2014

CISCO

TALOS

一年の総括

2024 一年の総括

cisco TALOS

目次

2024 一年の総括

はじめに

2024 年、攻撃者はステルス性、シンプルさ、効率性を優先して、カスタムマルウェアやゼロデイ脆弱性の利用をほぼ放棄し、より単純ながらも効果の高い手法を好んで用いました。このような状況は、セキュリティの基本を優先することが、組織にとってこれまで以上に重要であることを明確に示しています。

アイデンティティは、2024 年の変わることのないテーマであり、攻撃者は、ユーザー固有のデジタルフットプリントを侵害し、自分たちの悪意ある目的のために利用する方法を探していました。狙われたのは、ログイン情報、セッション ID、API キー、デジタル証明書などの識別子などです。アイデンティティベースの攻撃は圧倒的に多く、Cisco Talos インシデント対応チーム（Talos IR）が扱った全事例の 60% を占めています。攻撃者は攻撃の主要な段階（初期侵害、ラテラルムーブメント、特権昇格など）でこの手法を用いていました。防止が難しく検出はさらに困難なアイデンティティベースの攻撃が非常に効果的であることが、2024 年に証明されました。侵害された有効なアカウントを使用し、検出可能なマルウェアの使用を避けることで、攻撃者は長期間見つかることなく潜伏できます。時には、ネットワーク全体に自由にアクセスすることもありました。

「容易なアクセス」もまた主要なテーマでした。最も狙われた脆弱性として数十年前の CVE が上位にランクインし、システムの設定ミス、MFA の弱点、パッチ未適用のシステムなどのセキュリティ問題が Talos IR が扱った事例の半数を超えました。ランサムウェア攻撃グループは、特にこの点に着目し、Talos が対応したインシデントのほとんどで、不適切に設定されたセキュリティソリューションの無効化を試み、ほぼ 50% の確率で成功しています。驚くことではありませんが、最も標的にされた業種は教育と医療でした。攻撃者は、サイバー予算が少なく、事務官僚的に対処する傾向があるせいで、こうした脅威を防ぐために迅速かつ機敏に対応し続けることが困難な組織への侵害を続けています。

ネットワークを支えるシステムに対する脅威は続いており、組織は将来を見据えて引き続きセキュリティの基本を優先し、重大なリスクをもたらすインフラストラクチャの老朽化に対処する必要があります。

高度な攻撃者は、脆弱なネットワークハードウェア、外部公開されたアプリケーション、クラウドアプリケーションを利用します。これらはすべて、セキュリティの観点から見落としてはならないネットワーク環境への侵入ポイントです。さらに、この分野での攻撃がアイデンティティベースの手法にますます依存するようになったため、組織がセキュリティの基本を守ることがこれまで以上に重要になっています。こうした攻撃の多くは、多要素認証の導入と設定を適切に行ってソーシャルエンジニアリングのフィッシングの罠を検出し、ネットワーク上の正規のアカウントから行われる異常なアクティビティを特定すれば防げるからです。

人工知能（AI）の分野において、攻撃者が AI と機械学習（ML）を使用する状況は、2024 年の業界の予測を大幅に下回っています。攻撃者は、新しい攻撃手法を編み出すためではなく、自らの手法を強化するためにこれらのテクノロジーに頼っていました。攻撃者は、大規模言語モデル（LLM）などの生成 AI ツールを使用して、説得力のあるソーシャルエンジニアリング手法を編み出し、悪意のあるアクティビティを自動化します。2025 年には、生成 AI ツールの利用が拡大すると予想されます。おそらく、攻撃者はこのテクノロジーを活用し、AI モデル、システム、インフラストラクチャを侵害できる機能を作り出すでしょう。

シスコは *4,600 万* 台を超えるデバイスからテレメトリを受信し処理しており

それらのデバイスは世界中の *193* の国と地域に展開されていて

1 日あたりに発生するセキュリティイベントは *8,860 億*件を超えています。

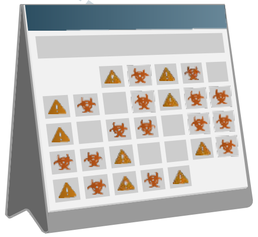


図 1

シスコのグローバルな可視性

シスコは、グローバルに事業を展開しネットワークインフラ分野で主要な役割を担っているため、持続的に展開される今日の新たな脅威の多くについて素晴らしいインサイトを得ることができます。本レポートの調査結果は、何百人もの脅威ハンター、マルウェアの専門家、検出のスペシャリスト、データモデリングの専門家、インシデント対応チームの担当者による共同調査から得たものです。シスコは、世界中の 193 の国と地域にまたがる 4,600 万を超えるデバイスからテレメトリを受信し処理しており、1 日あたりに発生するセキュリティイベントの数は 8,860 億件を超えています。2024 年 1 月 1 日から 2024 年 12 月 31 日までを対象とした Talos の『一年の総括』では、これらのデータと専門知識すべてを活用し、分析結果をお届けします。

2024

一年の総括

狙われることが多かった脆弱性

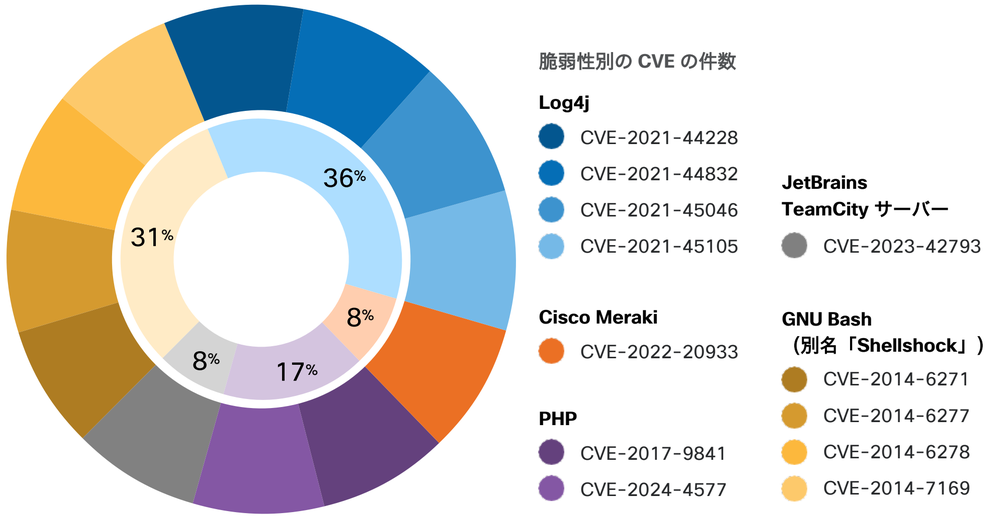
2024 年、攻撃者は広く利用されてきた既知の CVE に注目

2024 年に最も狙われた脆弱性のほとんどは、数年前に公開されていた比較的古い CVE でした。特に注目すべき点として、リストに挙がっている上位 12 件の CVE のうち 4 件は 10 年前に公開されたものであり、悪名高い Log4j の脆弱性（2021 年初めに公開）も含まれています。これは、攻撃者がパッチの適用されていないシステムを頻繁に標的としていることを明確に示しており、組織がセキュリティ更新プログラムの適用を怠った場合、本来防げるはずの多くの攻撃にさらされてしまいます。

Apache Log4j ロギングライブラリに対するエクスプロイトの試みは、脆弱性が発見されて 4 年近くたった今も、依然として多く見られます。Log4j は、世界中で最も広く使用されているオープンソースプログラムの 1 つです。「Log4Shell」と総称されるこれらの脆弱性には、発見後すぐにパッチが適用されましたが、Log4j はソフトウェア サプライチェーンに非常に深く組み込まれているため、組織にとって長期的なリスクとなる可能性があります。米国国土安全保障省は、すべての脆弱なインスタンスを見つけて修正するには、少なくとも 10 年はかかると予測しています。

これに関連して、リストに挙がっている脆弱性はすべて、広く使用されているソフトウェアやハードウェアに影響するため、攻撃者が幅広い業界や地域に侵入するために悪用できる非常に広範な攻撃対象領域を生み出しています。たとえば CVE-2017-9841 と CVE-2024-4577 は、一般的なプログラミング言語である PHP に影響を与えます。推定 では、Facebook や Wikipedia のような人気サイトや、Etsy や Shopify などの e コマースプラットフォームなど、世界の 20 億の Web サイトのうち 75 ～ 80% が PHP を利用しています。これらの Web サイトの基盤となるコードの脆弱性が原因で、攻撃者による不正アクセスが可能になり、大規模なデータ侵害につながる場合もあります。2024 年 1 月、CISA と FBI は、攻撃者が CVE-2017-9841 を悪用して Androxgh0st を展開しているというアドバイザリ 警告を公開しました。Androxgh0st は

図 2
2024 年に狙われることが多かった脆弱性



ボットネットを構築する機能で知られるマルウェアです。ボットネット構築後は、脆弱なネットワークをさらに特定して侵害できるようになります。

もう 1 つの一般的なスクリプト言語である Bash も重点的に狙われており、関連する 4 件の脆弱性が、最も頻繁に標的にされた CVE のリストに挙がっています。Bash は、多くの Linux/UNIX システムや古い MacOS バージョンで使用される一般的なコマンドラインシェルです。これら 10 年前の脆弱性は「Shellshock」 と総称されており、2014 年に世界的なセキュリティ危機を引き起こした悪名高い Heartbleed のバグ（CVE-2014-0160）に匹敵する問題 です。

前述のように、狙われることが多かった脆弱性はすべて、世界中のシステムで広く使用されているソフトウェアやハードウェアに影響するため、広範な攻撃対象領域を生み出しています。どのような攻撃グループがこれらの CVE をエクスプロイトしているかが明らかになることで、システムの脆弱性を抱える組織が直面しているリスクへの懸念が高まっています。たとえばさまざまな高度な攻撃グループが CVE-2023-42793（JetBrains の TeamCity サーバーに影響）を攻撃に利用していることが報告されています。具体的には、ロシア政府が支援する脅威グループ APT29（別名 CozyBear）や、北朝鮮政府が支援する複数のグループ、そしてランサムウェア集団 BianLian などです。

今なお続く Shellshock の影響

Shellshock の脆弱性は、Linux や macOS のような広く使用されているオペレーティングシステムに搭載されている Bash スクリプト言語に影響を与えるものであり、2014 年に発見されてから 10 年以上経過した今も問題となり続けています。Bash は、世界中のアプリケーションやシステムプロセスに緊密に統合されています。さらに、多くの Web サーバー、ルータ、IoT（Internet of Things）デバイスは Bash を使用してコマンドを実行しています。つまり、インターネットに接続されている脆弱なデバイスが攻撃対象になる可能性があるということです。これらのハードウェアコンポーネントは、特に産業（工業）部門や重要インフラ部門の環境では、更新頻度が低かったり、パッチの適用が困難だったりすることがよくあります。

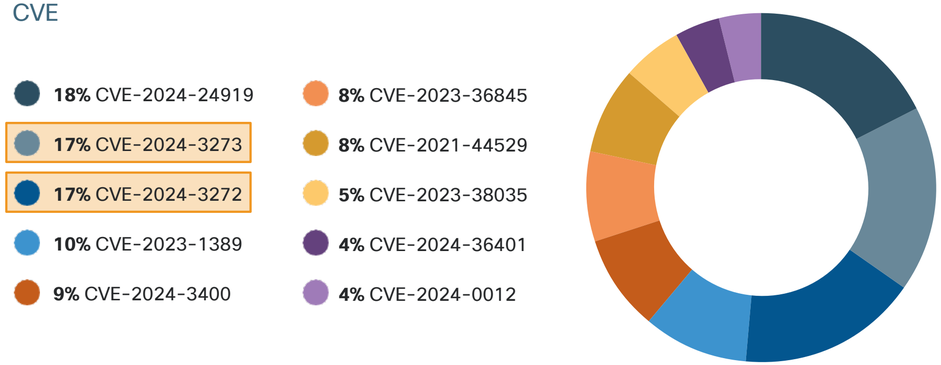
Shellshock の直接的な影響は、他の重大な侵害やサイバー攻撃ほど壊滅的なものではなかったかもしれませんが、それでも依然として継続的な問題となっています。たとえば Talos は 2019 年に、国家が支援する「Sea Turtle」という世界的なスパイ活動を発見しました。この攻撃では、DNS レコードを操作して機密システムにアクセスしていました。攻撃者は、Shellshock を含む複数の脆弱性を悪用して初期アクセスを確立しました。

国家支援のサイバー攻撃者が Shellshock を狙った事例（公に確認されたもの）は限られていますが、他の高度な攻撃者が Shellshock を悪用しようとした可能性は非常に高いと言えます。ロシア政府の支援を受けたグループである APT28 や北朝鮮政府の支援を受けた Lazarus Group など、多くの有名な攻撃グループが広く使用されているソフトウェアの重大な脆弱性を悪用しており、こうしたグループによる広範なスパイ活動やマルウェア攻撃で Shellshock が使用されている可能性があります。

狙われることが多かった脆弱性

図 3

狙われることが多かったネットワークデバイスの CVE



EOL デバイスに影響を与える脆弱性が、最も狙われたネットワークデバイスの CVE の 1 つ

攻撃者が、どのようなタイプのデバイスを攻撃で優先するかを確認するために、特に狙われたネットワークデバイスの脆弱性についても確認しました。このリストには、2023 年または 2024 年に CISA の「既知の悪用された脆弱性（KEV）」カタログに追加されたネットワークデバイスの脆弱性のみが含まれています。このうち 3 件（Check Point VPN ゼロデイ脆弱性である CVE-2024-24919 と、古い D-Link ハードウェアに影響を及ぼす CVE-2024-3273 および CVE-2024-3272）が、分析したデータセットにおける、特に狙われたネットワークデバイスの脆弱性の 50% 超を占めました（図 3 を参照）。

これらの脆弱性の多くは主に、Mirai や Gafgyt など既知のボットネットによってエクスプロイトされています。ボットネットを使用すると、侵害したデバイスの制御を確立し、コマンドを送って分散型サービス拒否（DDoS）攻撃などの悪意のあるアクティビティを実行させることができます。ルータやファイアウォールなどのネットワークデバイスはアクセスを許可しているため、攻撃者はそれらを侵害することで、簡単に横方向に移動して攻撃の他のフェーズを実行できるようになり、ネットワーク全体を乗っ取る可能性があります。ネットワークデバイスの脆弱性の少なくとも 1 件（CVE-2023-38035）は、ランサムウェアの攻撃者によってエクスプロイトされています。

特に注目すべき点として、最も狙われた脆弱性の中には、すでにサポートが終了した（EOL）デバイスに影響を及ぼすものもあります。EOL なので、今も攻撃者に積極的に狙われているにもかかわらず、パッチは提供されていません。たとえば CVE-2024-3273 と CVE-2024-3272（いずれも D-Link NAS デバイスの脆弱性）は、最も狙われたネットワークデバイスの脆弱性リストで 2 位と 3 位にランクインしました。この結果は、組織のネットワークの EOL コンポーネントをできるだけ早く廃止し、リプレースすることの重要性を浮き彫りにしています。

図 4

最も狙われたネットワークデバイスの脆弱性トップ 10

EOL 製品

CVE	製造元	製品	デバイスタイプ	脆弱性の説明
CVE-2024-24919	Check Point	Quantam セキュリティゲートウェイ	ファイアウォール/VPN	パスワードハッシュなどの機密データを読み取ることができます。
CVE-2024-3273	D-Link	複数の NAS デバイス	ネットワーク接続型ストレージ（NAS）	デバイス上で、base64 エンコードされた任意のコマンドを実行できる脆弱性です。
CVE-2024-3272	D-Link	複数の NAS デバイス	ネットワーク接続型ストレージ（NAS）	デバイス上で、base64 エンコードされた任意のコマンドを実行できる脆弱性です。
CVE-2023-1389	TP-Link	Archer AX21	ルータ	単純な POST リクエストにより、root として実行されるコマンドを挿入できます。
CVE-2024-3400	Palo Alto Networks	PAN-OS	ファイアウォール	ファイアウォール上でルート権限を使用してコマンドを実行できるようになります。
CVE-2023-36845	Juniper	Junos OS	ネットワーク デバイス ソフトウェア	悪意のあるコードを挿入して実行できます。
CVE-2021-44529	Ivanti	Endpoint Manager クラウド サービス アプライアンス	エンドポイント デバイス マネージャ	限定された権限で悪意のあるコードを実行できるようになります。
CVE-2023-38035	Ivanti	Ivanti Sentry	セキュリティゲートウェイ	API の機密データや設定にアクセスしたり、システムコマンドを実行したり、システムにファイルを書き込んだりできるようになります。
CVE-2024-36401	OSGeo	GeoServer	サーバー	細工された入力を使用してリモートでコードを実行できます。
CVE-2024-0012	Palo Alto Networks	PAN-OS	ファイアウォール	管理者権限を取得できるようになります。

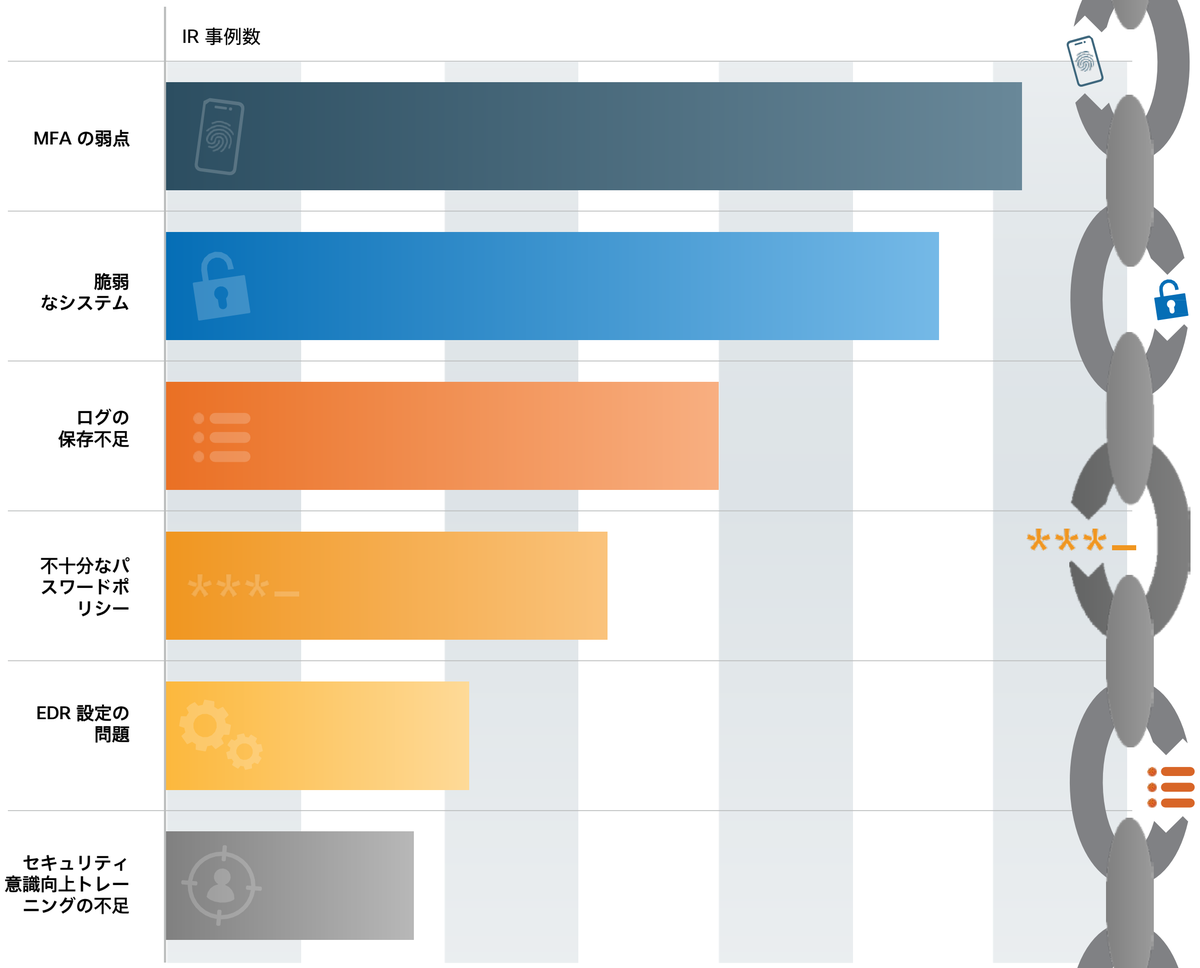
狙われることが多かった脆弱性

よく狙われた脆弱性のほとんどが何年も前から存在していることは驚きではありません。というのも、パッチ管理は組織にとって以前から問題となっているからです。Talos IR のデータによると、2024 年に確認されたセキュリティの弱点の中で 2 番目に多く見られたのが、パッチが適用されていない脆弱なシステムでした（図 5 を参照）。

スモールオフィス・ホームオフィス（SOHO）デバイスは攻撃の対象になりやすいと報告されています。その理由はおそらく、セキュリティの面で不十分である可能性があるからですが、攻撃を行う際に、攻撃者がデバイスの規模に強くこだわることはありませんでした。実際、攻撃対象を選ぶパターンは、小規模デバイス（50 ユーザー未満）、中規模デバイス（51 ～ 499 ユーザー）、大規模デバイス（500 ユーザー以上）で驚くほど類似していました。これは、攻撃者が機会をうかがっており、デバイスのユーザー数を優先していないことを示しています。

図 5

Talos IR の対応事例における主なセキュリティの弱点



特に注目すべき点として、最も狙われた脆弱性の中には、*EOL* デバイスに影響を及ぼすものもあります。*EOL* なので、今も攻撃者に積極的に狙われているにもかかわらず、パッチは提供されていません。

Talos が提案する、ネットワークデバイスを保護するための 10 のヒント

1. デバイスの更新は可能な限り積極的に行います。これには、既知の脆弱性に対するパッチを現在使用しているハードウェアとソフトウェアに適用することや、EOL ハードウェアおよびソフトウェアをリプレースすることが含まれます。
2. 堅牢な認証方式を導入します。多要素認証を使用して複雑なパスワードとコミュニティストリングを選択し、デフォルトのログイン情報の使用は避けます。
3. セキュリティのベストプラクティス（定期的なアップデートの実施、アクセス制御の管理、ユーザー教育の実施、ネットワーク セグメンテーションの適用など）を遵守します。
4. 監視と設定に関わるすべてのトラフィック（SNMPv3、HTTPS、SSH、NETCONF、RESTCONF など）を暗号化します。
5. 米国政府や業界が提供するセキュリティアドバイザリの最新情報を入手します。これらのレポートで検出された問題を軽減するために、推奨されている設定変更を検討します。
6. 認証システム（TACACS+ やジャンプホストなど）をロックダウンし、積極的にモニタリングします。
7. 設定は一元的に保存し、デバイスにプッシュします。
   デバイスを、そのデバイスの設定に関する信頼できる情報源として扱わないようにします。
8. 認証、許可、およびアカウンティング（AAA）を使用して主要なデバイス保護の設定変更を拒否します（ローカルアカウント、TACACS+、RADIUS など）。
9. 動作や設定に異常な変更がないか環境をモニタリングします。
   SNMP、SSH、HTTP(S) など、管理インターフェイスや異常なインターフェイスの露出に注意し、異常なアクティビティがないか syslog や AAA を監視します。
10. デバイスのベースラインをプロファイルして変更を特定します。NetFlow とポートスキャンを使用してネットワークデバイスのフィンガープリントを取得して、攻撃対象領域の変化（新しいポートの開閉や、送受信されるトラフィックなど）を確認します。可能であれば NetFlow の可視性を高め、異常なデータ量の変化を特定します。

関連資料

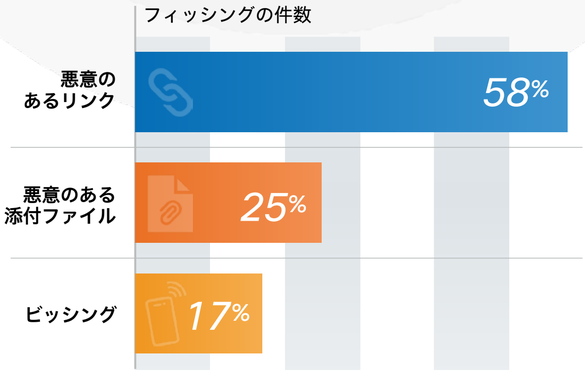
- Salt Typhoon の攻撃活動に関する Talos のブログでは、この高度な攻撃者がネットワークインフラを標的にするために用いる戦術、手法、手順（TTP）について詳しく説明しているほか、検出と予防のガイダンスも掲載しています。
- Talos はまた、通信インフラを強化するためのこちらのガイド について、CISA およびその他のパートナーと連携しました。
- 最後に 2023 年のブログ では、国家が支援する攻撃グループによるネットワークインフラへの高度な攻撃の詳細について、攻撃チェーンの情報と実用的なセキュリティの推奨事項を紹介しています。

2024
一年の総括

電子メールによる脅威

図 6

Talos IR の事例で確認されたフィッシングの種類



有名ブランドになりすましたフィッシングの罠

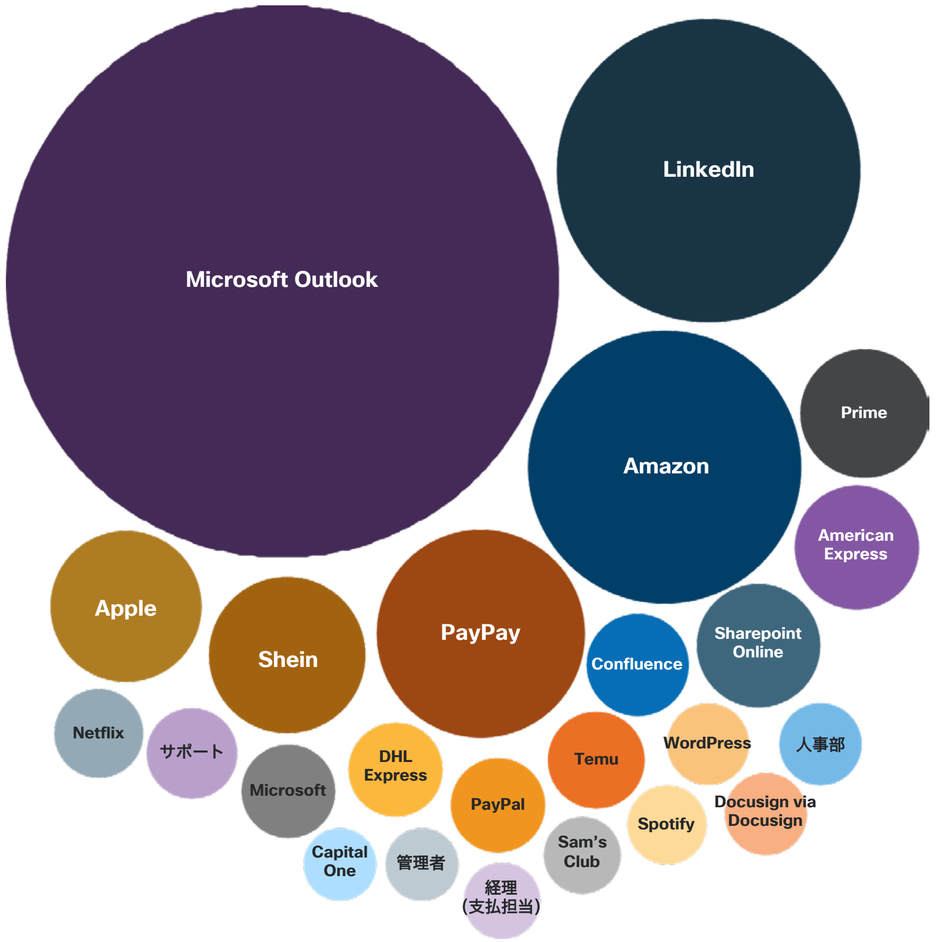
フィッシングが相変わらず主要な侵害の手段である理由は、匿名で簡単に大量のメールを送信し、被害者に接触できるからです。Talos IR が確認したインシデントの約 4 分の 1 で、攻撃者はフィッシングによって初期アクセスを取得していました。これらの事例では、悪意のあるリンクを埋め込む手法のほうが、メールの添付ファイルや音声フィッシング（ビッシング）などの他のフィッシング手法よりも成功率が高かったようです。この分野ではソーシャルエンジニアリングが特徴的ですが、人工知能（AI）ツールの活用によって、攻撃者は標的に合わせて細工された信憑性の高い罠をより簡単に作成できるようになりました。

Talos は電子メールのテレメトリを分析し、ソーシャルエンジニアリングに主に使用されているブランドや傾向を特定しました。図 7 に示しているのは、ブロックされた電子メールの送信者の表示名として最もよく使用されていたブランドです。調査結果から、被害者を騙してフィッシングの罠に引っかけるために、攻撃者がどのような種類の企業になりすまそうとしているのかを推測できます。

最も頻繁になりすましの対象にされたのは Microsoft Outlook であり、ブロックされたメールの 25% で送信者の名前として使用されていました。Amazon や Apple といった大手テック企業も、高い頻度でなりすましの対象になっていました。その他、リストの上位に挙がっている名前には、人気のオンライン決済サービス、国際的な小売企業、一般的な企業向けコラボレーション アプリケーションなどがあります。これらが世界的に広く知られている企業であることを考えると、攻撃者が好んで採用するのは当然と言えます。ブランドの認知度が高いと、信頼度も高くなり、クリック率も高くなると考えられるからです。

図 7

送信者名でなりすましの対象にされた上位のブランド



フィッシングメールで単純な件名を使う一方、重要なイベントには便乗

攻撃者は、正当で信頼できる送信者からメールが送信されたように見せかけるだけでなく、メールの件名も工夫し、被害者を巧妙に騙してメールを開かせるようにします。図 8 に示しているのは、ブロックされたメールの件名に使用された最も一般的な語句です。ここに示しているように、日常的に受信トレイで目にするような、ごくありふれた一般的な語句でした。攻撃者が緊急や至急といった件名を詐欺メールで使用することはほとんどありません。代わりに、あまり目立たず、無害なメッセージだと思いかねない語句を使用します。

年間を通して、メールの件名に最も多く使用されたのは一般的な語句でしたが、攻撃者が重要な国家的イベントに便乗している証拠も確認しました。フィッシングの手口やスパムメールに素早くこれらのテーマを取り入れ、クリック率を高めています。この例を見ると、件名に「バイデン」「ハリス」「トランプ」が使用された頻度にばらつきがあることがわかります。その理由は、攻撃者が時事に合わせてメッセージの内容を変えたからです。これらの変化のいくつかは、2024 年の大統領選挙における主要なイベントと一致しています。たとえば前副大統領のハリス氏が出馬表明したときは「ハリス」を利用した詐欺メールが増加し、一方で「バイデン」を利用した詐欺メールは減少し始めました。選挙直後の数週間は「ハリス」を利用した詐欺メールが激減した一方、「トランプ」を利用した詐欺メールは一貫して多い状態が続きました。

図 8

悪意のあるメールの件名に使用されている一般的な語句

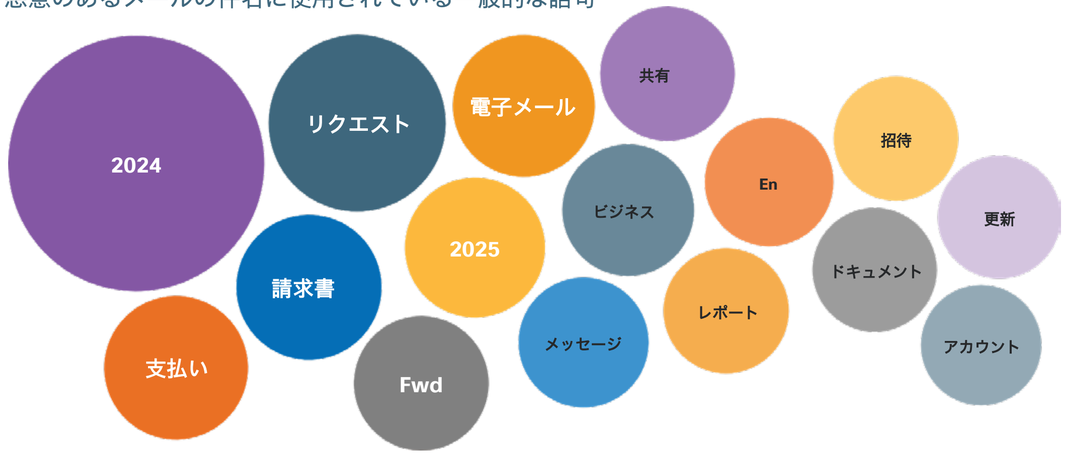
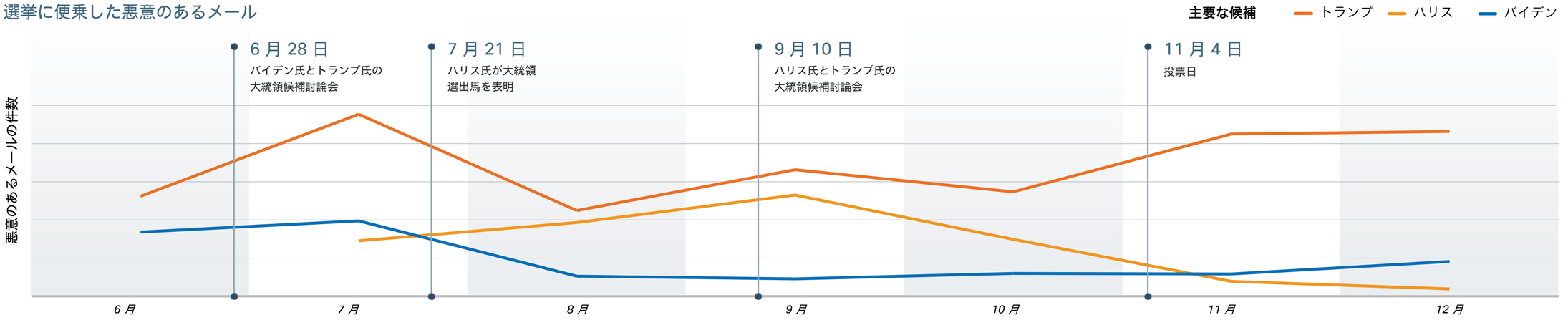


図 9

選挙に便乗した悪意のあるメール



2024
一年の総括

最も使用されたツール

通常のトラフィックに紛れ込ませることができる LoLBin を攻撃者が多用

Talos IR の対応事例でどのようなツールが使用されたか確認したところ、攻撃者は商用ツールやオープンソースツールよりも、環境寄生型バイナリ（LoLBin）、つまりエンドポイントに元々存在するツールやユーティリティを重用していました（図 11）。LoLBin は使用頻度こそ高かったものの、商用ツールやオープンソースツールの種類の多さに比べれば、その種類ははるかに少ないものでした（図 10）。その理由は、攻撃者が使用できる、標的のエンドポイントに元からある LoLBin の数はごく限られているからです。対照的に、商用ツールやオープンソースツールは増え続けており、攻撃者は独自のツールを継続的に開発または作成し、侵害したシステムに展開しています。

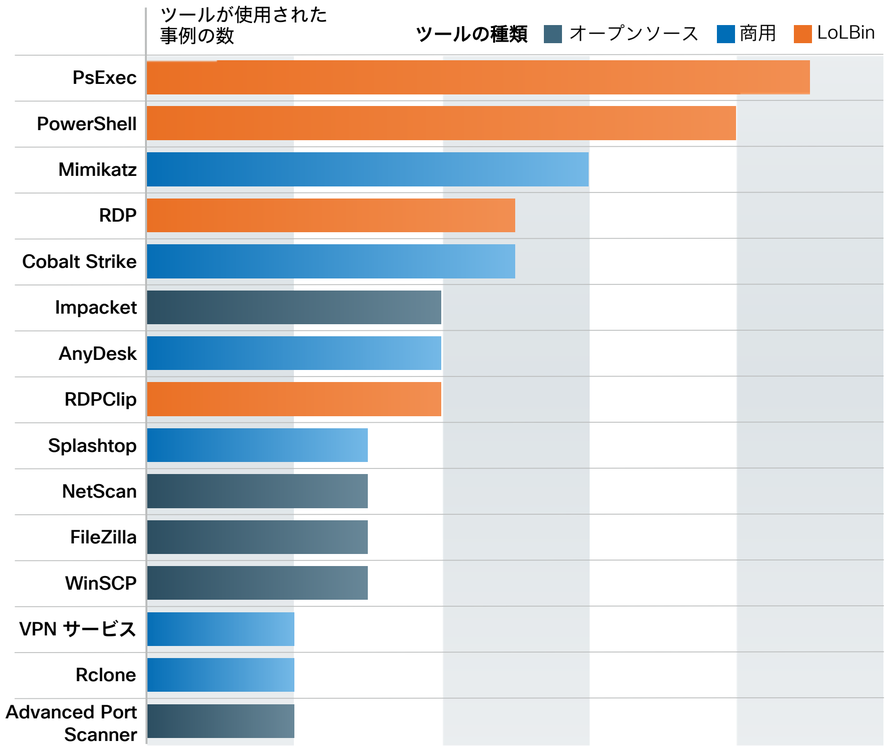
PsExec、PowerShell、Remote Desktop Protocol（RDP）などの一般的な LoLBin は、攻撃者の攻撃チェーンの大部分を円滑に進めるために使用された上位 5 つのツールのうちの 3 つです。たとえば Talos IR がランサムウェアのインシデントに対応した事例では、元々ネットワーク管理用に設計された PsExec を使用して悪意のあるバッチ（BAT）ファイルと最終的な Black Basta ランサムウェアバイナリが実行されており、一般的な LoLBin の悪用が及ぼす影響が明らかになっています。次ページの表に、PsExec などのよく使用されたツールと Mimikatz のような商用ツールのフレームワークの本来の使用目的と、攻撃者がこれらのツールを攻撃でどのように悪用しているかをまとめています。

図 10

Talos IR が対応したインシデントで確認されたツールの分類

図 11

Talos IR が対応したインシデントにおいて攻撃チェーン全体で使用された LoLBin



LoLBin を利用することで、攻撃者は通常のネットワークトラフィックに紛れて、ウイルス対策やエンドポイント検出ソリューションのトリガーを回避できます。さらに、これらのバイナリは、デフォルトの Windows ユーティリティとして Windows オペレーティングシステムにプリロードされているという性質上、通常の使用パターンを定義することが難しく、悪用を特定するための防御側の取り組みが複雑になっています。LoLBin は、攻撃の効率を高めるうえでも役立っていると考えられます。攻撃者が時間をかけて追加のソフトウェアをインストールしたり、外部のツールやエクスプロイトの有効性をテストしたりする必要がないからです。

Talos のインシデント対応業務で今年新たに確認されたオープンソースツールの 1 つが、DonPAPI です。複数の Windows コンピュータ上でのログイン情報のダンプをリモートで自動化するために使用されます。このツールは、Windows Data Protection API（DPAPI）で保護されたログイン情報を見つけて取得します（DPAPI ダンプとも呼ばれます）。アイデンティティの観点から見ると、DonPAPI のようなオープンソースツールは、GitHub などのコードリポジトリで広く公開されていて、インストールも簡単なので、組織に重大なリスクをもたらします。DonPAPI は、Wi-Fi キー、RDP パスワード、Web ブラウザに保存されているログイン情報など、特定のファイルの検索に使用されます。見つかった情報を使用すれば、認証とラテラルムーブメントを行って環境内の他のアセットを特定することができます。ランサムウェアグループは数年前から DonPAPI を使用していると報告されており、攻撃者はこの種のツールを使用してログイン情報を取得することに重点を置いていることがわかります。

組織は日常業務をサポートするためにこうしたツールの多くを定期的に使用しているため、エンドポイントでの使用や存在が悪意のあるものである可能性を見極めるのは難しい場合があります。次ページの表に、各カテゴリ（LoLBin（PsExec）、オープンソース（Impacket）、商用（Mimikatz））から、Talos IR の事例で最もよく確認されるツールの本来の使用目的と、攻撃者が悪意のある目的のためにどのように利用するかをまとめています。

アイデンティティの観点から見ると、*DonPAPI* のようなオープンソースツールは、*GitHub* などのコードリポジトリで広く公開されていて、インストールも簡単なので、組織に重大なリスクをもたらします。

Talos IR の事例における最も一般的なツールの使用と悪用

	PsExec	Impacket	Mimikatz
本来の使用目的	Microsoft 社の Sysinternals ツールスイートの一部で、ユーザーがローカルおよびリモートシステム上でコマンドを実行できるようにします。	オープンソースの Python ライブラリで、ネットワーク監査を行うために使用します。	クレデンシャルダンピング ユーティリティで、ペネトレーションテストの担当者やレッドチームがプレーンテキストのパスワードを抽出するためによく使用します。
悪意のある機能	他のシステムのプロセスをリモートで実行し、標的のシステムにリモートでアカウントを作成して、ネットワークで共有したファイルをダウンロードまたはアップロードする機能があります。	攻撃者は SecretsDump のような Impacket モジュールにより、Active Directory データベースからアカウントとパスワード情報を窃取できます。	LSASS メモリ、レジストリハイブ、DPAPI などから、ログインに関する情報を取得する機能を備えています。
攻撃者による悪用	多くのランサムウェア攻撃では、PsExec を使用してドメイン内のすべてのシステムでペイロードを実行します。	APT や他の攻撃者は Impacket を頻繁に使用し、被害者の環境で最初のアクセスを確保してラテラルムーブメントを行います。	サイバー犯罪者や APT グループは Mimikatz を使用してアカウントのログイン情報や認証情報を窃取することによって、被害者の環境でラテラルムーブメントを行えるようにします。

2024
一年の総括

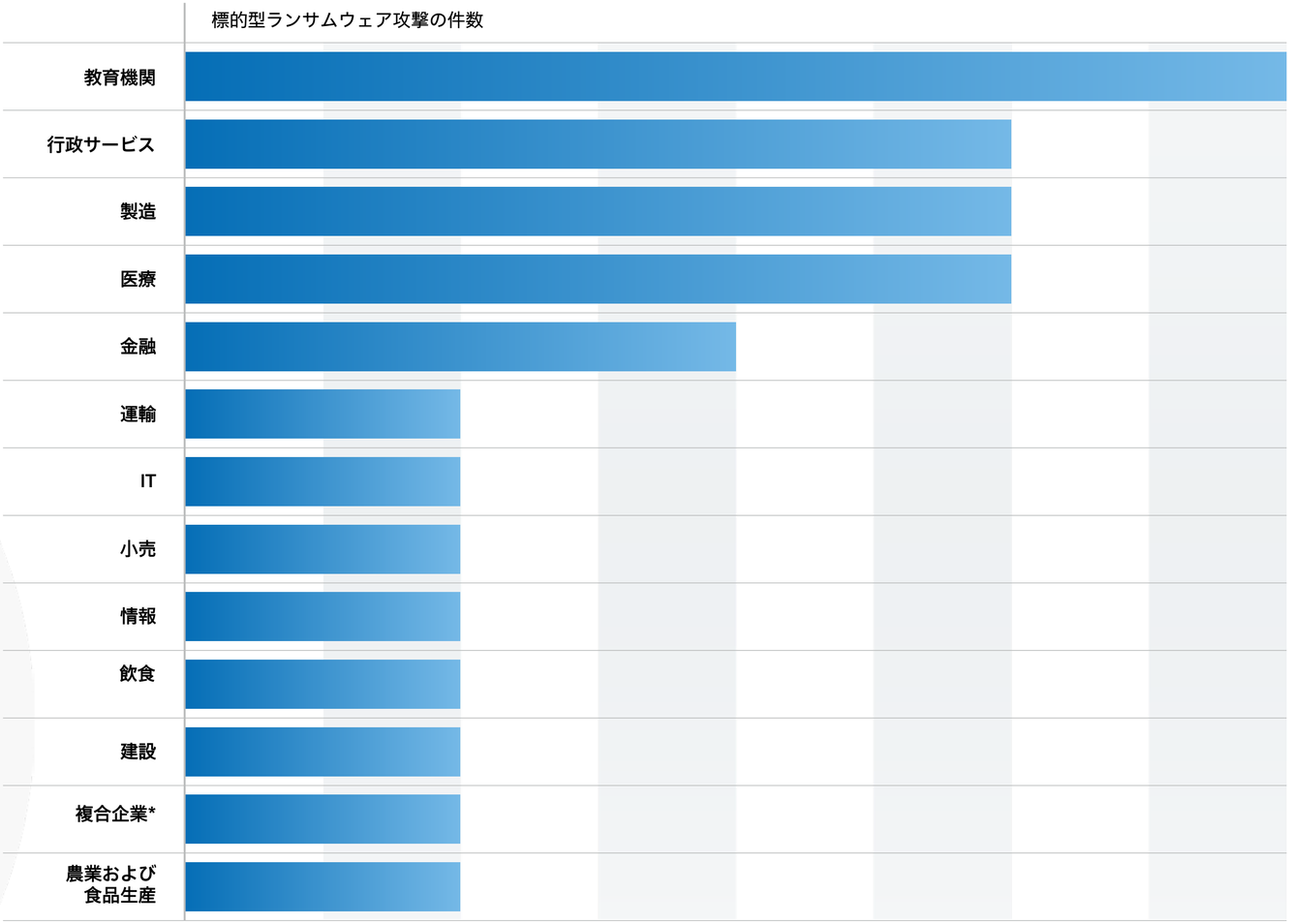
ランサムウェア

2024 年に最も標的にされたのは高等教育機関

2024 年に、他のどの業界よりもランサムウェア攻撃グループの標的となったのが教育機関です。この傾向は過去数年間変わっておらず、2022 年は教育機関が最も狙われ、2023 年には 2 番目に標的とされました。行政機関、製造業、医療機関に対するランサムウェア攻撃も多発しており、ダウンタイムの許容度が従来から低く、セキュリティ予算が限られている大規模な組織をランサムウェア攻撃グループが集中的に攻撃していることがうかがえます（図 12 を参照）。

興味深いことに、教育業界に対するランサムウェア攻撃のほぼすべてが、高等教育機関を標的としていました。大学のサイバーセキュリティ予算は通常、小学校や中等教育学校に比べて大きく、おそらく十分に保護されていると考えられます。ただし、独自の研究や政府の資金提供を受けた研究など、大学が保管するデータは価値が高く、ランサムウェア攻撃の対象になりやすい傾向があります。また大学は、オンライン授業や学生の研究など、IT インフラへの依存度も高いため、運用の中断を最小限に抑えたいというインセンティブが働きます。

図 12
標的となった業界



*複合企業組織とその子会社は、他の業種には含まれません。

教育業界が格好の標的にされる理由

資金不足

特に小学校、中学校、高校では、適切な情報セキュリティ機能のための資金が不足していることが多く、攻撃者が最大の損害を与えることができるのに対し、被害者は迅速に回復できる能力が最小限に抑えられています。

不定期な監視

効果的なサイバーセキュリティというと、多くの場合、24 時間 365 日体制で脅威を監視し、対応する能力が求められます。学校では、授業時間外や週末、休暇中にそのためのリソースを確保できない場合があります。

最小限のネットワークセグメンテーション

多くの大学では、学生用ネットワーク、研究用ネットワーク、事務管理用ネットワークの間でネットワーク セグメンテーションが最小限のため攻撃対象領域が広く、攻撃者がラテラルムーブメントを行いやすくなっています。

価値のあるデータを保有

学校、特に大学は、金融口座情報、個人を特定できる情報（PII）、機密研究データなど、ランサムウェア攻撃グループが関心を持つさまざまなデータを保有しています。

デバイス状態チェックが不十分

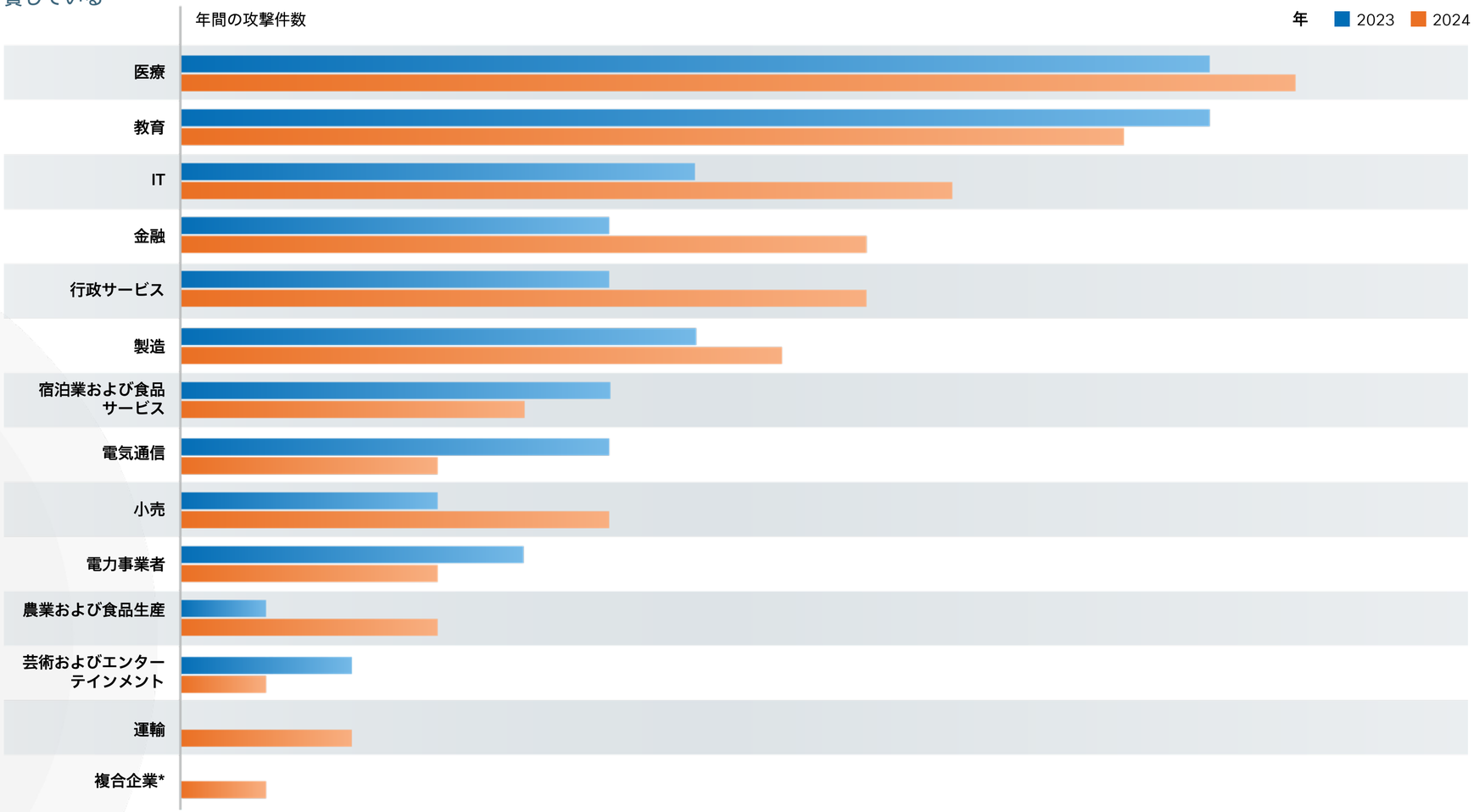
学生はサイバーセキュリティのトレーニングを受けていないことが多く、学校のネットワークセキュリティにあまり関心がないため、個人用デバイスのセキュリティレベルが低くなっています。このようなセキュリティが不十分な環境は、簡単な標的を侵害することで学校のネットワークにアクセスしようとする攻撃者にとって、手っ取り早い攻撃ポイントを数多く生み出します。

ランサムウェア

ランサムウェアの標的傾向と、より広範な Talos のデータセットにおける標的傾向はある程度似ており、いずれの場合も、医療と行政サービス（地方自治体）が最も狙われた業種のトップ 5 に入っています。興味深いことに、2023 年と 2024 年では標的となる業界に大きな変化はなく、攻撃者がよく狙う業種はほぼ一貫していることがわかります（図 13 を参照）。

図 13

2023 年と 2024 年のインシデント対応データにおいて、ランサムウェアの影響を最も受けた業種と、より広範なデータセットにおける最も影響を受けた業種は一貫している



*複合企業組織とその子会社は、他の業種には含まれません。

ランサムウェア攻撃は春と夏に増加

Talos IR の調査結果によると、ランサムウェア攻撃は春と夏に、平均して活発になる傾向が見られました（図 14 を参照）。学校が休みに入る時期や、休暇を取る職員や学生が増えてくる時期と重なるため、サイバーインシデントへの対応が遅くなったり、サイバーセキュリティ態勢が全体的に緩くなったりすることが要因と考えられます。教育機関は、夏休みの間は縮小運営していることが多く、学校のカレンダーがオンラインで公開されていることも珍しくありません。つまり、攻撃者も参照できるということです。

Talos IR の事例で、担当者が「オフィス外」にいる状況が悪用されたことがありました。たとえば、LockBit ランサムウェア攻撃者が休暇中の職員の IT アカウントを乗っ取った事例などです。攻撃者は簡単にアクセス権を獲得し、ドメイン全体への管理者権限を持つ別のアカウントを作成してラテラルムーブメントを行いやすくしました。

攻撃者は多くの場合、攻撃の初期段階でセキュリティソリューションを無効にすることを優先

ランサムウェア攻撃グループは、Talos IR が確認した事例のほとんどで標的のセキュリティソリューションを無効化しようとし、ほぼ確実に成功していました（図 15 を参照）。これは、侵害したネットワークにログインした際、攻撃者が最初に行うアクションの 1 つであることが多く、エージェントまたはコネクタにパスワードを設定する必要のないエンドポイント ソリューションや、適切に設定されていないエンドポイント ソリューションが狙われます。

攻撃者は、システム上でランサムウェアのような脅威の展開を検出して隔離するエンドポイントのセキュリティ製品を即座にアンインストールしました。また、攻撃者によるリモートアクセスを可能にする新しいファイアウォールルールを作成するなど、特定のソリューションに変更を加えたほか、シャドウコピーを削除し、システム、アプリケーション、セキュリティに関連するイベントログを消去して、攻撃の証拠を削除しました。これは、よく確認されるランサムウェアの TTP です。こうした行為は検出能力を大幅に低下させるだけでなく、システムの復旧を非常に困難にします。

これとは別に、適切に設定されていないセキュリティソリューションをランサムウェア攻撃グループが悪用する事例も確認しました。すぐに使用できるセキュリティ製品の多くは、ベースラインまたはデフォルトのポリシーが有効となっていますが、多くの場合、こうした製品は自社のネットワークのニーズに合った設定になっていません。そのため、セキュリティポリシーが「監査のみ」モードに設定されている環境でランサムウェア攻撃が成功した事例が多く確認されました。つまり、セキュリティ製品が悪意のあるアクティビティについて管理者に警告はしたものの、自動的にはブロックしなかったということです。

最初の侵害で生成されたアラートに続いて、特権昇格とラテラルムーブメントに関連する不審な動作に関するアラート、最後に悪意のあるペイロードの実行に関するアラートと、何度もアラートが発行されていましたが、ブロックや対応が行われたイベントは 1 つもありませんでした。ソリューションが受動的に導入されている場合、セキュリティチームがアラートを確認して実際の攻撃であるかどうかを検証し、対策を講じてリスクを緩和するのに、わずかな時間しか残されていません。

図 14

月ごとのランサムウェア攻撃件数

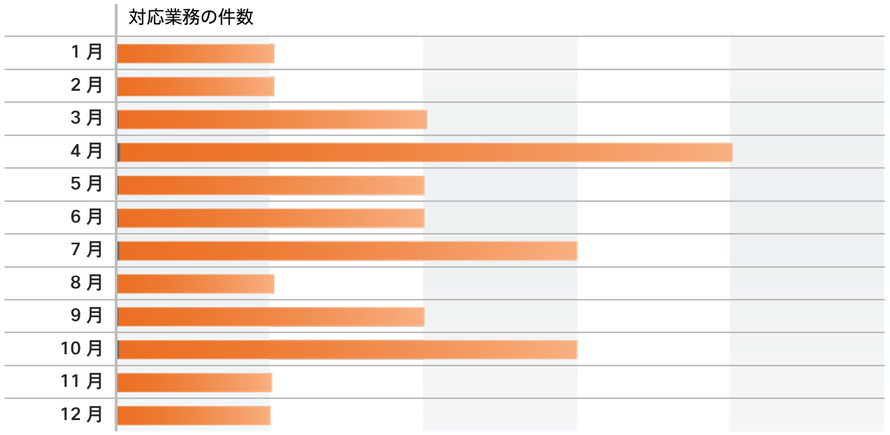
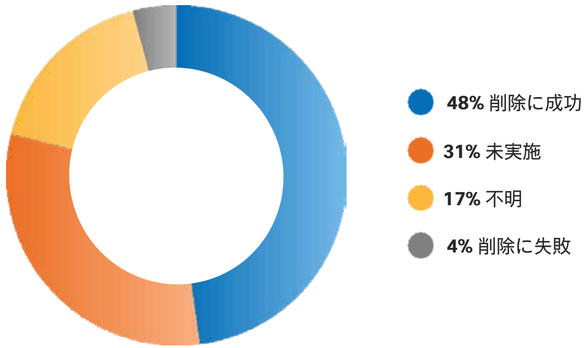


図 15

セキュリティソリューションの無効化



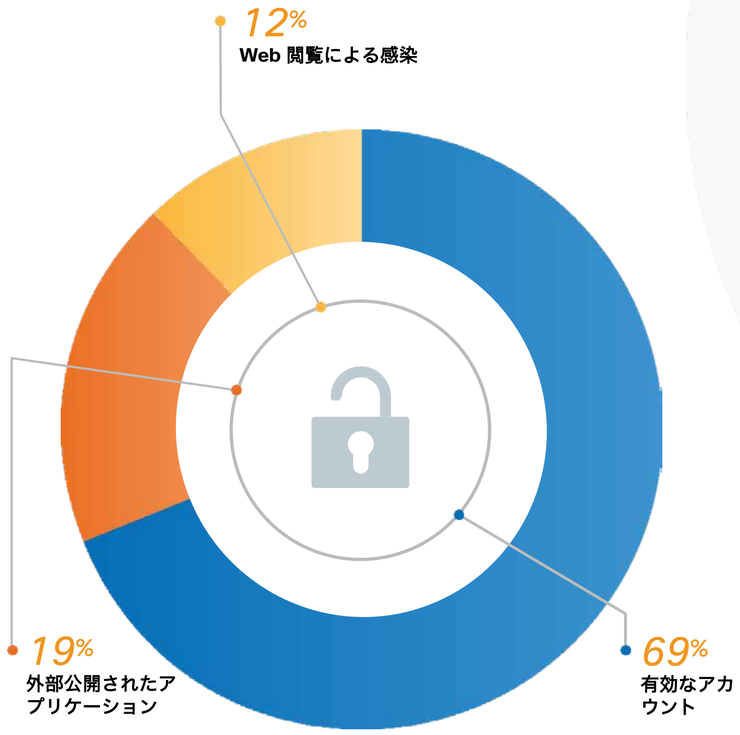
多くの組織は、エンドポイント保護機能を受動的に導入しています。つまり、エンドポイント保護製品はユーザーにアラートを送信していますが、悪意のあるアクティビティをブロックしていません。

初期アクセスは主に、有効なアカウントを介して取得

2024 年は、ランサムウェア攻撃グループが有効なアカウントを使用して初期アクセスを取得する事例が圧倒的に多かった年であり、関連する事例の約 70% でこの手口が確認されました（図 16 を参照）。このレポートの後半で概説するように、攻撃者は、脅威環境においてアイデンティティベースの攻撃を増やし、大きな成功を収めています。多くの場合、脆弱性のエクスプロイトやマルウェアの展開など複雑な手段を使うよりも、盗まれたログイン情報を使用して正規のユーザーアカウントにログインするだけのほうが、攻撃者にとってはるかに簡単で安全です。この手口がよく用いられる主な要因は、漏洩したログイン情報がダーク Web フォーラムで販売されていることであり、ランサムウェア攻撃グループは、標的とする組織に侵入するための鍵を実質的に購入できます。

ランサムウェア攻撃グループは全体の約 20% で、外部公開されたアプリケーションをエクスプロイトしていました。外部公開されたアプリケーションは企業の社内ユーザーだけでなく、インターネット上の誰もがアクセスできるため、非常に広大な攻撃ベクトルとなります。これには、オンライン ショッピング プラットフォーム、カスタマーログインポータル、ソーシャル メディアサイト、オンライン バンキング システム、メール サーバー、カスタマーサービスポータルなどをサポートするアプリケーションが含まれます。攻撃者は多くの場合、既知の脆弱性や設定不備を悪用してアクセスを取得します。通常、これらの攻撃にはより高い技術力が必要であり、攻撃者は SQL インジェクション、クロスサイト スクリプティング（XSS）、リモートコード実行などの手法を用います。有効なアカウントを侵害するという単純な手法と比べてこれらの攻撃の発生頻度が低い理由はそのためだと考えられます。

図 16
初期アクセス



初期アクセスを確立する手段として有効なアカウントが広く使用されていることから、ランサムウェアエコシステムにおける初期アクセスブローカー（*IAB*）の役割が浮き彫りになっています。漏洩したログイン情報は依然として価値の高い商品であり、これを利用して *IAB* はビジネスを続け、攻撃者は攻撃を合理化しています。

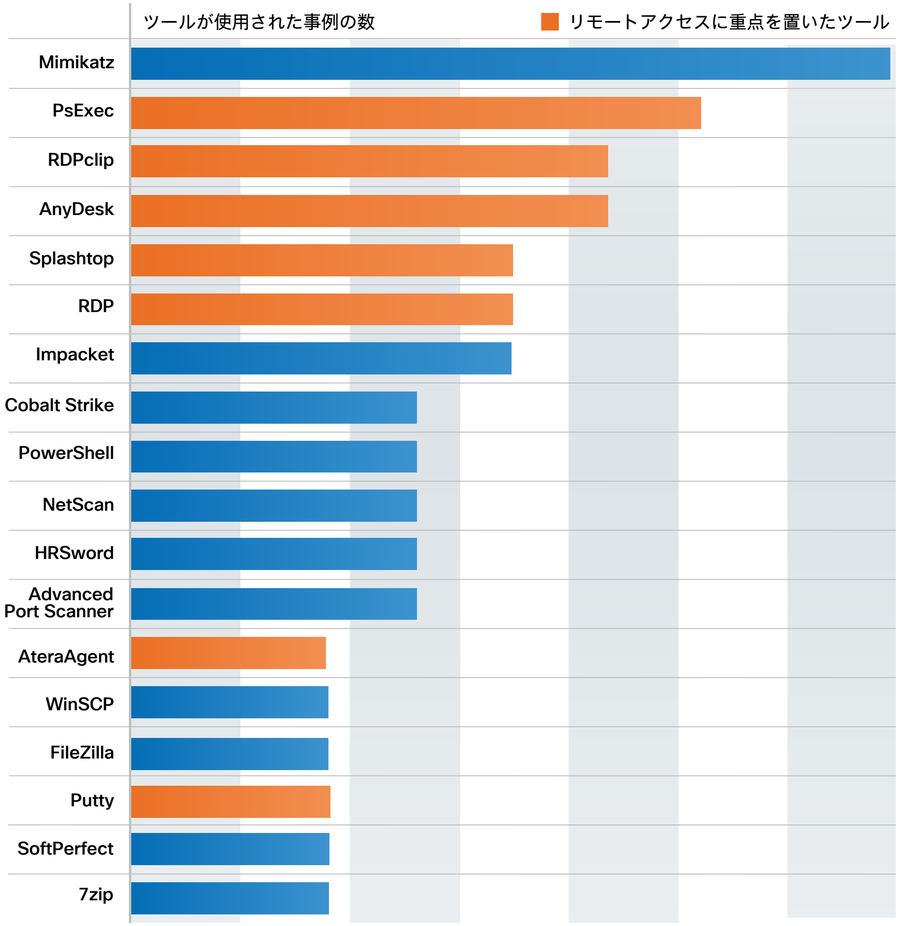
攻撃者はリモートアクセスツール、商用製品、LoLBinを多用

2024 年にランサムウェア攻撃者が最も頻繁に使用したツールを調査したところ、リモートアクセスに集中していること が確認されました（図 17 を参照）。具体的には、攻撃者はコマンドアンドコントロール（C2）において、商用製品と LoLBin を使用していました。多くの組織は、テレワークや IT ヘルプなどの日常業務で AnyDesk や Splashtop などの正規のリモートアクセス アプリケーションを使用しているため、こうしたツールが悪意のある目的で使用された場合の検出やブロックが難しくなっています。

無許可のリモート管理ツールすべてを効果的にブロックするのは難しいとしても、ポリシーや技術的な制御を通じてセキュリティを大幅に向上させることは可能です。使用を許可するリモートアクセス ソリューションを 1 つか 2 つに限定して導入し、それ以外はすべて禁止にするのは良い対策です。そうすれば、選択したソリューションをセキュリティチームが徹底的にテストし、可能な限り安全に展開できるからです。その他の対策（リモートアクセスツールに関連する DNS クエリの監査とブロック、リモートアクセス ソフトウェア インストーラに関連したハッシュのブロック、アプリケーションの許可リスト作成プログラムの利用など）もこの脅威を軽減するために利用できます。

図 17

Talos IR のランサムウェア対応業務で確認された上位のツール



ランサムウェア攻撃者が IT 担当者になりすまし、リモートアクセスを取得

2024 年 11 月以降、BlackBasta と Cactus ランサムウェアを配布する攻撃者が、ソーシャルエンジニアリングを駆使して標的のコンピュータへのリモートアクセスを取得する攻撃を開始したことを Talos IR は確認しています。

攻撃者はまず、被害者のメールボックスに大量のスパムメールを送信しました。その数日後に、通常は Microsoft Teams で被害者に電話をかけ、IT サポートを装ってスパムメール問題に関するサポートを申し出ています。標的となったユーザーは Microsoft Quick Assist のリモートアクセスセッションを開始するように促され、システムに Microsoft Quick Assist がインストールされていない場合はインストールするよう指示されました。Quick Assist セッションが確立されると、攻撃者は標的のシステムに関する情報を収集し、永続性を確保し、権限を昇格させ、最終的にランサムウェアを展開するためのツールをロードしました。初期の攻撃で確認されたのは BlackBasta ランサムウェアですが、攻撃の後半では、攻撃者は Cactus ランサムウェアを使用するようになりました。

この攻撃は、組織が正当な目的でリモートアクセスツールを使用している状況が、攻撃者にどう操られる可能性があるかを浮き彫りにしています。また、IT 担当者がユーザーと連絡を取る際に許可された方法について、ユーザー教育を行うことの重要性を改めて組織に認識させる事例でもあります。

RansomHub は金銭目的の RaaS グループであり、遅くとも 2024 年 2 月から活動を活発化させています。このランサムウェアはおそらく、2024 年 2 月にアンダーグラウンド フォーラムで販売された Knight ランサムウェアの更新バージョンだと考えられます。RansomHub の関係者は通常、二重恐喝手法を用います。被害者のデータを暗号化すると同時に情報も盗み出し、身代金を支払わなければデータリークサイトに公開すると脅す手口です。

現在、RansomHub はランサムウェアの脅威環境において重要な役割を果たしています。LockBit と ALPHV（いずれも有名なランサムウェアグループ）の関係者や、Scattered Spider（以前は ALPHV ランサムウェアを攻撃に使用していた金銭目的のサイバー犯罪集団）が RansomHub に注目するようになっています。RansomHub は通常、多額の支払いを得るために大規模な組織を標的にします。今年 Talos が対応した RansomHub インシデントでは、標的となった組織の平均従業員数は 18,000 人以上でした。

前述の詳細な傾向と一致していますが、今年の RansomHub の対応業務の大半で、攻撃者が重要なサーバーを含む侵害を受けたホストでエンドポイント保護機能のアンインストールを成功させ、ランサムウェアを密かに展開していたことが確認されました。

1 位は引き続き LockBit、新勢力の RansomHub が 2 位に急浮上

ランサムウェア攻撃グループのリークサイトへの投稿をモニタリングした結果、LockBit は 3 年連続で、最も活発な RaaS（サービスとしてのランサムウェア）グループでした。LockBit は、Talos が追跡している 60 以上のグループの中で投稿件数が最も多く（つまり、被害者を侵害した疑いがあり）、この過密な環境において、事実上 16% の市場シェアがあることになります（図 18 を参照）。LockBit が 3 年連続トップを維持しているというのは、非常に注目に値することです。新たなランサムウェアグループが現われては消え、状況が常に変化する動的な環境の中で、予想以上に長く生き残っているからです。さらに、LockBit は 2024 年初めに法執行機関による大規模なテイクダウンの対象となりました。しかし、すぐに立ち直って再編成を果たし、その後すぐに通常の活動レベルに戻っています。なお、2022 年 9 月に LockBit のビルダーが流出しました。これが原因で、この暗号化ツールを利用する攻撃者の数が増えたため、LockBit ランサムウェアの使用が広がった可能性があります。

特に注目すべきは、新勢力の RansomHub です。2024 年 2 月に初めて確認された Knight ランサムウェアグループの後継と考えられており、LockBit に肉薄し、投稿の 11% を占めました。

RansomHub に加え、Akira、Hunter's International、INC Ransom、Qilin、BlackSuit が、今年活発に活動した RaaS グループのトップ 10 にランクインしており（昨年はランク外）、この脅威環境における勢力図が急速に変化していることがわかります。特定のグループが勢いを増す一方で、他のグループが停滞している状況については、既存グループの名称変更、ソースコードの流出、攻撃者間の紛争、法執行機関の介入など、さまざまな説明がなされています。

図 18
2024 年におけるランサムウェアグループによるデータリークサイトへの投稿数

- **16%** LockBit 3.0
- **11%** RansomHub
- **8.5%** Akira
- **7%** Play
- **5%** Hunters International
- **4%** INC Ransom
- **4%** Black Basta
- **4%** Qilin
- **3%** BianLian
- **3%** BlackSuit
- **3%** 8Base
- **2%** Cactus
- **2%** Everest
- **2%** FOG
- **2%** Rhysida
- **25%** その他

*四捨五入しているため、割合は合計で 100% になりません

今年最も活発に活動した *RaaS* グループの多くが昨年はトップ *10* に入っていなかったことが、この環境が絶えず変化していることの証左です。

復号ツールの公開が、ランサムウェアグループを阻止するための画期的な手段に

2024 年は法執行機関が主導する摘発作戦が数多く実施され、対象となったランサムウェアグループにさまざまな影響を与えました。1 つ明確になったことは、関連する復号ツールが公開された場合、ランサムウェア攻撃グループがテイクダウンから完全に復活する可能性がはるかに低くなるということです。2023 年末の FBI による妨害により、ALPHV の勢力は失墜しました。同グループは 2023 年のレポートでは 2 位でしたが、2024 年は 22 位に後退しています。妨害の一環として、FBI はグループが運営する複数の Web サイトを押収し、影響を受けた被害者に復号ツールを提供してシステムを復旧できるようにしました。グループはテイクダウン後に新しいサーバーを立ち上げましたが、復号作戦がグループの収益に大きな影響を及ぼしました。3 月には管理者が活動停止を決定し、ソースコードを販売する意向を表明しています。

一方、LockBit ランサムウェアグループも大規模なテイクダウンの対象となりましたが、この作戦では復号ツールは公開されませんでした。クロノス作戦と名付けられたこの撲滅作戦では、ウクライナ、ポーランド、米国の当局が 2 月に LockBit に対して同時に作戦を開始し、主要なダークネットのインフラを掌握して複数の関係者を逮捕しました。LockBit の活動は衰退し、データリークサイトへの投稿件数も前年の 926 件から 2024 年は 783 件に減りましたが、それでも 3 年連続で、LockBit がこの分野での攻撃グループのトップとなりました。

最終的に、2024 年 5 月に欧州刑事警察機構は、IcedID、Smokeloader、SystemBC、Pikabot、Bumblebee など、ランサムウェアの第 1 段階の展開をサポートするマルウェアローダーとボットネットに対して史上最大の作戦を開始しました。この作戦で、関係者の逮捕、犯罪インフラの解体、違法収益の凍結が行われました。それにもかかわらず、ランサムウェアの活動やデータリークサイトへの投稿全体の件数の顕著な落ち込みが確認されていないことから、関係者が他のツールの使用に切り替えたか、マルウェアのインフラが再構築されたことが示唆されています。さらに、この 1 年間で有効なアカウントが広く使用されたことを踏まえると、ランサムウェア攻撃グループは、ランサムウェアを展開する方法として、これらのツールに依存しなくなったという可能性もあります。

2024
一年の総括

アイデンティティベースの脅威

2024 年の脅威の中心はアイデンティティ攻撃

2024年に本レポートのために調査したデータの多くで共通していたのは、アイデンティティでした。初期アクセス経路から、攻撃チェーンの後半の攻撃手法に至るまで、攻撃者は、活動を強化するためにアイデンティティベースの攻撃を多用していました。攻撃者は、脆弱性のエクスプロイトやマルウェアの展開など複雑な方法を使用せずに、単にログインするだけでネットワークやアカウントを侵害する手法を選ぶようになっています。

アイデンティティベースの攻撃が攻撃者にとって魅力的な理由は、多くの場合は最小限の労力で、またセキュリティ上の観点からは大きな抵抗を受けることなく、さまざまな攻撃を実行できるからです。その大きな要因は、正規のユーザーアカウントから発生しているアクティビティのように見えるため、検出が困難なことです。

こうした攻撃が非常に効果的であることに加え、盗んだログイン情報を販売する大きな市場も生まれています。攻撃の初期段階では、漏洩したログイン情報がよく使用されており、有効なパスワードとユーザー名の組み合わせがダーク Web 上で頻繁に取引されています。つまり、サイバー犯罪者にとって、将来販売することを目的にログイン情報を盗み出すことには強力な金銭的インセンティブがあるということです。また、攻撃者が、盗まれたログイン情報を簡単に入手して攻撃に使用できることも、これで明らかになっています。

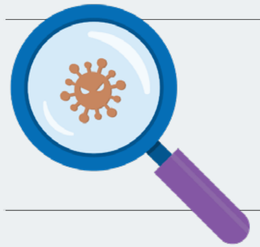
ダーク Web 上の不正なマーケットプレイスでは、ログイン情報や個人を特定できる情報（PII）に加えて、アイデンティティベースの攻撃を実行する Tools-as-a-Service や、特定のデータや特定の被害者のネットワークへのアクセスを取得するアウトソーシングサービスも提供されています。Talos によるダーク Web の調査から得られた、この領域における知見をいくつかご紹介します。

- 販売されている盗難データは、プレーンテキストのログイン情報（特にメールアカウントのもの）、SSH ログイン情報、銀行識別番号（BIN）やクレジットカード番号などの財務データ、ブラウザのキャッシュから抽出されたセッショントークン、住所などです。サイバー攻撃者は、このセクションで後ほど概説する 1 つまたは複数の TTP を使用して、あるいは情報窃取マルウェアのようなマルウェアを使用して、データを取得した可能性があります。
- ソフトウェアとインフラストラクチャはサービスとして販売されており（as-a-Service 型）、フィッシングキットや情報窃取マルウェアなど、ログイン情報を盗み出すことを目的としたツールを中心に、通常は 50 ドル未満から 750 ドル程度の階層型サブスクリプション形態で提供されています。これらのツールには、使いやすいインターフェイスが用意されており、顧客サポートも提供されているため、新参者のサイバー攻撃者でも扱いやすくなっています。
- 経験豊富な攻撃者は自分のサービスを宣伝しており、特定の機能を実行するために、そうした攻撃者のサービスが採用される場合もあります。また、有名企業へのアクセスもオークションにかけられており、平均 1,000 ～ 3,000 ドルで取引されています。
- 大量のログイン情報が記載されたリストは、通常、ダーク Web マーケットプレイスでわずか 10 ～ 15 ドルで販売されています。

アイデンティティベースの攻撃が増えている理由

攻撃対象領域が拡大

近年は、特にテレワークが常態化したことに伴い、Web アプリケーションやクラウドベースの環境、BYOD ポリシー、SSO ソリューションの利用が増加しています。その結果、攻撃者が悪用する可能性がある、ログイン情報が有効なアクセスポイントがネットワーク内で増えています。



検出が困難

攻撃の多くは正規の認証プロセスを利用しているため、ネットワーク境界での検出は困難です。さらに、攻撃者がアクセスを獲得すると、侵害されたユーザーのアカウントから実行された悪意のあるアクティビティが検出されにくくなります。

実行が容易

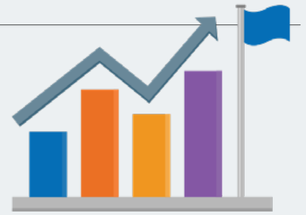
攻撃者は、盗まれたログイン情報を簡単に入手できます。多くの場合は、ダーク Web で販売されている情報や、過去に流出した情報を取得します。さらに、アイデンティティベースの攻撃では、高度な技術的手法ではなく、ソーシャルエンジニアリングが主に使用されます。

他の攻撃が可能になる

攻撃者は、標的のデバイスへの最初のアクセスを取得した後も、権限の昇格、侵入拡大、内部のソーシャルエンジニアリング攻撃などを行うために、攻撃活動全体を通してアイデンティティ攻撃を続けることができます。

重要なアクセスを達成

攻撃者は、比較的単純な手段を使ってアイデンティティベースの攻撃に対するセキュリティ対策を突破し、組織全体のアクセス権と権限が管理されている Active Directory や、日常業務を支えるクラウドアプリケーション、あるいは IT ネットワークや運用テクノロジー（OT）システムといった、組織のサイバーセキュリティの重要な要素にもアクセスできるようになります。



アイデンティティ攻撃とは？

アイデンティティベースの攻撃は、データやネットワークにアクセスするために、ユーザー、組織、またはマシンの一意のデジタルアイデンティティを標的にします。デジタルアイデンティティは、有効なアカウントのユーザー名とパスワードだけに限定されません。攻撃者は初期アクセスを取得するために、デジタル証明書、API キー、暗号化キー、セッショントークンなど、さまざまな識別子を悪用します。

ログイン情報

クリアテキストおよびプレーンテキストのパスワードおよびユーザー名

API キー

ユーザーまたは API を呼び出すプログラムを認証および承認するために使用される一意の識別子。セキュリティの目的と、使用状況を監視したり、使用を制限したりするために利用されます。

デジタル証明書

ユーザー、デバイス、またはサーバーのアイデンティティを検証する電子ファイル

暗号化キー

データの暗号化と復号を行うためのランダムなビット列。SSH、HTTP、Telnet などの安全な接続で使用されます。

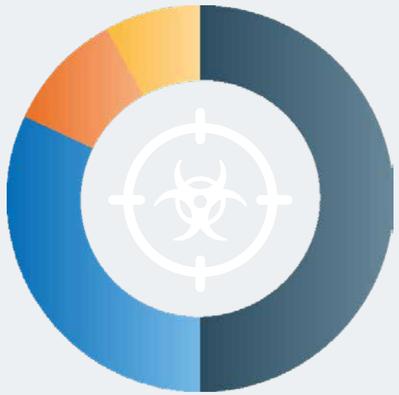
セッション ID

Web サイトまたはアプリケーションでのユーザーのセッションを識別するもの。盗まれた場合、攻撃者は正規の認証済みユーザーとしてリソースにアクセスできるようになります。

2024 年のアイデンティティ攻撃

Talos IR のインシデント事例で、アイデンティティベースの攻撃に大きく移行している状況が確認されました。2024 年に、初期アクセスを獲得するために最もよく使用された手法は有効なアカウントであり、2 年連続でこのアクセス手法がトップとなりました。

アイデンティティ攻撃における攻撃者の目的



- **50%** ランサムウェアおよびランサムウェア感染前
- **32%** 収益化を目的としたログイン情報の窃取
- **10%** 将来の攻撃のためのデータ窃取
- **8%** 金融詐欺

60%

2024 年の Talos IR の事例の半数以上に、アイデンティティ攻撃の要素が含まれていました。

44%

すべてのアイデンティティ攻撃のほぼ半数が Active Directory を標的にしたものであり、その他の 20% はクラウドアプリケーションを標的にしていました。

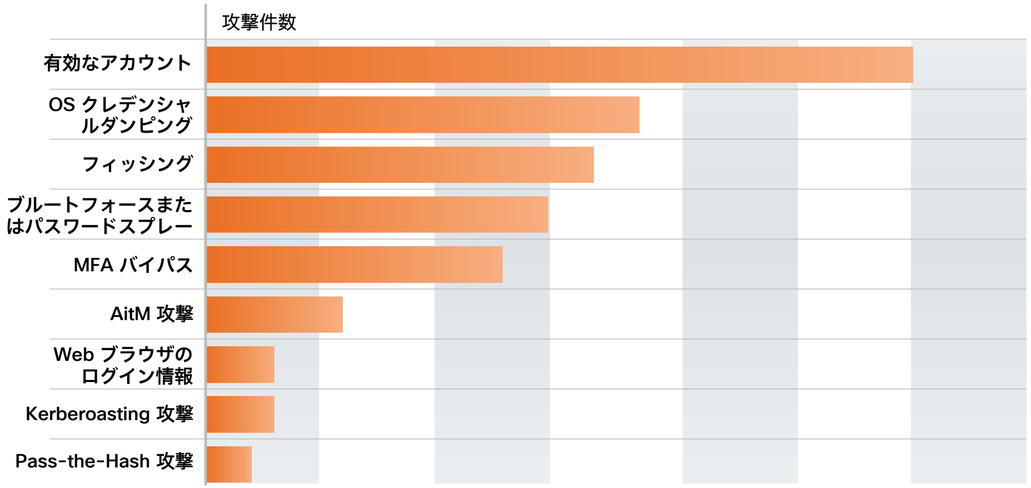
攻撃チェーン全体に広がるアイデンティティ攻撃

Talos IR の対応業務で確認された最も一般的な手口は、有効なアカウントを使用することでした。この手口は通常、初期アクセスの段階で確認されます。攻撃者は、既存アカウントのログイン情報を取得し、これを悪用することで、攻撃のさまざまな段階を実行しました。OS クレデンシャルダンピングも非常に一般的な手口でした。攻撃者の大半は、LSASS メモリと Active Directory のログイン情報を標的にしていましたが、この脅威カテゴリではその他にもさまざまな手法が確認されています。たとえば、Security Account Manager（SAM）のデータベースからログイン情報を抽出する試み、キャッシュされたドメインのログイン情報にアクセスする試み、Windows ドメインコントローラの API を悪用する目的での DCSync という手法の使用、さまざまなログイン情報が含まれるローカルセキュリティ機関（LSA）の機密情報にアクセスする試みなどです。これらは、攻撃者がホストへのシステムレベルのアクセスを取得することで可能となります。

攻撃者の目的を評価したところ、すべてのアイデンティティベースの攻撃のうち半数は、ランサムウェアとランサムウェア感染前の攻撃に関連していることがわかりました。窃取したログイン情報を売って利益を得ることも攻撃者の目的であることが多く、たとえば初期アクセスブローカーによるログイン情報の販売（32%）などが確認されました。また、スパイ活動や将来の攻撃を可能にするためのログイン情報の窃取（10%）のほか、クレジットカードデータの盗難や、被害者を騙して送金させるといった金融詐欺（8%）も確認されています。

図 19

Talos IR で確認されたアイデンティティ攻撃の種類



実際のアイデンティティ攻撃：Active Directory の侵害

前述のように、Talos IR が対応したインシデントで確認されたアイデンティティベースの攻撃の 44% は、広く使用されている Microsoft の Windows サービスである Active Directory を標的としたものでした。Active Directory には、ユーザー名、パスワード、アクセス権限などの重要なユーザー情報が保持されているため、攻撃者にとって価値の高いデータの宝庫となっています。しかも、最近の政府の報告書によると、Active Directory は、世界中のエンタープライズ IT ネットワークで最も広く使用されている認証および承認ソリューションです。

Active Directory が攻撃者にとって非常に重要な標的であるというリスクに加え、組織がこれらの環境を適切に保護していないことも少なくありません。Active Directory の侵害に関連する Talos IR の事例の多くでは、セキュリティ製品の設定ミスや、業界が推奨するベストプラクティスと矛盾するポリシーを持った企業環境で攻撃が成功していました。

Active Directory は重要な企業ユーザー情報を保持し、世界中で最も広く使用されているアイデンティティおよびアクセス管理（*IAM*）ソリューションです。そのため、*Talos IR* の事例で確認されたアイデンティティベースの攻撃の *50%* 近くが、このサービスを標的としている理由は明らかです。

ケーススタディ：Active Directory を利用してデータセンターと重要なサービスを停止させる攻撃手法

2024 年 8 月、自社のマネージドデータセンターでホストされているサーバーから複数の Endpoint Detection and Response（EDR）ソリューションが予期せずアンインストールされていたという報告を製造業のシスコのお客様から受けました。その中には、2 台のドメインコントローラも含まれていたので、攻撃者が Active Directory ドメインへの完全なアクセスを得ていたと考えられます。この調査で、攻撃者がランサムウェアを展開する準備として Active Directory を侵害したことを示唆する証拠が見つかりました。攻撃者は、Sysinternals 管理ツールスイートの一部である ADExplorer を利用して環境内のさまざまなドメインを参照し、Active Directory データベースをダンプしていました。

攻撃の初期段階でアイデンティティベースの攻撃が使用されたこの事例から、この手法がいかに有効であるかがわかります。また、Active Directory への初期アクセスが、より広範な攻撃を始めるために不可欠であることと、その手のアクセスがランサムウェアなどの影響力の大きい脅威の展開に役立つことも確認しました。

ケーススタディ：Active Directory への攻撃

1. Active Directory データベース内のローカルパスワードとパスワードハッシュを抽出
2. 特権管理者アカウントに昇格
3. パスワードをリセットし、新しいアカウントを作成して永続性を維持
4. ドメインコントローラへのラテラルムーブメントと Mimikatz の使用
5. 持続的なアクセスを維持するためにバックドアやその他のソフトウェアをインストール
6. バックアップシステムにアクセス
7. ランサムウェア感染前の TTP が発生（迅速に対応しなければ、最終的にランサムウェアが展開される可能性があった）

過剰な権限または不適切な権限を持つアカウント（ユーザー、管理者、サービス）、脆弱なパスワードまたはデフォルトのパスワードを使用しているアカウント、フラットネットワーク アーキテクチャ、*MFA* の未導入や設定ミスが頻繁に確認されています。*Active Directory* の侵害を軽減するための Talos の推奨事項は *CISA の戦略* に沿ったものであり、攻撃者や悪意のある者が *Active Directory* を侵害するために使用する *17* の最も一般的な手法への対策となります。

実際のアイデンティティ攻撃：クラウド サービス プロバイダーの API を侵害

クラウドを標的とした攻撃も増加しており、Talos IR の調査結果によると、アイデンティティベースの侵害の 20% がクラウドアプリケーションに影響を及ぼすものです。さまざまなクラウドサービス間や、クラウドとオンプレミスのアプリケーション間のシームレスな通信、統合、データ転送を円滑に行うには、クラウド API が必要です。

API が格好の標的となっている理由は、あらゆる業種のユーザーと企業をサポートするように設計されたソフトウェアで使用されているため、機密データと重要なアプリケーションの機能に直接アクセスできるからです。クラウド API には、管理が難しいという特性もあります。非常に多くの種類があり、さまざまなクラウドプロバイダーにまたがる多様な機能を備えていて、進化するクラウドサービスに合わせて API を常にモニタリングして更新する必要があるからです。さらに、多くのクラウド API は公開されているため、攻撃者は潜在的な脆弱性を簡単に発見し、テストすることができます。

ここでは、こうしたインシデントに対応した経験に基づき、攻撃者がアイデンティティベースの多くの攻撃手法を利用してクラウド API を侵害する方法の例を紹介します。

ステップ 1：侵害したデジタル ID を使用してクラウド API にアクセスする

- 初期アクセスで、攻撃者は窃取した API キーまたはセッション Cookie を利用して MFA をバイパスし、クラウド環境に侵入します。クラウドベースの IAM サービスである Microsoft Entra ID の場合、盗まれたプライマリ更新トークンを利用すれば、Microsoft クラウド全体のサービスへのアクセスとサインインを維持できます。
- 攻撃者が、フィッシングや情報窃取マルウェアの展開によってログイン情報を盗み出す可能性もあれば、弱いログイン情報や簡単に推測できるログイン情報を API が使用している場合は、パスワードスプレーやクレデンシャル スタッフィングなどのブルートフォース手法を使用してログイン情報を窃取する可能性もあります。
- 攻撃者が、従来の手法を転用してクラウド環境を侵害することに成功していることに注意してください。

ステップ 2：クラウド専用のツールを使用してデータを列挙する

- スキルの高い攻撃者が作成したツールが、オープン Web 上で無料で入手可能です。こうしたツールは展開が容易で、クラウド環境に特化した設計になっています。
- たとえば、ROADtools と AADInternals は、Microsoft Entra ID 環境を列挙するために設計された公開フレームワークです。これらのツールは、ユーザー、グループ、アプリケーション、サービスプリンシパル、デバイスに関するデータを収集し、コマンドを実行できます。ROADtools はカスタムプラグインと連携して、データをクエリおよび分析することもできます。

ステップ 3：侵入後のアクティビティのためのコマンドを実行する

- 攻撃者が適切な権限を持っていれば、クラウド API を悪用し、本来はクラウドリソースの管理に使用されるクラウドプロバイダーのコマンドライン インターフェイスを利用してコマンドを実行することが可能です。
- 攻撃者がコマンドを実行してバックドアを設置したり、リバースシェル接続を作成して永続性を確保したり、データを流出させたりする可能性があります。

ステップ 4：広範なサービス停止や破壊的な攻撃が行われる可能性がある

- API で処理されるデータを攻撃者が窃取する可能性があります。たとえば、個人を特定できる情報（ソーシャルセキュリティ番号など）や、財務データ（クレジットカード情報など）、健康関連のデータ（医療記録など）、知的財産、個人的なやり取り、ユーザー アクティビティ データ（閲覧履歴や物理的な位置情報など）です。
- 潜在的な攻撃：
  - 盗まれたアイデンティティを使用して被害者になりすまし、金銭を窃取する。
  - 盗まれたアカウントを使用して、顧客や信頼できるビジネスパートナーなどの第三者にビジネスメール詐欺攻撃を仕掛ける。
  - 事業運営を中断させる（重要なサービスの遅延につながる可能性あり）。
  - アカウントへのユーザーのアクセス権を削除する。
  - ランサムウェア攻撃やデータ窃盗による恐喝を行う（経済的損失、社会的信用の低下、法令違反につながる可能性あり）。

ステップ 5：検出を回避する

- 攻撃者は、ログを削除または改ざんしたり、正規の API トラフィックを模倣して悪意のあるアクティビティを埋もれさせたり、クラウドインスタンスに加えた変更を元に戻したり、他にもさまざまな手口を使って検出を回避しようとします。
- 回避手段は、攻撃ライフサイクルのどの時点でも実行できます。

2024
一年の総括

MFA に対する攻撃

協力：
CISCO DUO

CISCO TALOS

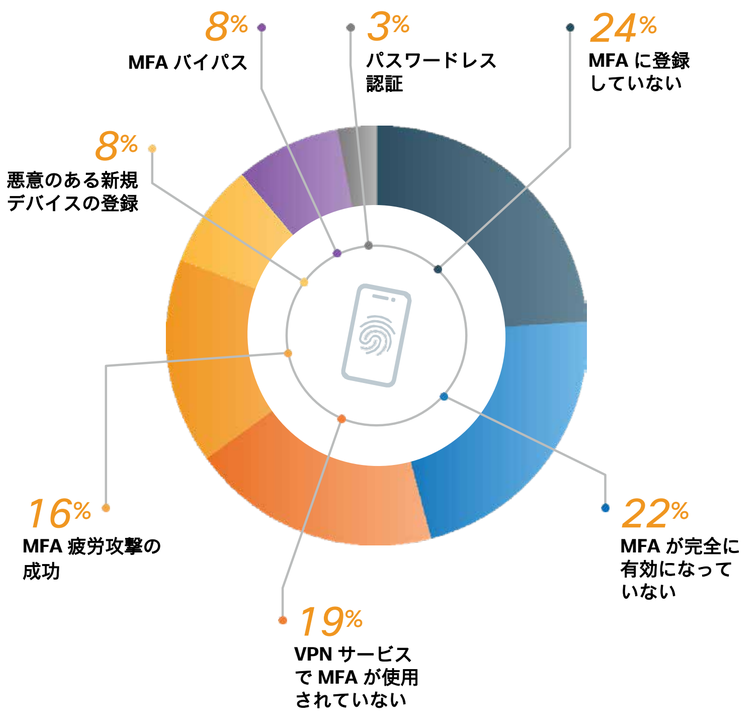
攻撃者が悪用する MFA のさまざまな弱点

前述したとおり、攻撃者がユーザーのアイデンティティを侵害する主要な方法は、多要素認証（MFA）プロセスを標的にすることです。この領域での攻撃活動の量と、防止できた可能性のある攻撃において MFA が果たした役割を踏まえ、本レポートでは MFA 攻撃に特化したセクションを設けることにしました。ここでは、2024 年にアイデンティティ攻撃の急増が見られた主な要因である、MFA が直面する脅威について掘り下げます。

今年の Talos IR のデータによると、MFA の弱点が主要なセキュリティの弱点でした。この傾向は前年から変わらず続いています。確認された MFA 問題の 4 分の 1 は、MFA に登録していないことが原因でした。しかし、それ以外にも今年は MFA の導入が不十分であった事例がさまざま見られ、その結果、攻撃者が重要なリソースへのアクセスを取得し、標的のネットワークで永続性を確立できていました。

図 20

Talos IR の事例で確認された MFA の弱点



MFA は強力なセキュリティを提供することが実証されていますが、どのシステムやリソースを *MFA* で防御するかを把握するためのコストと複雑さを考慮し、導入を見送る組織もあります。

Talos IR が提案する、MFA 導入にあたっての 4 つの重要なセキュリティ対策

1. VPN サービスで MFA を有効にする：VPN サービスで MFA が導入されていない状況を攻撃者が悪用する事例が一貫して確認されました。特に従業員が VPN を使用して企業ネットワークにアクセスする組織では、VPN へのアクセスに MFA を必須にする必要があります。

2. ユーザー教育を行い、MFA プロンプトのしきい値を設定する：攻撃者は、MFA 疲労攻撃も利用していました。この攻撃では、ユーザーが最終的に承認するまで認証要求が繰り返し送信されます。この攻撃は、ユーザー教育を改善するとともに、同一の IP アドレスまたはデバイスから送信された失敗した MFA 要求の数を制限することで緩和できます。

3. より高度なセキュリティ要素を導入する：ユーザーが質問に対して正しく回答する必要がある「チャレンジレスポンス認証」のような、追加のセキュリティ対策を導入します。この例としては、セキュリティに関する質問（「母親の旧姓は何ですか」、「通っていた高校の名前は何ですか」など）や、CAPTCHA（ユーザーが人間であることを確認するために、画像に表示されている文字の入力を求める認証方式）が挙げられます。こうすることで、目的の情報やデジタル資産にアクセスするには、さらに 1 つ課題をクリアしなければならなくなります。

4. デバイス登録を確実に監視する：新しいデバイスが MFA に登録された場合に、セキュリティチームが継続的に監視してログを記録するか、新しいデバイスが登録される前に、追加の方法による認証を要求するようにします。Duo などの一部の MFA 製品では、組織向けにロギング機能を提供しています。多くの事例で、攻撃者が被害者の MFA システムに自分の認証デバイスを追加し、検出されることなく攻撃を仕掛けていました。

MFA 攻撃者は直接 IAM アプリケーションを攻撃

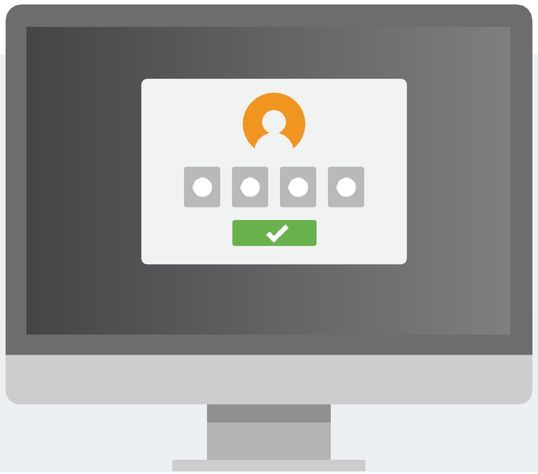
Cisco Duo のデータによると、MFA 攻撃で最も頻繁に狙われたのは IAM アプリケーションで、関連するインシデントの 4 分の 1 近くを占めました。IAM アプリケーション、ネットワークセキュリティ、認証とネットワーキング、リモートアクセス アプリケーションを合わせると、攻撃者が MFA 導入環境を標的にしたインシデントの 50% を超えていました（図 21 を参照）。

以下に示しているのが、最もよく狙われる IAM アプリケーションです。Citrix、Microsoft、Fortinet、Palo Alto Networks、Cisco、F5 など、さまざまなベンダーが標的になりました。これらの企業の製品が世界中で広く使用されていることを考えれば、驚くことではありません。

図 21

MFA 攻撃で標的となるアプリケーションの種類

- **24%** アイデンティティおよびアクセス管理（IAM）
- **14%** ネットワークセキュリティ
- **10%** 認証とネットワーキング
- **9%** リモートアクセス
- **9%** アプリケーション配信とセキュリティ
- **8%** ソフトウェア開発キット（SDK）
- **6%** 認証プロトコル
- **6%** 認証およびネットワーク アクセス コントロール（NAC）
- **6%** クラウドセキュリティと認証
- **3%** オペレーティングシステム
- **3%** API 通信プロトコル
- **2%** メールとコラボレーション



IAM 攻撃の標的として最も頻繁に狙われるアプリケーション

Shibboleth

教育機関や研究機関で広く使用されているオープンソースの SSO ソリューション。

Central Authentication Service（CAS）

Web アプリケーションのセキュアな認証を提供するオープンソースの SSO ソリューション。

Active Directory フェデレーション サービス（ADFS）

SSO およびアイデンティティ フェデレーションのための Microsoft のソリューション。

Duo Central

ユーザーが自組織のアプリケーションにアクセスするための、Duo の一元化された Web ポータル。

Microsoft 365 SSO

Microsoft サービスの統合認証を可能にする Microsoft 365 向け SSO。

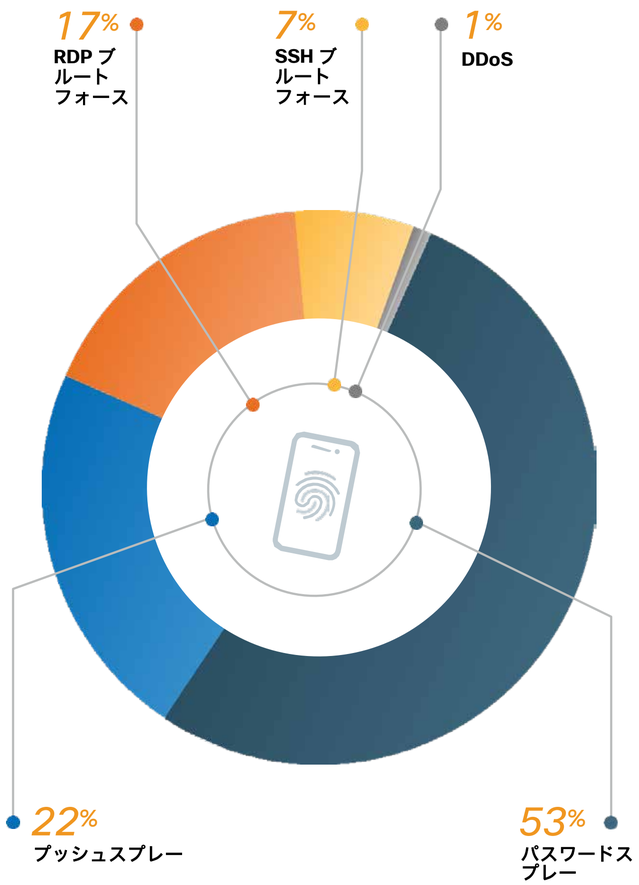
頻繁に発生する、簡単に防止できるスプレー攻撃が最も一般的

攻撃者は、MFA を導入していない、または MFA が正しく設定されていない組織を探し回っています。パスワードスプレー攻撃は、攻撃者が共通のパスワードを使用して多数のアカウントにアクセスしようとする攻撃であり、MFA で保護されたアプリケーションに対して最も頻繁に発生した脅威の種類でした。ただし、MFA はブルートフォース攻撃やパスワードスプレー攻撃の緩和に非常に効果的です。その理由は追加の認証手段が必要なためですが、結果として、この種の攻撃の成功率が低くなる傾向にあります。

プッシュスプレーが 2 番目に一般的な攻撃タイプでした。この手法は、「MFA 爆撃」または「MFA 疲労攻撃」とも呼ばれ、スプレー攻撃に見られる単純なパスワード推測アプローチを超えるものです。攻撃者は、被害者のデバイスに MFA プッシュ通知を大量に送り、ログイン要求を確認または承認するように促します。これにより、最終的に被害者が根負けしてうっかりアクセスを許可してしまうことを狙っています。

図 22

MFA 攻撃の種類



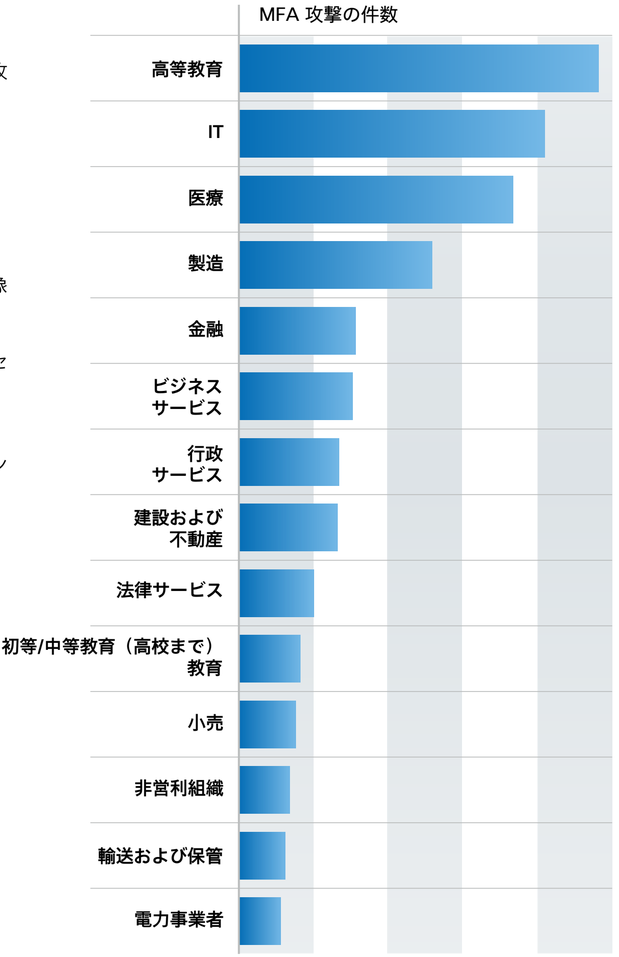
狙われた上位の業種は広範な攻撃傾向と一致

MFA 攻撃で最も狙われた業界が教育と医療であったのは驚くべきことではありません。Talos IR の調査結果でも、ランサムウェア攻撃だけでなく、すべての攻撃タイプにおいて、これらの業種が常に上位に挙げられていました（このレポートの冒頭で説明）。

影響を受けた教育機関の種類を見ると、大学が標的にされた件数は、小中高教育機関の 6 倍でした。高等教育機関が、データ窃取とパスワード収集の格好の標的となる理由はいくつかあります。1 つは、攻撃対象領域が広く、多くの学生が自分のモバイルデバイスを使用して大学のリソースにアクセスするからです。2 つ目は、情報にアクセスできる学生が適切なサイバーセキュリティ対策を行っていないケースが多いため、攻撃者に狙われやすいのだと考えられます。3 つ目は、大学が使用するアプリケーションは、ソーシャルセキュリティ番号、請求および支払い情報、運転免許証、その他の個人を特定できる情報 （PII）など、学生に関する機密情報を保存している可能性が高いからです。これらの情報は通常、小学校、中学校、高校では収集されません。

図 23

MFA 攻撃で狙われた上位の業界



実際の MFA 攻撃：フィッシングとデバイス侵害により、大規模な大学で重大な侵害が発生

ここで紹介するケーススタディは、MFA 攻撃が日常的なシナリオでどのように行われるかの例です。このインシデントでは、10 万人を超えるユーザーを抱える大規模な大学が、フィッシングとデバイス侵害の被害に遭いました。

Talos の調査によると、攻撃者はすでにこの組織の標的ユーザーの盗まれたログイン情報（ログインとパスワードの組み合わせ）を入手していました。ログイン情報は、初期アクセスブローカー（IAB）から購入したか、別のデータ漏洩から入手したと考えられます。攻撃者はシステム管理者にフィッシングメールを送りつけて認証用のリンクをクリックするように仕向け、攻撃者のデバイスを被害者の MFA アカウントに追加させました。これにより、攻撃者はネットワーク上の他の複数のユーザーに内部でフィッシングメールを送信できるようになりました。

この組織の重大なセキュリティの落とし穴の 1 つは、管理者アカウントが 50 個もあったことでした。管理者が機密情報へのアクセス権限を持っていることを考えると、この数はあまりに多すぎると言えます。さらに、管理者は全員が請負業者であり、これはセキュリティのベストプラクティスではありません。Talos 独自の調査でも、攻撃者は同等の権限を持つアカウント所有者よりも請負業者を標的にする場合が多いことがわかっています。

ケーススタディ：大学に対する MFA 攻撃

被害者：大規模な大学
（ユーザー数は *10* 万人以上）

2024
一年の総括

AI の脅威

2024 年および 2025 年における AI の脅威の概況

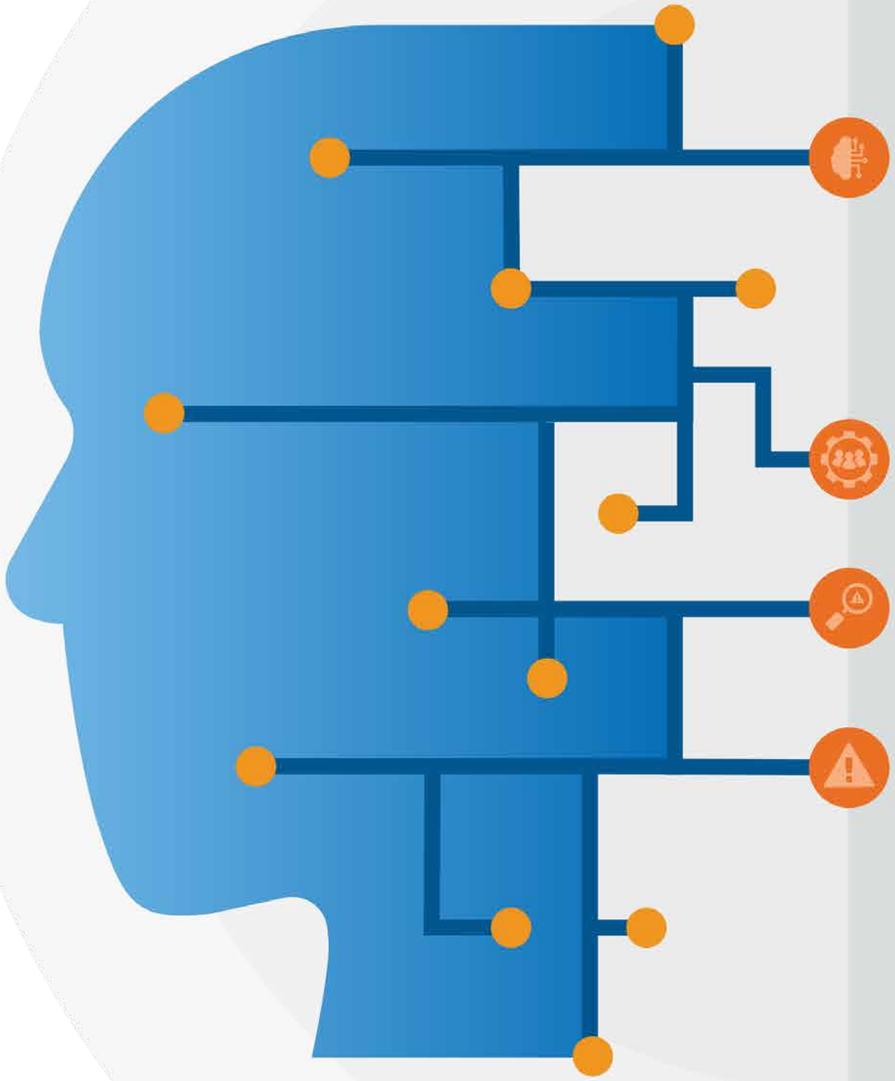
2024 年には、AI と機械学習（AI/ML）アプリケーションが引き続き急増し、さまざまなビジネス統合とツールが登場しました。一方、サイバーセキュリティ分野では、脅威と脆弱性の検出を強化し、対応を自動化し、組織の全体的なセキュリティ態勢を強化するために、サービスプロバイダーが製品やワークフローへの AI の統合を進めています。AI/ML テクノロジーの進歩と導入により新たなビジネスチャンスが生まれましたが、リスク環境や脅威環境の複雑化の要因ともなっています。シスコの Robust Intelligence チーム（シスコの新しい AI Defense セキュリティソリューションを支える脅威研究者/開発者）は、この領域を注意深く監視しています。以下は、今後最も懸念される、潜在的な AI ベースのサイバー攻撃です。

- AI システム、アプリケーション、インフラストラクチャに対するサイバーセキュリティのリスク
- AI モデルによるデータ漏洩、改ざん、アクセシビリティのリスク
- AI を使用したサイバー攻撃（特にソーシャルエンジニアリング）の自動化と巧妙化

こうした脅威は 2025 年以降に顕在化する可能性がありますが、2024 年における AI の主な用途は、新しい手口を編み出すことではなく、既存の手口を強化することでした。

2024 年は、攻撃者の AI の利用はまだそれほど活発ではない

生成 AI は強力であり、脅威の状況に大きな影響を及ぼす可能性がありますが、2024 年時点では、AI を使用したことで攻撃者の TTP が大幅に強化されることはありませんでした。攻撃者が AI を活用し、今までにない機能を開発する可能性はありますが、そうした機能が実際に大規模に展開された事例はまだ確認されていません。一方、国家が支援する攻撃グループとサイバー犯罪者の両方が、1）ソーシャルエンジニアリング、2）タスクの自動化をはじめとする、攻撃ライフサイクルにおける生産性向上に AI を使用しています。



2025 年に予想される攻撃者の AI 活用方法

2025 年には次のような進展が見られると予測しています。

エージェント型 AI の台頭

エージェント型 AI （人間が常に指示しなくても自律的に動作して目標を達成できる AI システムとモデル）は、エージェント型システムやその潜在的な危険性に対処する準備も態勢も整っていない組織にとって脅威となります。エージェント型システムと、異なるサービスやベンダーとの統合が進むにつれ、エクスプロイトや脆弱性のリスクが高まります。またエージェント型システムが、多段階攻撃を実行し、制限されたデータシステムにアクセスする独創的な方法を見つけ、一見無害な動作を有害なシーケンスに連鎖させたり、ネットワークやシステムの防御担当者による検出を回避する方法を学習したりする可能性があります。

大規模なソーシャルエンジニアリングを継続

ソーシャルエンジニアリングからプロパガンダの拡散まで、サイバー犯罪者や国家が支援する攻撃グループは、引き続き AI 技術を活用して、悪意のあるアクティビティをさらにカスタマイズし、巧妙化していくと考えられます。

脆弱性の自動検出とエクスプロイト

攻撃者は、ゼロデイエクスプロイトなど、脆弱性を発見するために AI を使用する可能性があります。これにより、公共部門も民間部門もエクスプロイトが加速し、リスクが増加することになります。

AI モデル、システム、インフラストラクチャを侵害する可能性のある機能

AI モデルやシステム自体を標的にする機能の開発において、多くの領域でリスクが生じる可能性があります。たとえば AI を活用したセキュリティフィルタを欺くために攻撃的な入力を使用する、業務ワークフローで使用される AI エージェントをハイジャックする、AI のサプライチェーンの要素を攻撃する（例：トレーニングデータの破損、モデルのクラウド インフラストラクチャの侵害）などが考えられます。AI モデルやシステムを標的とした従来のサイバー攻撃は言うまでもありません。

ソーシャルエンジニアリングにおける生成 AI

大規模言語モデル（LLM）やディープフェイク技術などの生成 AI ツールが利用しやすくなったことで、高度なソーシャルエンジニアリング攻撃が急増しました。しかしこの増加は、ソーシャルエンジニアリングにおける AI の使用と、悪意のあるアクティビティを自動化するための AI の使用という 2 つの異なる要素に分けることができます。これら 2 つの要素を組み合わせることで、攻撃者は成功率を飛躍的に高めることができます。LLM と生成 AI の支援により、より高度なソーシャルエンジニアリングの罠を大量に作成できるからです。このように、フィッシングや他のソーシャルエンジニアリングの手法は AI の支援によって今後も巧妙化していくと予想しています。一方、スパムとフィッシングの検出もこれに追随するでしょう。

2024 年、サイバー犯罪者はこうした手法を活用して説得力のあるフィッシング攻撃を仕掛け、個人を巧みに操って機密情報を漏洩させたり、組織のネットワークやシステムへの不正アクセスを許可させたりしました。

国家が支援する APT（Advanced Persistent Threat）グループやその他の高度な攻撃者は、ディープフェイクビデオやディープフェイク音声など、生成 AI 機能を利用して、インタビューを行ったり、電話をかけたり、ソーシャルエンジニアリングを自動化したりする可能性があります。

攻撃ライフサイクルにおけるタスクの自動化と生産性の向上

攻撃者は、マルウェア開発やタスクの自動化を支援するためにチャットボットを利用し、成功率を高めようとしています。たとえば、標的に関するオープンソース インテリジェンス を収集して要約する手段としてチャットボットを使用しています。

調査では、LLM を使用してワンデイ脆弱性を悪用 できることが明らかになっています（ワンデイ脆弱性とは、情報は公開されたものの、システムにパッチが適用されていない脆弱性のことです）。攻撃者は、基本的なスクリプト作成作業やコードのデバッグを支援するツールとして LLM を活用してきました が、高度な AI 機能を展開して脆弱性のスキャンやエクスプロイトを実際に行った攻撃者はまだ確認されていません。しかしサイバー犯罪者は、脆弱性の調査、偵察、エクスプロイトの作成に役立つ複数のツール を開発し、販売しているとされています。

AI に関するシスコの見解をまとめた詳細レポート

2024 年には、AI を活用したテクノロジーの普及とその市場拡大に主に対応する形で、新たな AI 政策が数多く打ち出されました。シスコがリリースした「State of AI Security（AI セキュリティの現状）」レポートの初号では、AI 脅威環境における動向の概要を包括的に説明しています。このレポートで取り上げている内容は、米国および国際的な AI 政策における重要な進展、AI インフラストラクチャ、AI サプライチェーン、AI アプリケーションに対する脅威の詳細な分析、数々の最先端 AI セキュリティのトピックに関する独自の調査（アルゴリズムによるジェイルブレイク、データセットポイズニング、データ抽出など）です。

詳細はこちら

2024
一年の総括

Cisco Talos について

Cisco Talos は、信頼性で世界トップクラスの脅威インテリジェンス リサーチ チームであり、業界屈指の研究者、アナリスト、インシデント対応担当者、エンジニアで構成されています。包括的で実績のある検証済みのインテリジェンスを通じてシスコのポートフォリオを強化し、何が起きても、世界中のお客様のあらゆる環境を休むことなくサポートしています。Talos のコアミッションは、シスコのお客様を脅威から守り被害を防ぐことです。お客様とユーザー、そしてインターネット全体のために脅威の状況を広く理解し、収集した膨大な量のテレメトリを分析することによって、検証可能な形で脅威を検出し、インテリジェンスを導き出し、対応にあたっています。

お客様を守ることが Talos の使命です。

最新情報

ブログを読む：TalosIntelligence.com/blog | **登録する：**脅威情報ニュースレター | **フォローする：**LinkedIn、X、Mastadon 、BlueSky