知し、確認を取ります。	T1098.005

まとめ

攻撃者は、従来のフィッシング対策の対象範囲を超えて攻撃手法の有効性を高めてきました。「信頼できる送信者からのメールにだけ対応する」といったユーザー意識のコンセプトは、攻撃者が侵害した第三者のアカウントを使用した場合や、会話の乗っ取り、内部フィッシング、インタラクティブなソーシャル エンジニアリングといった手法を使用した場合には有効ではなくなっています。組織の可視化範囲外にあるユーザー デバイスも標的にされるようになっており、技術を駆使して認証を厳重に制御し、不審なアクセスを検出する必要性が増しています。感染チェーンに複数の攻撃者が関わっていることがよくあります。この場合、最初のフィッシング アクセスを確立してバックドアを制御するグループと、攻撃活動を短期間に重ねて発生させるグループが異なります。検出と脅威ハンティングに関する包括的な戦略を策定する際に、侵入ライフサイクルの全段階にわたって行動指標に焦点を当てると、これまでにない初期アクセス手法であっても識別しやすくなります。セキュリティ インシデントの影響を限定的なものにとどめるには、侵入アクティビティを早期に検出してシステムを迅速に封じ込めることが欠かせません。

AiTM を利用して MFA を突破する攻撃者の実態

Mandiant は、多要素認証（MFA）で構成されたクラウドベースの ID に対する侵害が増えていることを観測しています。組織全体で MFA を導入することが一般的になり、それに合わせて攻撃者は広く導入された MFA 手法の弱点を突く各種方法に習熟しつつあります。
そのことは、ウェブプロキシや敵対的中間者（AiTM）フィッシング ページの導入が増えていることに如実に表れています。センシティブなログイン セッション トークンを盗み出すことで、ほとんどの MFA 実装を無効化しています。

よく使用される MFA 手法

MFA ソリューションの多くは、認証リクエストを管理および承認できるさまざまなメカニズムを備えています。AiTM フィッシングに耐性があるメカニズムであっても、さらに別のインフラストラクチャとオーバーヘッドが必要になることがよくあります。一方、最もよく使用される MFA メカニズムは、AiTM フィッシングを利用する攻撃者の対象になりやすいメカニズムでもあります。

MFA タイプ	説明
プッシュ通知	通話アプリのプッシュ通知を受け入れるか、モバイル デバイスのキーを押すことだけをユーザーに求める通話アプリまたはモバイル アプリベースのプロンプト。プッシュ通知にはアクセス対象のリソースに関するコンテキストが欠けていることがよくあり、そのために MFA 疲労攻撃を受ける可能性があります。その場合、プロンプトが承認されるまで、繰り返しリクエストがユーザーに送信されます。
ワンタイム パスワード（OTP）/ 時間ベース ワンタイプ パスワード（TOTP）	SMS メッセージやメール メッセージからのコード、つまりモバイルアプリやハードウェア デバイスによって生成された時間制限コード。認証中か認証後にユーザー名とパスワードとともに入力します。SIM スワッピングと認証情報窃取のウェブフォームは、こうしたコードを盗み出す際によく使用される方法であるだけでなく、シードを盗み出して情報を漏洩させる、クラウドと同期している TOTP コードにアクセスできるアカウントを乗っ取るといった攻撃を受けやすい方法でもあります。
番号照合で確認するためのプッシュ通知	ユーザーのモバイル デバイスで生成されるプッシュ通知プロンプト。ログオン ポータルによって生成されたコードを入力する際にのみ同意できます。MFA 疲労に関連する悪用メカニズムだけでなく、TOTP コードやシードの盗難にも対処できます。
証明書ベースの認証（CBA）	デバイスにインストールされる X.509 証明書を必要とする認証。AiTM フィッシング攻撃に対する耐性。
ハードウェア キー	FIDO2 標準または U2F 標準と互換性がある物理デバイス。サポートされているクラウド認証サービスで公開鍵暗号を使用します。この標準では、サーバーから鍵をリクエストされ、その鍵に関連付けられたサーバーが照合されます。そのため、AiTM フィッシング攻撃に耐性があります。

認証情報窃取の進化: 中間者攻撃

攻撃者は、標的からログオン認証情報を入手する手段として認証情報窃取フォームやフィッシング ページを利用することがよくあります。このようなウェブサイトはよく使われるログイン ポータルによく似せて作られ、ここに標的ユーザーが入力した認証情報と MFA コードが攻撃者に転送されるようになっています。ビジネスメールの侵害の調査中に、Mandiant は攻撃者が認証情報と時間ベースの MFA コードを非公開の Telegram チャネルに転送する認証情報窃取フォームを運営していることを観測しました。このように認証情報を盗み出したことが即座に通知されるので、攻撃者はその機会を逃さず MFA コードが期限切れになる前にまんまとログインし、標的となったアカウントへの初期アクセスを確立できます。

AiTM フィッシング ページは一般的な認証情報窃取フォームに勝る攻撃力があり、一般に広く導入されている MFA 手法に対処するように設計されたインフラストラクチャを使用しています。従来の認証情報窃取フォームと異なり、AiTM ページは標的のユーザーと正規のログオン ポータルとの間でリバース ウェブプロキシとして動作します。AiTM ページは、認証情報と MFA コードを傍受するだけではありません。それ以上に重要なのは、ログオン ポータルから発行される認証後のセッション トークンも傍受することです。こうしたトークンを攻撃者が使用した場合、最初のログインで評価されるだけのセキュリティ管理をバイパスできます。

従来の認証情報窃取フォームと比べると、AiTM フィッシング インフラストラクチャの設定は相対的に複雑であることから、これまで攻撃者による導入は限られてきました。ところが、2023 年に Mandiant は攻撃者によって導入された AiTM フィッシング ページが著しく増加していることを観測しました。攻撃者の間で AiTM を使用する動きが加速しているのは、サイバー犯罪の闇市場で Phishing as a Service というパッケージが提供されているためである可能性があります。このようなパッケージを利用すると、高度な技術力を持たない攻撃者でも、定期的に保守されるフィッシング インフラストラクチャにアクセスして、複雑なキャンペーンを展開できます。

検出と緩和

AiTM フィッシングは MFA など厳格な管理手法に直面している攻撃者の能力が進化した表れですが、AiTM フィッシング ページでまず侵害し、その後に盗み出したセッション トークンを使用するという手順は防御側に検出の機会を与えます。AiTM フィッシング ページは標的ユーザーのログイン情報を傍受してクラウド認証サービスに転送するように作られているため、このフィッシング インフラストラクチャに関連付けられている IP アドレスがユーザーの送信元 IP アドレスとして認証ログに記録されます。盗み出したトークンで認証するときに、攻撃者の IP アドレスとその関連するユーザー エージェント文字列（初期の AiTM ログオンとは異なることがあります）も記録されます。とはいえ、防御側は、地理的に不審あるいは想定外の送信元 IP アドレス、データセンターを発生源とするログインなどの異常のモニタリングを継続する必要があります。

Mandiant が実施したほぼすべての調査でクラウド アカウントが侵害されており、攻撃者は初期アクセスを獲得するとすぐに自身の MFA 手法を登録することが観測されています。これは通常、セルフサービス セキュリティ ポータルとやり取りすることによって行われます。これは AiTM 攻撃と盗み出したセッション トークンに限ったアクティビティではありませんが、それでも効果的な検出機会として強調しておきます。他のログオン異常とペアで考えた場合には特にそうです。新しい MFA 登録を定期的に確認するだけでなく、複数の MFA 手法を構成してアカウントを監査すると、さらに調べてみる価値がある事象を明らかにできます。

AiTM 攻撃から効果的に防御するには、AiTM に耐性のある MFA 手法とアクセス ポリシーの組み合わせを追求する必要があります。ほとんどのクラウド認証サービスが、ログオンをブロックできるアクセス ポリシーをサポートしています。ブロックする基準は、組織が定義した場所、デバイス管理ステータス、アカウントのログオン プロパティ履歴に基づいたリスク評価などです。こうしたアクセス ポリシーを実装するときは、ログオン セッション全体を通して継続的に適用できるかを理解することが重要です。通常、ほとんどのアクセス ポリシーは、最初にトークンを発行する段階で適用されるだけで、以前に盗まれたトークンが使用された場合には保護できません。

検出機会	MITRE ATT&CK	ルールロジック
Okta - FastPass を使用して AiTM フィッシングを検出する	T1078 T1556	eventType = "auth_via_mfa" AND result=FAILURE AND reason ="FastPass がフィッシング攻撃を拒否"
Azure - 認証方法の変更	T1098 T1556	LoggedByService="認証方法" AND Category="UserManagement" AND OperationName="ユーザーが登録したセキュリティ情報"
M365 - 多要素認証の無効化を検出する	T1556	LogSource = M365 監査ログ AND Operation="*強固な認証を無効にする。*"
MFA なしのデバイス登録	T1078.004	Logsource = Azure ログインログ AND resourceDisplayName = “デバイス登録サービス” AND status = “成功” AND NOT authenticationRequirement = “multifactorAuthentication”
ユーザーの Okta MFA 要素をリセットする試み	T1098	Logsource = Okta システム イベント AND action = “user.mfa.factor.reset_all”

まとめ

AiTM フィッシング ページは今後も増えていく見込みであるにもかかわらず、組織の多くが依然としてトークンの盗難から保護できないセキュリティ対策を利用しています。そのうえ、トークンの盗難と盗み出されたトークンの使用を軽減できたとしても、今のところそれだけであらゆる状況に対応できるわけではありません。組織は、フィッシングに耐性のある MFA 手法と効果的なアクセス ポリシーを実装することで、AiTM トークンの盗難からさらに効果的に保護できます。また、ログオン セッションの間継続してポリシーを評価するようにして、盗み出されたトークンが使用されるリスクを軽減できます。こうした管理対策を異常に基づく効果的な検出手法と組み合わせることで、フィッシング攻撃のリスクと攻撃者の滞留時間を大幅に削減できます。

クラウド侵入の動向

企業によるクラウドの導入とハイブリッド クラウド / オンプレミス環境の使用が拡大を続ける中で、攻撃者も同じく標的の後を追いかけています。攻撃者は、クラウド環境に保存されているデータと、将来の悪意ある活動に利用できるコンピューティング リソースの価値を理解しています。Mandiant は、さまざまな動機を持つ攻撃者がクラウド環境に狙いを切り替えてクラウドにホストされているデータを標的とし、攻撃活動でクラウド コンピューティング リソースを利用していることを継続的に観測しています。

Identity and Access Management を標的とし、MFA 要件をバイパスする

従来、クラウドとハイブリッド環境への初期アクセスを獲得する場合、多要素認証 (MFA) が必要なかったこともあって、攻撃者は盗み出した認証情報とアクセス トークンを利用してきました。ここ数年、セキュリティ意識が高まり、MFA の導入が増えてきたことから、攻撃者はソーシャル エンジニアリングにますます重点を置くようになっています。標的を狙ったソーシャル エンジニアリング キャンペーンの展開中、攻撃者はユーザーを誘導して認証情報を入手し、革新的な方法を使用して MFA をすり抜けるか、その実装に潜む弱点を悪用しようとします。

Mandiant は、セッション トークンをキャプチャして MFA 要件をバイパスする目的で敵対的中間者 (AiTM) 手法を使用する例が増えていることを観測しています。AiTM キャンペーンでは、標的のユーザーから正規のクラウド サービスへの接続が攻撃者の制御下にあるサーバーでプロキシされます。そうすることで、ユーザーの認証情報と MFA 手法が正規のクラウド サービスにリレーされるとともに、攻撃者はユーザーに返されるアクセス トークンをキャプチャできます。正規のクラウド サービスのログオンページを模倣した本物そっくりのランディング ページを自動的に構築できる AiTM キットが、攻撃者から数多く提供されています。Mandiant が 2023 年に対応したビジネスメール侵害 (BEC) 事例のほとんどで、攻撃が成功した標的のユーザーは MFA を構成していたものの、AiTM フィッシング キャンペーンによって回避されていました。

攻撃者は、ソーシャル エンジニアリングを利用してユーザーを狙うことが知られています。Mandiant はこうしたキャンペーンの有効性を継続的に観測しています。スパイ関連の調査から、標的と同じ業界の個人になりすませるようにスピア フィッシング メールをかなり調整したうえで使用し、ユーザーに関連する正規のコンテンツを使用して信頼性を築いていることが明らかになりました。標的のユーザーは、メール内のリンクをクリックし、さらに保護された情報にアクセスするための認証情報を入力するよう誘導されていました。ユーザー名とパスワードを入手したら、攻撃者は MFA プッシュ通知をトリガーして、標的のユーザーの同意を得ます。

また、攻撃者がヘルプデスクとテクニカル サポート担当者の信頼された役割を悪用していることを Mandiant は観測しました。あるケースでは、テクニカル サポートを送信元と詐称するフィッシング メッセージを配信して、ユーザーを誘い込んでクラウド プラットフォームへの悪意あるログインを MFA で承認させようとしていました。また別のケースでは、金銭目的の攻撃者 UNC3944 が権限を昇格できるユーザーの認証情報を入手するためにソーシャル エンジニアリングを大いに活用していました。SMS フィッシングを利用するだけでなく、標的組織のヘルプデスクに電話をかけて、ユーザーのパスワードや関連する MFA デバイスをリセットしました[31]。

2023 年に、標的を狙った SIM スワッピングを使用してアカウントへのアクセスを獲得する例が増えていることを観測しました。これが効果的であったのは、組織が時間ベース ワンタイプ パスワード MFA コードを SMS メッセージで送信していたからです。このほか、パスワード再設定リンクを送信する前に、SMS を使用してアカウントの所有者であることを確認するケースもありました。金銭目的の攻撃者が SIM スワッピングを利用して両方のタイプの SMS コードを受け取り、容易にアカウントを乗っ取っていることが観測されています。金銭目的の脅威クラスタ UNC3786 は、認証情報を侵害して標的組織の Okta や Microsoft 365 アカウントへのアクセスを獲得するために、日常的に SIM スワッピングを実行していました。UNC3786 侵入のあるケースでは、SIM スワップの実行中、攻撃者は標的ユーザーの電話にスパム SMS メッセージを送信して、携帯通信会社から送られてくる SIM スワップ関連の通知に気付かせないようにしていました。UNC3944 も同じように、ユーザーの認証情報と SMS MFA コードへのアクセスを獲得するために SIM スワッピングを利用していました[32]。

攻撃者がクラウド ログイン ポータルに対するパスワード推測攻撃を実行して MFA が構成されていないアカウントを特定しようとしていることを Mandiant は継続的に観測しています。MFA デバイスをユーザー自身が登録することになっている組織が少なくありません。つまり、アカウントにまだ MFA がない場合、初めてパスワードの認証に成功すると、すぐに MFA デバイスを登録するように求められます。これまで、スパイ活動を展開する攻撃者がこうした推測攻撃を実行して、MFA が構成されていない休眠アカウント (本来なら無効にすべきアカウント) や MFA が求められないサービス アカウントを見つけて乗っ取る事例を見てきました。

脆弱な認証情報保管

他に、攻撃者が適切に保管されていない認証情報を使用して、クラウド環境へのアクセスを獲得したケースを Mandiant は観測しました。あるインシデントでは、インターネットにアクセスできるサーバーのデフォルトの構成が原因で、クリアテキストの AWS 認証情報が検出されて侵害されました。その結果、攻撃者は標的の AWS 環境へのアクセスを獲得できました。また別のケースでは、攻撃者は以前のインシデントで盗まれたと思われるアカウント認証情報を利用して、標的組織のクラウドにホストされているコード リポジトリ（MFA が求められないリポジトリ）へのアクセスを獲得していました。Mandiant はこのほか、攻撃者が漏洩した AWS アクセスキーを使用して標的組織の AWS 環境にアクセスするというインシデントに対応しました。調査したところ、このアクセスキーは EC2 インスタンスにホストされた組織所有の Docker コンテナから発信された可能性が高く、そのコンテナはインターネットに公開されていたことが明らかになりました。同じキーのコピーが、パブリック IP アドレスを指定できる標的組織が所有していない他のリソースでも見つかりました。

攻撃者によるクラウド サービスの悪用

クラウド環境への初期アクセスを獲得した後、攻撃者がクラウド ネイティブのツールとサービスを悪用してアクセスを維持し、ラテラル ムーブメントを行って、最終的にデータを盗み出すなどのミッション目標を達成していることを Mandiant は観測しました。攻撃者は、プリインストールされたツールだけを利用するように制限することで、目立たないように活動して検出を逃れ、クラウド環境に長期間存続できます。

攻撃者が Azure Data Factory と AirByte を使用してデータ ウェアハウス、ストレージ blob、SQL データベースなどのさまざまな統合プラットフォームに保存されているデータを盗み出すように既存のパイプラインを変更したことを Mandiant は観測しています。特に、攻撃者はそうしたデータソースから攻撃者が管理する SFTP サーバーにデータをエクスポートするパイプライン ジョブを作成していました。データ ファクトリーを使用すると、攻撃者は安定した高帯域幅のプラットフォームを利用して大量のデータをコピーできます[33]。

Mandiant は 2023 年に、金銭目的の攻撃者 UNC3944 がこれまでエスピオナージ グループによる使用しか観測されていない手法を使用して、クラウド ID プロバイダ（IDP）のバックドアを仕掛けたことを観測しました。何度か調査したところ、UNC3944 は Entra ID（旧 Azure AD）に対する管理者権限を獲得し、不正なフェデレーション ID プロバイダを構成して、ゴールデン SAML 攻撃を実行していました。この場合、攻撃者は、Entra ID によって保護されたリソースに対し、組織内の任意のユーザーとして認証できるようになります。そのユーザーのパスワードや MFA デバイスの所有の有無を知らなくてもかまいません。ある調査で、Mandiant は UNC3944 が組織の Active Directory Federated Services（ADFS）サーバーを標的として、Mimikatz を実行したことを観測しました。トークン署名証明書を入手して、ゴールデン SAML 攻撃を仕掛けることが目的です。

Mandiant はこのほか、攻撃者がクラウド コンピューティング インスタンスを標的として、標的のクラウド環境にステルス型で永続的に存続していたことを確認しました。複数のインシデントで、攻撃者は Azure Virtual Machines（VM）を作成して、パブリック IP アドレスを割り当てていました。攻撃者が作成したこうした VM には、組織が義務付けているセキュリティとロギングのソフトウェアがインストールされていませんでした。それにより、攻撃者は組織の仮想ネットワークまたは Virtual Private Cloud の内側にある信頼されたシステムにモニタリングされずにアクセスできる方法を確立したうえで、侵入を進めていました[34]。

クラウド コンピューティング インスタンスは、仮想プライベート ネットワークを介して組織のオンプレミス ネットワークとのネットワーク接続を確立していることがよくあり、それがラテラル ムーブメントの足がかりとなることがあります。UNC3944 が Azure コンソールにアクセスしてから Special Administration Console を使用して Azure ホステッド VM にラテラル ムーブメントを加え、シリアル コンソール経由で VM に接続するというケースが何度か発生しています。攻撃者は、Azure VM でシリアル コンソールを悪用してサードパーティのリモート管理ソフトウェアをインストールし、VM に永続的にアクセスできるようにしています。この攻撃方法は、Azure 内で採用されていた従来の検出方法の多くをすり抜け、VM に対する完全な管理者権限を与えるという点で、これまでにないものです。

Mandiant は、攻撃者が自ら把握した重要な処理能力に基づいてクリプトマイニングを行うという特定の目的でクラウド インフラストラクチャを標的としていることも観測しています。あるインシデントでは、攻撃者は漏洩したサービス アカウント キーを利用して標的組織の Google Cloud Platform（GCP）プロジェクトへのアクセスを獲得していました。プロジェクトにアクセスした後、攻撃者は起動スクリプトを備えた 1,200 を超える仮想マシンをデプロイしていました。スクリプトは、XMR-Stak マイナーを使用して Monero 暗号通貨マイナーを実行します。

このほか、攻撃者がオープンソースの攻撃的なセキュリティ ツール セットを利用して環境を調査するケースもいくつか見られました。あるケースでは、オープンソースの AWS エクスプロイト フレームワークである Pacu や、クラウド インフラストラクチャへの悪用可能な攻撃パスを検出できるオープンソースのコマンドライン ツールである CloudFox といったツールを利用して、自動偵察を実行していました。また別のケースでは、クラウド型のセキュリティ監査ツールである ScoutSuite を使用して、AWS API とコンソールへのアクセスを獲得し、AWS 環境に暗号通貨データマイナーをデプロイするといった活動を実施していました。

推奨事項

Mandiant は、攻撃者が ID 管理プラクティスと認証情報保管の実装に見られる脆弱な部分を標的とし、正規の認証情報を入手して MFA をすり抜けるケースを継続的に観測しています。攻撃者は MFA をバイパスする新たな方法の開発を続けているため、それに応じて組織は強固なセキュリティ ポスチャーを維持できるように認証ポリシーに変更を加える必要があります。フィッシングに耐性のある MFA 手法は、ウェブブラウザ、オペレーティング システム、クラウド サービス プロバイダによって広くサポートされています。 フィッ

シングに耐性のある MFA 手法の中でもよく使用されるのが、証明書ベースの認証（CBA）と FIDO2 セキュリティ キーの 2 つです。組織は、SMS、通話、TOTP コードといった以前の MFA 手法を段階的に廃止し、こうした新しい手法を優先することで、MFA による保護をすり抜けようとする攻撃を抑制できます。

CBA では、ユーザーの身元、使用中のデバイス、対応する秘密鍵を特定する証明書がプロビジョニングされます。秘密鍵は、クラウド サービス プロバイダに対してユーザーの ID を証明するために使用するものです。ユーザーが秘密鍵の入力を求められることはありません。ユーザーが秘密鍵を意識することもありません。今日使用されているほぼすべてのエンドユーザー システムには、トラステッド プラットフォーム モジュール（TPM）が含まれています。CBA で使用される秘密鍵などの暗号鍵の安全な保管と管理を別々のチップで行うモジュールです。鍵マテリアルは TPM のハードウェア境界を離れることはないため、デバイス上のマルウェアが鍵マテリアルを盗み出すことはできません。CBA を使用している場合、相互 TLS 認証を使用して接続がネゴシエートされます。この認証は、ほとんどのフィッシング手法に耐性があります。ユーザーはシークレット キーについて認識せず、指定を求められることもないからです。AiTM を使用する手法も阻止されます。標的ユーザーのログイン セッションをプロキシするには、攻撃者は TLS 接続を終了することで CBA を突破する必要があるからです。

FIDO2 セキュリティ キーは、CBA と同じようなセキュリティ モデルを利用してフィッシングに対する耐性を確保しています。両者の大きな違いは鍵のポータビリティです。FIDO2 セキュリティ キーは USB デバイスであることが多く、鍵マテリアルが物理キーのハードウェア境界を離れることはありません。ユーザーは、キーの値を認識せず、指定を求められることもありません。FIDO2 用に構成されているウェブサイトごとに一意の秘密鍵があり、各鍵が特定のアプリケーションに関連付けられています。ユーザーがフィッシング ウェブサイトを閲覧した場合、ブラウザはセキュリティ キーの入力をユーザーに求めることを拒否します。フィッシング ドメインが、構成済みのいずれのキーとも一致しないからです。

クラウド サービス プロバイダ（CSP）では、よく使用されるクリプトマイナー スキームを検出して阻止する場合に役立つツールを数多く提供しています。まずいずれの CSP も、アクセスキーと API シークレットを上回るセキュリティ機能を備えた認証方法をサポートしています。組織には、クラウド アカウントを監査し、アクセスキー（特に「root」や「superuser」）を削除して、最新のロールベースのプログラマティックなアクセス シークレットの採用を進めるプログラムを確立することが望まれます。また、予算編成のアラートと制限は、異常な支出がないかクラウド アカウントをモニタリングする場合に効果的です。これは、クラウド アカウントをハイジャックした暗号通貨スキームの高忠実度を表すシグナルとなることがよくあります。最後に、新しいクラウド環境を構築する場合には、「デフォルトで保護」という設計の使用を検討してください。「デフォルトで保護」をベンダーのベスト プラクティスに設計段階から組み込むと、攻撃対象領域を減らすことができます。

また、クラウド リソースへのアクセスを信頼できるデバイスだけに限定する管理手法を追加で実装することも考慮してください。正確な表現は異なっても、各 CSP はなんらかの形でこうした管理手法をサポートしています。これを行うには、モバイル デバイス管理（MDM）テクノロジーを使用して、デバイスの状態を維持し、登録済みのデバイスからの認証だけを許可します。信頼できないデバイス（たとえば、ホテル内のパソコン）を使用してリソースにアクセスしなければならない場合、組織は何にどのようにアクセスできるかを制限するポリシーを導入する必要があります。たとえば、ユーザーは信頼できないデバイスからクラウド管理コンソールにアクセスできないようにします。同様に、信頼できないパソコンへのドキュメントのダウンロードを限定または制限します。

レッド（およびパープル）チームの活動における AI

John McCarthy は、コンピュータ サイエンスと認知科学の両方の分野で知られ、1955 年に「知的な機械を作る科学と工学」を意味する「人工知能（AI）」という用語を作りました。この研究は機械の振る舞いを作る手段、人間のように機能する手段として始まりましたが、最新の動向を見ると、その意味は人間のように学習できる機械を網羅するまでに進化しています。人気のある SF で描かれる AI システムにはまだ遠く及ばないものの、AI は今大きく成長し、投資が拡大して、期待の膨らむ時期にあります。大規模なディシジョン ツリーを備えたロジック マシンとして始まったものが、無数の統計と大規模なコンピューティング能力に基づいて非常に複雑なアルゴリズムへと発展してきました。こうしたアルゴリズムの中でもこのところ特に話題を集めているのが、何かを作り出すように設計されたアルゴリズムです。こうしたシステムは、一般に生成 AI と呼ばれています。

標的型攻撃ライフサイクル: 標的型攻撃活動を実施するときに攻撃者が発生させるイベントの一般的なシーケンス

生成 AI は、複数の生成 AI ツールがリリースされたのを受けて、このところ関心を集めるとともに一定の成果を上げています。生成 AI は今、かつてないスケールでコンテンツを作成し、コンピュータ サイエンスの単なる技術基盤とは異なる分野を支援しています。サイバーセキュリティでは、生成 AI が検出エンジニアリングの分野に革命をもたらしています。ニューラル ネットワークと ML アルゴリズムは今、さまざまな検出対応ツールセットの中核をなしています。その一方で、まだ導入が大きく進んでいないものの、著しく進歩する可能性を秘めている分野に、プロアクティブなセキュリティとレッドチーム評価があります。

レッドチーム評価では、Mandiant エキスパートが現実世界の攻撃シナリオをシミュレートすることで、顧客のセキュリティ プログラムの機能を評価します。Mandiant は、攻撃者による AI の使用が主に標的型攻撃ライフサイクルの初期アクセス ステージに限られていることを観測しています。中でも特に、ソーシャル エンジニアリングと情報活動に限って使用されています。Mandiant のレッドチームは、同じように生成 AI を利用してきました。そこで明らかになったのは、AI を利用してクライアント環境への初期アクセスを獲得するようになって生成 AI の導入が大きく進んだことです。

ソーシャル エンジニアリングのプリテキスティング

レッドチーム診断で生成 AI を使用する際によく見られる例の一つに、コンテンツとメディアを生成するプロセスを支援することがあります。Mandiant レッドチーム診断では、ソーシャル エンジニアリングを実施することもよくあります。その場合、Mandiant は知らないうちに悪意ある行動を取るようにクライアントを誘導します。これは、なりすましのメールやウェブサイトなどテキストや画像ベースのチャネルを通して一般に広く行われています。Mandiant のコンサルタントは、生成 AI ツールを使用して、いつもと変わらないコミュニケーションを装って悪意ある最初の草稿メールと、よくあるようなランディング ページを作成しました。こうしたソーシャル エンジニアリングに成功すると、クライアント ネットワークへのアクセスを獲得できます。多くの場合、これが評価の最初の目標です。

ただし、レッドチーム診断でソーシャル エンジニアリング活動を実行するときに有益な指標は成功のみではありません。設定ワークフローを AI システムにオフロードすることで、Mandiant は全体的なスループットを高めることができます。ソーシャル エンジニアリング キャンペーンの設定と実行を迅速化すればするほど、より多くのキャンペーンを実施できる可能性があります。テンプレートを最初から作成すると、細部の調整にかなり時間がかかることがありますが、代わりに生成 AI を活用すると、ソーシャル エンジニアリングのプリテキスティングをすばやく準備できます。

迅速なツール開発

生成 AI を活用してソーシャル エンジニアリングのプリテキスティングを作成できることと同様に、ソフトウェア開発においても、プログラミングの多くの領域で生成 AI の有用性が実証されてきました。Mandiant は、レッドチームのエンゲージメントの際に AI を使用してカスタムツールの開発を支援する際にも、同様の進歩があったことに気付きました。生成 AI は、よく知られたアルゴリズムとデータ構造を支援するときに有用なリソースであることが明らかになっています。自然言語で書かれた説明からコードを生成できるほか、一般的なデベロッパー環境に統合することも可能です。レッドチーム診断では、一般的ではなかったり新たに導入されたアプリケーションやシステムに出会うことがよくあるのですが、そうしたときにこれらの機能とインテグレーションは大きな価値をもたらします。

環境が運用規範に適さない場合、Mandiant はさまざまなエンゲージメント目標の達成を支援できるよう、可能な限りツールを活用することを目指します。あるシナリオでは、Mandiant のコンサルタントは、生成 AI を活用して構築した一連のツールで、アクセス可能なクラウド環境を列挙し、顧客の環境のセキュリティ ポスチャーを改善するための推奨事項を提示できるようにしました。生成 AI がなければ、このプロセスにはるかに長い時間がかかり、コンサルタントは運用や配信の価値をもたらすことではなく関連するドキュメントをくまなく調べることに時間を費やさざるをえなかったはずです。

エンゲージメントを進める中で構築したツールは、エンゲージメントの終了後も問題なく動作することが多く、再利用すれば将来にわたって引き続き価値がもたらされます。初期の調査と作成にかかる時間を解消することで、反復利用によって得られる価値が高まります。ツールの利用が形式化され、今後のエンゲージメントでも同じツールが利用されるようになるからです。

迅速な知識獲得

パープルチームのエンゲージメントでは、Mandiant は攻撃者と防御側の両方の視点からクライアントの環境の理解に努めます。ロギング、データ ストレージ、検出スタックには、オフザシェルフ ソフトウェアからオーダーメイドのソフトウェアで構成されたカスタムビルドの検出スタックまで、さまざまなパッケージが存在します。そのため、コンサルタントが配属された環境で、顧客の日々の運用に利用されている防御ツールキットについての知識が十分にないという状況がよく発生します。そのため、Mandiant のコンサルタントは使用中のプロダクトだけでなく、それがテスト対象の攻撃にどのように対応するかについてもよく理解することが必要になります。

> **レッドチーム:** レッドチームは、脆弱性を特定する目的で組織を攻撃する計画を立てて実行します。

> **パープルチーム:** パープルチームは、レッドチームと防御側とのコミュニケーションとコラボレーションを促進して、インシデント対応能力を高めます。

先ごろ、Mandiant は会話機能での生成 AI の使用を開始しました。まずはプラットフォームの理解を深め、その後プラットフォームのセキュリティの側面に重点を移すことが狙いです。生成 AI による会話は何度も繰り返されることがよくあります。最初のリクエストは、たとえばソフトウェアのある特定の部分をロギングする場合によく使用される方法について AI に尋ねる、といった流れになります。これを会話の糸口として、以前の回答と一般公開されているドキュメントを参照して質問を続け、より詳細なトピックに進みます。このワークフローでは、回答とそれに続くテストを入念に調べる必要があります。その作業の性質上、複数人が関わることになるため、フレームワークと初期ナレッジベースを用意して作業を進めると効果的です。最終的に、顧客の環境内にデプロイされた技術スタックをさらに正確に理解し、より良いエンゲージメント ワークフローとプロダクトを提供できるようになっています。

レッドチームでの今後の AI の導入

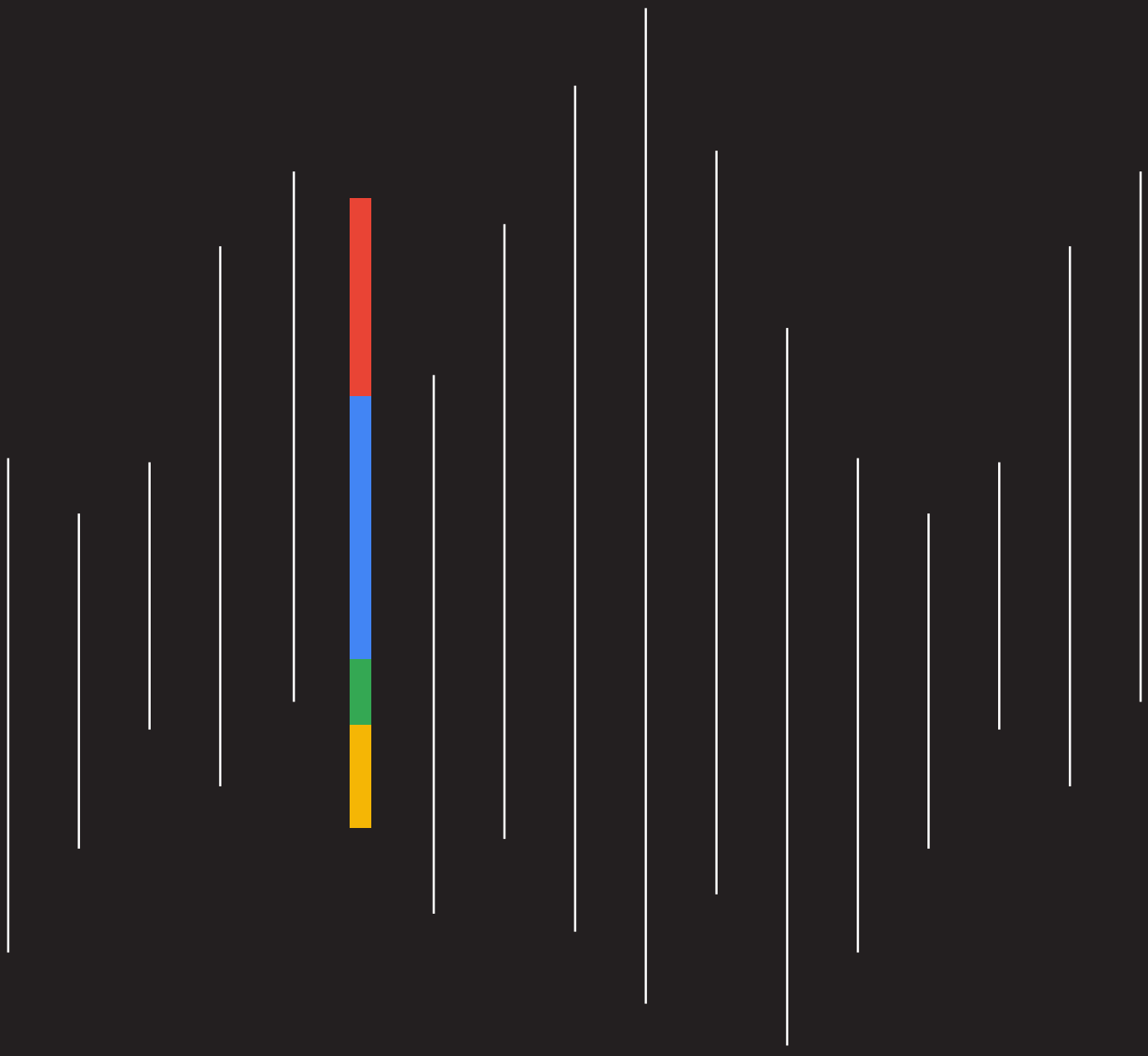
AI と大規模言語モデル（LLM）の開発チームは、開発済みの言語モデルに適切な価値というコンセプトを埋め込むことを目指しています。これは「AI アライメント」と呼ばれるコンセプトで、設計者が意図した目標に向けて、定義された価値の範囲で動作を進め、価値の範囲外にあるリクエストを拒否するモデルを生成しようというものです。AI アライメントは、AI の悪用を制限するガードレールとしての役割を果たします。攻撃者は、AI を利用して効率を高めてきましたが、独自のモデルを開発していないため、アライメントで定義されている範囲内で活動するか、アライメントを打破することが必要になります。Google は、さらに AI の不正使用の可能性がある事例を見つけて対処する、AI に特化した独自のレッドチーム[35] を運用しています。ただし、Mandiant のレッドチーム診断では、AI アライメントによって必然的な難題が発生します。

Mandiant のレッドチームは、顧客の環境のセキュリティを全体的に改善するために、顧客からのリクエストに応じて、容認された悪意あるアクションを実行します。AI アライメントというコンセプトによって、どの水準まで AI が適用され、どのようなときに AI がエンコードされた価値に応じて回答を提供しないかをレッドチームが想定できます。その一方で、レッドチームのエンゲージメントによって生み出された高品質のデータを活用して顧客のセキュリティに関する成果を改善し、さらにそれを使用して AI モデルをトレーニングできます。

LLM の魅惑的な機能に、分野固有の知識と言われるものをファインチューニングまたはトレーニングできることがあります。一般に使用される LLM のほとんどは、ジェネラリスト LLM です。つまり、モデルは奥深くかつ幅広い範囲の多様な知識分野を対象とするさまざまなデータでトレーニングされます。プログラミングに関してチューニングされる LLM もあれば、MedLM などのように医療分野の知識に的を絞った LLM もあります[36]。サイバーセキュリティ エキスパートを目的としたものには、Google の SecLM があります[37]。これは、最新の脅威を可視化して対策を講じられるようにするものです。特定の知識分野で LLM をチューニングするには、標的ドメイン内に莫大な量の専門データが必要です。レッドチームは、プロフェッショナルな組織として、大量のデータを生成して保存しています。こうしたデータを使用すれば、顧客の環境の保護に役立つようチューニングされたモデルをトレーニングできます。

こうした必然的かつ技術的な課題を解決するには、多面的なアプローチが必要です。レッドチームは、モデルのトレーニングに使用できる構造化データを生成し、対象となる分野の専門知識を AI デベロッパーに提供する必要があります。その一方で、AI デベロッパーは、AI アライメントで悪意あるアクティビティを正規に利用し、生成データでトレーニングするモデルへのアクセスを適切に保護する新たな方法を見つける必要があります。レッドチームの専門知識と高性能の AI リードとを組み合わせることで、将来はレッドチームの有効性が大幅に向上し、組織は強い動機を持つ攻撃者がもたらすリスクに常に先回りして対処できるようになる可能性があります。

まとめ



世界全体の滞留時間の中央値が継続的に減少していることは、好ましい傾向であり、防御側の取り組みによってできる限り早く脅威を検出できるという証しでもあります。ただし、攻撃者はあきらめていません。実際、攻撃者は検出回避に注力し始めています。それは、ゼロデイ脆弱性を使用する事例が増え、エッジデバイスやその他従来のセキュリティ対策による可視性にギャップのあるテクノロジーを標的としていることからも明らかです。こうした傾向は、2024 年に防御側が直面する難しい課題となることは避けられそうにありません。

組織は、セキュリティ チームがどのくらい早く検出回避戦術（さらに、フィッシングや MFA バイパスなど M-Trends 2024 で説明しているその他の脅威）から防御できるかをテストできます。その方法の一つが、レッドチームによる演習を利用することです。M-Trends 2024 では、Mandiant のレッドチームとパープルチームがどのように AI（さらには最新の攻撃戦術、手法、手順）を使用して、エンゲージメントの有効性を強化、改善して、顧客がセキュリティ管理の有効性を明確に理解できるようにしているかという点に着目しています。AI は高機能のツールであり、セキュリティ ツールキットで AI を使用してすばやく脅威を特定し、手間と時間のかかる作業を排除して、人材ギャップを埋める組織が増えています。攻撃側においては AI の使用は今のところ限定的[38]で、その中ではソーシャル エンジニアリングと情報作戦での使用が目立ちます。

準備は不可欠であり、包括的かつ多層的なものでなければなりません。レッドチームをはじめとするさまざまな演習を行ってセキュリティ チームをテストします。また、その他のベスト プラクティスには、コミュニケーションや法務など関連するチームが年間を通して定期的な机上演習に参加し、インシデント対応計画をテストして、継続的にレビューすることなどがあります。

脆弱性と漏洩の管理、最小権限の付与、セキュリティの強化などのしっかりとした基盤作りも、強固な防御態勢を築くうえで役割を果たしています。組織は、クラウドとオンプレミスから IT / OT、すべてのアセットに至るまで、全社にまたがる包括的なセキュリティ プログラムの構築に焦点を当てる必要があります。このプログラムは、影響力のある脅威インテリジェンスによって支えられている強固な検出機能とプロアクティブなハンティング機能に裏付けられたものである必要があります。

Mandiant のミッションは、あらゆる組織がサイバー脅威から保護され、万全な準備態勢を維持できるように支援することです。M-Trends 年次レポートは、エンゲージメントから得たデータと知見を掲載し、そのミッションの進展に大きな役割を果たしています。今後も集団安全保障の意識、理解、機能を高めるべく、M-Trends を通して最前線の知識を紹介していきます。

文献情報

1. https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
2. https://cloud.google.com/blog/topics/threat-intelligence/separating-signal-noise-how-mandiant-intelligence-rates-vulnerabilities-intelligence
3. https://nvd.nist.gov/vuln/detail/CVE-2008-2463
4. https://nvd.nist.gov/vuln/detail/CVE-2017-0144
5. https://nvd.nist.gov/vuln/detail/CVE-2019-18935
6. https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation
7. https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023
8. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/
9. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware
10. https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing
11. https://cloud.google.com/blog/ja/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation
12. https://cloud.google.com/blog/ja/topics/threat-intelligence/how-mandiant-tracks-uncategorized-threat-actors
13. https://cloud.google.com/blog/ja/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage
14. https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
15. https://www.justice.gov/usao-nj/pr/russian-national-charged-conspiring-commit-lockbit-ransomware-attacks-against-us-and
16. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
17. https://cloud.google.com/blog/products/identity-security/attacker-visibility-threat-campaigns
18. https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
19. https://www.progress.com/security/MOVEit-transfer-and-MOVEit-cloud-vulnerability
20. https://cloud.google.com/blog/ja/products/identity-security/cloud-ciso-perspectives-late-june-2023
21. https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
22. https://cloud.google.com/blog/ja/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation
23. https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
24. https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook
25. https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
26. https://services.google.com/fh/files/misc/barracuda-esg-rpt-en.pdf
27. https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
28. https://cloud.google.com/blog/ja/topics/threat-intelligence/barracuda-esg-exploited-globally
29. https://cloud.google.com/blog/topics/threat-intelligence/putting-model-work-enabling-defenders-vulnerability-intelligence-intelligence-vulnerability-management-part-four
30. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
31. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware
32. https://cloud.google.com/blog/topics/threat-intelligence/sim-swapping-abuse-azure-serial

33. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware
34. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware
35. https://blog.google/technology/safety-security/googles-ai-red-team-the-ethical-hackers-making-ai-safer/
36. https://cloud.google.com/blog/ja/topics/healthcare-life-sciences/introducing-medlm-for-the-healthcare-industry
37. https://cloud.google.com/blog/ja/products/ai-machine-learning/gemini-for-google-cloud-is-here
38. https://cloud.google.com/blog/ja/topics/threat-intelligence/threat-actors-generative-ai-limited