CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

September 10, 2024

2024年上半期:
マルウェアと脆弱性の傾向レポート

2024年上半期に最も悪用されたのは、Ivanti Secure Connect、Palo Alto Networks PAN-OS、Microsoft Windows SmartScreenなど、広く使用されているリモートアクセスおよびセキュリティソフトウェアに影響を与える脆弱性でした。

2024年上半期のマルウェア業界は情報窃取型マルウェアが圧倒的な人気を博し、その中でもLummaC2が最も蔓延した種となりました。また、Insikt Groupは、2023年下半期以降、Magecartの感染が103%増加したことを観察しています。

Fog、Raspberry Robin、SocGholishなどのマルウェア運営者は、既存のツールを更新し、ランサムウェア、トロイの木馬、情報窃取型マルウェア、マルウェアローダーに新しい手法を導入して、検出を回避し、分析を妨害する可能性を高めました。

エグゼクティブサマリー

2024年上半期のマルウェアと脆弱性の悪用においては、脅威アクターが既知のTTP（戦術、技術、手順）を改良し、企業の依存する防御を混乱させ、回避するための新しいTTPを実験する動きが見られました。

新たに公開されたゼロデイ脆弱性の悪用が長期化し、パッチが利用可能となった（脆弱性がnデイとなる時点）後でもリモートアクセスとセキュリティソリューションに影響を与えていることが観察されました。また、脅威アクターは、マルウェアの機能をアップデートし、配信メカニズムを改良して、検出を回避し、分析を妨害するようになりました。これには、ランサムウェア運営者が被害者のシステム上でマルウェアを実行するためのパスワードを要求するなどの動きがあります。全体として、情報窃取型（インフォスティーラー）マルウェアがマルウェアの世界を支配しており、脅威アクターが顧客の個人情報や財務情報を盗むように設計された悪意のあるコードでeコマースウェブサイトを侵害するMagecart攻撃は2024年前半期に約103%増加しました。

ゼロデイ脆弱性の悪用と、検出と分析を防ぐための新しいマルウェアTTPは、いずれも悪意のあるアクティビティをタイムリーに検出する防御者の能力を低下させる要因となるため、組織に対する脅威を高めます。その結果、脅威アクターは目標に向かって行動する時間を増やすことができ、標的となる組織に対してより深刻な被害を及ぼす可能性が高くなります。

2024年上半期の脅威の傾向に対処するには、多層防御とプロアクティブな監視が不可欠です。パッチ管理手順を強化することで、特にリモートアクセスやセキュリティツールなどのターゲットを絞ったソフトウェアの場合、nデイ脆弱性に対抗しやすくなります。一方、権限を最小化し、異常な動作を迅速に検出することは、ゼロデイエクスプロイトへの対策に役立ちます。加えて、企業は、著名な情報窃取型マルウェアやeスキマーについての情報を収集し、フィッシングやeコマースプラットフォームの脆弱性の悪用などの配信方法にセキュリティ制御を適応させる必要があります。脅威インテリジェンスに投資することで、セキュリティチームは長期的に最新のTTPを認識し、対応することができるようになります。

主な調査結果

- 2024年上半期のデータセットで最も言及の多かった脆弱性は、Ivanti Secure Connectに影響を与えた3つの脆弱性、PAN-OSの脆弱性、Microsoft Windows SmartScreenの脆弱性の5点でした。

- これらの脆弱性は当初、国家支援型の攻撃者によってゼロデイとして悪用され、おそらくPoC（概念実証）エクスプロイトコードが利用可能になったことを理由に、パッチのリリース後もサイバー犯罪者による標的化が続いています。

- 情報窃取型マルウェアは2024年上半期も依然として主要なマルウェアカテゴリーでした。LummaC2は、Recorded FutureのMalware Intelligenceデータに基づくと、この種のマルウェアの中で最も蔓延しています。

- 2024年上半期を通じ、ランサムウェア、トロイの木馬、情報窃取型マルウェア、マルウェアローダーの更新は、既存のTTPを更新し、新しいTTPを導入することで、分析を妨害し、検出を回避することに重点を置いています。

- 比較的新しいランサムウェアであるFog、RansomHub、3AMの運営者は、ペイロードの実行を検証し、サンドボックスやその他のセキュリティソリューションによる分析を回避する手段としてパスワードを採用しました。

- Raspberry Robin、SocGholish、HijackLoaderなどのマルウェアは、新しいアンチエミュレーション、実行、プロセスハロウイング技術を実装しました。ClearFake、RedLine、Coyoteは、あまり人気のないプログラミング言語やソフトウェアツールを使用した新しい配信手法を実験しました。

- Magecartの感染は、Recorded FutureのPayment Fraud Intelligenceモジュールの統計に基づくと、2023年上半期から2024年上半期にかけて約103%増加しました。こうした増加は、Adobe Commerce

で新たに発見された脆弱性（CVE-2024-20720）の悪用や、「Sniffer By Fleras」と名付けられた新しいMagecartスキマーの登場などの要因に一部よるものであると評価されます。

脆弱性の悪用の傾向

2024年上半期は、広く採用されているセキュリティソフトウェアとリモートアクセスソフトウェアに影響を与える5つの脆弱性の悪用が中心となりました。これらは、Ivanti Secure Connect（旧Pulse Secure）に影響する3つの脆弱性、Palo Alto Networks PAN-OSに影響する1つの脆弱性、Microsoft Windows SmartScreenに影響する1つの脆弱性です。これらの各脆弱性に関する追加情報は以下の**表1**で確認できます。

脆弱性	影響を受けた製品	Recorded Futureでのリスクスコア	CVSS v3	概要
CVE-2024-21887	Ivanti Connect Secure	89	9.1	Ivanti Connect Secure（9.x、22.x）およびIvanti Policy Secure（9.x、22.x）のウェブコンポーネントにコマンドインジェクションの脆弱性があり、悪用されると、認証された管理者が特別に細工されたリクエストを送信し、任意のコマンドを実行することができます。
CVE-2023-46805	Ivanti Connect Secure	89	8.2	Ivanti ICS（9.x、22.x）およびIvanti Policy Secureのウェブコンポーネントに認証バイパスの脆弱性があり、悪用されると、リモートの攻撃者が制御チェックをバイパスして制限されたリソースにアクセスできるようになります。
CVE-2024-21893	Ivanti Connect Secure	89	8.2	Ivanti Connect Secure（9.x、22.x）、Ivanti Policy Secure（9.x、22.x）、Ivanti Neurons for ZTAのSAMLコンポーネントにサーバーサイドのリクエストフォージェリの脆弱性があり、悪用されると、攻撃者は認証なしで特定の制限されたリソースにアクセスできるようになります。
CVE-2024-3400	Palo Alto	89	10	特定のPAN-OSバージョンおよび異なる機能設定

	Networks PAN-OS			のGlobalProtect機能にコマンドインジェクションの脆弱性があり、悪用されると、認証されていない攻撃者がファイアウォールでroot権限で任意のコードを実行できるようになる可能性があります。
CVE-2024-21412	Microsoft Windows SmartScreen	99	8.1	Microsoft Windows SmartScreenに悪意を持って作成されたファイルの処理エラーに起因するセキュリティバイパスの脆弱性があり、悪用されると、リモートの攻撃者はSmartScreenのセキュリティ警告ダイアログをバイパスしてマルウェアを配信できます。

***表1**：Recorded Future データに基づく2024年上半期のエクスプロイト活動に関連する上位5つの脆弱性の概要（出典：Recorded Future）*

PAN-OSに影響を与える脆弱性であるCVE-2024-3400は、2024年上半期のRecorded Future Intelligence Cloudにおいて、サイバー攻撃およびサイバーエクスプロイト活動への言及が最多となりました（**図1**）。2つの脅威アクター（TAG-100およびUTA0218）がこれを悪用していることが報告されており、さらにRedTailを配布するエクスプロイト活動が行われています。ただし、組み合わせとして最も言及が多かったのはIvanti Connect Secureに影響する3つの脆弱性でした。さらに、Insikt Groupとサードパーティの報告によると、これらの攻撃者は最も多くの脅威アクター（サイバー犯罪者と国家支援型アクターの両方）によって悪用されており、個々の悪意のあるエンティティがこれらの2つまたは3つを運用において連携させています。

Mandiantの報告によると、中国関連の脅威アクターUNC5325とUNC5221は、2023年12月以降、BUSHWALK、THINSPOOL、LIGHTWIRE、その他のマルウェアなどのウェブシェルを含むスパイ活動で、CVE-2024-21893とCVE-2024-21887の両方をゼロデイとして悪用しています[1、2]。Volexityは同じキャンペーンを追跡しており、これらのキャンペーンがUTA0178と呼ばれる中国国営と思われるグループによるものであるとしています。

同様に、サイバー犯罪の脅威アクターであるMagnet Goblinは、2024年前半にIvanti Connect Secureの3つの脆弱性すべてを悪用し、コードがオンラインで公開されてからわずか1日後にエクスプロイトコードを組み込みました[1、2]。Magnet Goblinは、公開されたIvanti Connect Secure VPNインスタンスを狙い、新しいLinuxバージョンのNerbianRAT、JavaScriptの認証情報スティーラーであるWARPWIRE、Goで記述されたオープンソースのトンネリングツールLigoloなどのマルウェアを配信しました。

Ivanti Connect Secureの脆弱性のその他の悪用には、SkibidiやMiraiなどのボットネットを配布するサイバー犯罪活動、クリプトマイナーのRedTail、バックドアのArcSiltやDSLogが関与する国家支援型アクティビティの可能性などがあります[1、2、3、4]。

脆弱性CVE-2024-21412に関しては、https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html韓国なども標的としているDarkCasino、コモディティローダーのDarkGateの運営者、情報窃取型マルウェアのPhemedroneを配布するサイバー犯罪活動に帰属すると考えられる悪用が見られています。

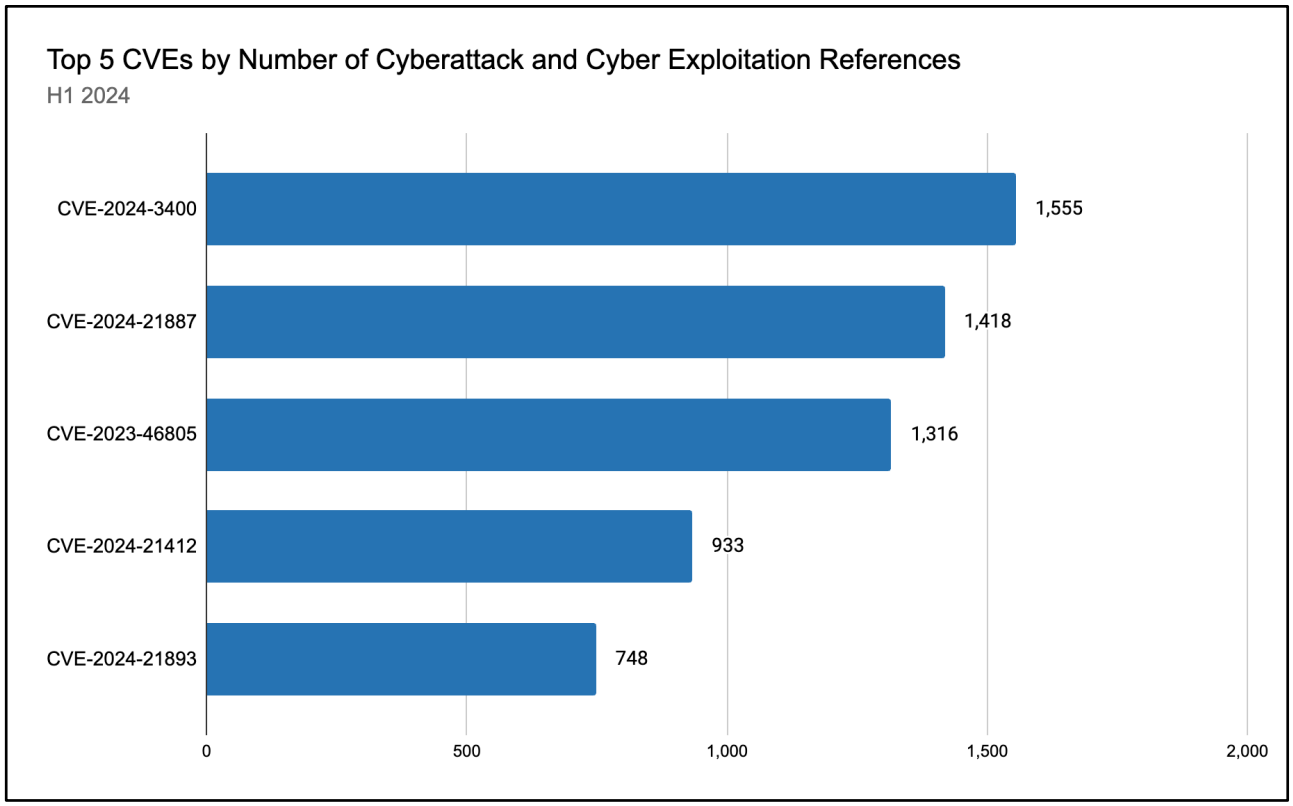

***図1**：2024年上半期のサイバー攻撃とサイバーエクスプロイトに関する言及から見る上位5つの脆弱性（出典：Recorded Future）*

5つの脆弱性が脅威アクターの間で人気を博したことには、悪用の容易さ、エクスプロイトコードの可用性、影響を受けるソフトウェアの広範な採用といった要因がほぼ確実に寄与しています。

- **悪用の容易さ**：米国のNational Vulnerability Database（NVD）や他のベンダーのデータによれば、これらの5つの脆弱性にはすべて攻撃の複雑性が低いという特徴があり、特定の権限を悪用する必要がありません。一例として、Volexityは、CVE-2023-46805とCVE-2024-21887を連携させることで、攻撃者が標的のシステム上でコマンドを実行するのが「きわめて簡単」になると報告しています。

- **PoC（概念実証）エクスプロイトコードの可用性**：PoCエクスプロイトコードは、ゼロデイエクスプロイトとして開示されエビデンスが確認された後、5つの脆弱性すべてで利用可能になりました[1、2、3、4、5、6]。これにより、参入障壁が大幅に低下し、それほど熟練していない脅威アクターでも脆弱なインスタンスを調査して標的にできるようになりました。注目すべき例は前述のMagnet Goblin

です。また、5つの脆弱性とPoCエクスプロイトコードに関連するチャットが、さまざまなアンダーグラウンドやダークウェブのフォーラムやメッセージングプラットフォームで確認されています。

- **影響を受ける製品の幅広さ**：Ivanti Secure Connect、PAN-OS、Microsoft Windows SmartScreenは広く採用されており、脅威アクターが侵害しうる潜在的ターゲットは数千にも上ります。Ivantiの報告によると、Fortune 100企業のうち96社を含む40,000社以上の顧客がIvanti製品を使用しており、当社はCensysを使用してインターネット上で実行されている21,000を超えるIvanti Secure Connectホストを特定することに成功しました。6Senseによると、PAN-OSはPalo Alto Networksの次世代ファイアウォール（NGFW）を支えており、同製品は境界セキュリティ・ファイアウォール市場で8.27%の市場シェアを占めています。Palo Alto Networks自体の報告によると、世界中で85,000社を超える顧客が同社のネットワークセキュリティ製品を使用しています。一方、Microsoft Windows SmartScreenは、対応バージョンのWindowsオペレーティングシステムにデフォルトでインストールされています。また、当社は、脅威アクターが近年、すでにIvanti Secure Connect、PAN-OS、SmartScreenの脆弱性を悪用していることにも注目しています[1、2、3]。

2024年上半期のサイバー攻撃やサイバーエクスプロイト活動で大いに言及されたその他の脆弱性は、SmartScreenやIvanti Connect Secureと同様の性質を持つ他の製品に影響を与えました。このことは、脅威アクターがリモートアクセスやエンタープライズソリューションを好むことを改めて浮き彫りにしています。この主な理由は、こうしたソリューションが広く普及していることと、侵害された後に得られるアクセスのレベルにあると考えられます。これらの追加の脆弱性には以下のようなものがあります。

- CVE-2024-21762：Fortinet FortiOS SSL VPNに影響する重大な領域外書き込みの脆弱性。2024年2月9日CISAは、活発な悪用の証拠に基づいて、この脆弱性を既知の悪用された脆弱性カタログに追加しました。

- CVE-2024-1709：ConnectWise ScreenConnectに影響する重大な認証バイパスの脆弱性で、脅威アクターはこれを悪用してLockBit、BlackBasta、およびBl00Dyランサムウェアを配信しました[1、2]。

- CVE-2024-4577：脅威アクターが悪用してTellYouThePassランサムウェア、Gh0st RAT、RedTail、XMRigクリプトマイナーを配信するために悪用したPHPの重大な脆弱性[1、2]。

- CVE-2024-27198：JetBrains TeamCityに影響する重大な認証バイパスの脆弱性で、脅威アクターはこれを悪用してJasminランサムウェア、XMRig、Cobalt Strike Beacons、SparkRATを配信し、ドメイン検出および永続化コマンドを実行しました。

- CVE-2023-36025：Windows SmartScreen Securityの重大な機能バイパスの脆弱性で、脅威アクターはこれを悪用してMispadu、Phemedrone、Darkgateを配信しました[1、2、3]。

2024年上半期に観測された脆弱性の悪用の傾向は、2023年のInsikt Groupの観測と一部一致しています。ファイル転送ソリューションの脆弱性を含む広範なエクスプロイト活動が繰り返されることはなかったものの（2023年上半期のCL0PのGoAnywhereキャンペーンやMOVEitキャンペーン[1、2]など）、脅威アクターは引き続きリモートアクセスソリューションの脆弱性を狙いました。Recorded Futureの2023年アニュアルレポートで強調されているように、2023年後半には国家が支援するグループとランサムウェアグループの両方がCitrix製品の脆弱性を悪用し、世界中の数百におよぶ組織の侵害に成功しています[1、2、3]。

マルウェアの傾向

2024年上半期のマルウェアの状況は、引き続き情報窃取型マルウェアが非常に大きなシェアを占めていました。より一般的には、マルウェア作成者は、被害者を騙して悪意のあるPowerShellコードを実行させたり、プロセスハロウイングとプロセスドッペルゲンギングを組み合わせたりするなど、分析を妨害し、検出を回避するための新しい手法を導入しました。また、Magecartの侵入の増加も観測されましたが、これはほぼ間違

いなく、eコマースプラットフォームで新たに発見された脆弱性の悪用や新しいeスキマーの登場などの要因によって引き起こされています。

情報窃取型マルウェアが支配的、攻撃的なセキュリティツールがC2検出で上昇

Recorded Future Intelligence Cloudにおけるマルウェアファミリーに関するC2（コマンド&コントロール）検出への言及は、2023年上半期から2024年上半期にかけて顕著な変化を遂げました（**図2**）。Recorded Future Intelligence Cloudは、Recorded Future Malware Intelligenceに提出されたサンプルより抽出したマルウェア構成に基づいてC2サーバーを特定します。

過去1年間では情報窃取型マルウェアが依然として主要なマルウェアカテゴリーとなっています。これは、脅威アクターがクレジットカード情報や暗号資産ウォレットの資格情報などの盗難データを、被害者から直接資金を窃取したり、ダークウェブやアンダーグラウンドマーケットで他の脅威アクターにデータを販売したりすることで収益化できることから、脅威アクターの大多数に金銭的な動機があることが要因と考えられます。このカテゴリーを推進する一部のマルウェアファミリーは、Vidar、RedLine、LokiBot（Windows亜種）など、2023年上半期から2024年上半期にかけて引き続き登場していますが、新たに注目を集めたRiseProなど、今年になってトップ10に入ったファミリーも存在します。最も顕著な進展は、2023年上半期にはトップ10に入らなかったLummaC2が、2024年上半期にはマルウェアファミリーランキングの首位に躍り出たことです。この情報窃取型マルウェアは少なくとも2022年8月から活動していましたが、Insikt Groupは最近、LummaC2が新しいTTPを採用し始めていることを発見しました。具体的には、LummaC2はSteamコミュニティプロファイルのユーザー名を悪用してC2サーバー設定を配布し始めており、この動作は、以前にVidarキャンペーンで観測されています。同時に、2003年に初めて活動が観測されたポリモーフィックボットネットであるSalityの復活は、レガシーマルウェアの継続的な蔓延を浮き彫りにしています。

また、RedLineでC2検出への言及が大幅に減少していることも注目に値します。これは、ESET ResearchとGitHubが協力して2023年4月にRedLineの運用を中断させたことによるものと考えられます。GitHubは、同マルウェアが現在使用しているパネルの認証を破った4つのリポジトリを削除しました。これらのパネルは、新しいサンプルの生成を可能にし、窃取された情報を管理するC2サーバーとして機能していました。

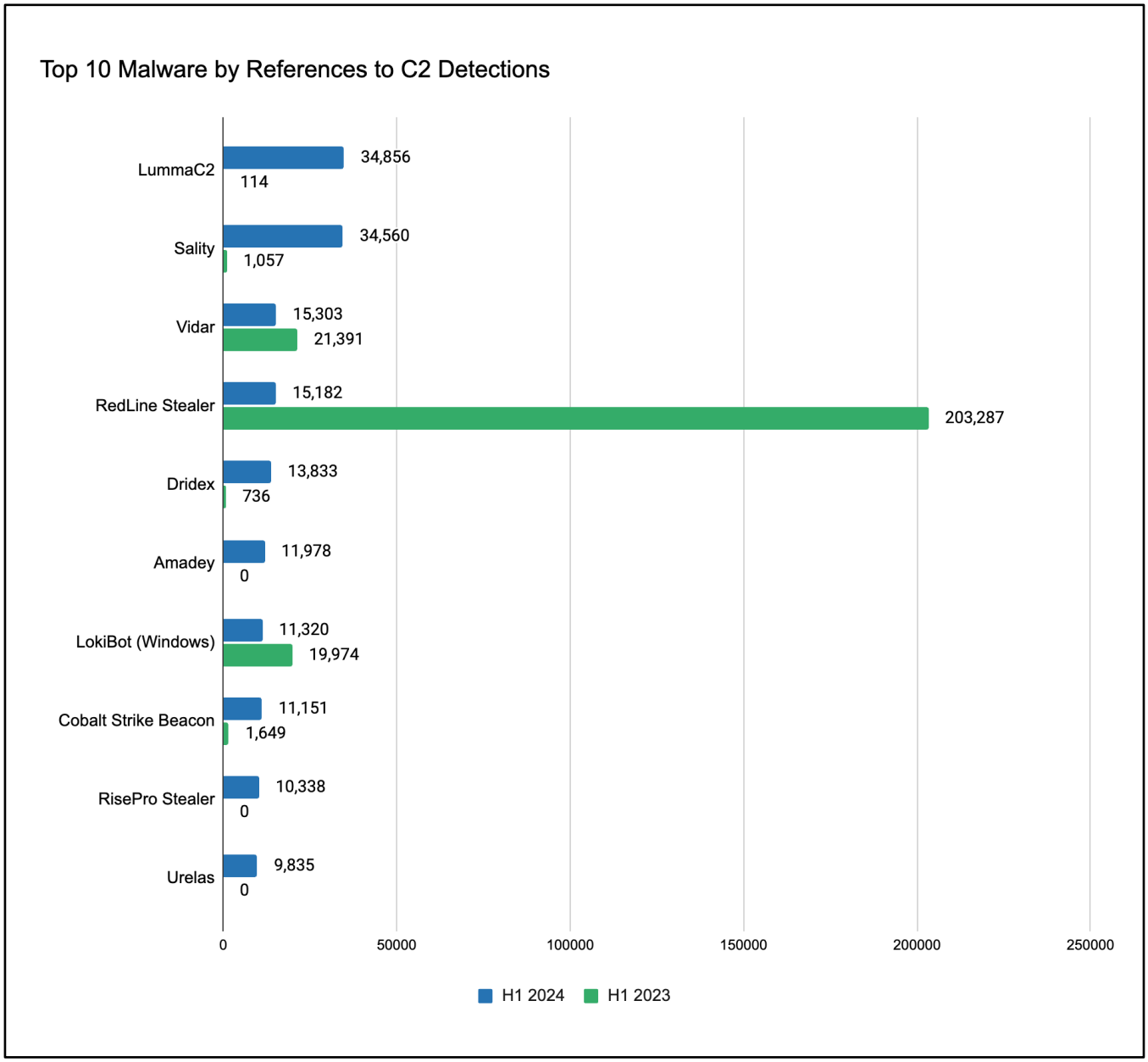

***図2**：2024年上半期と2023年上半期のC2検出での言及数による上位10のマルウェアファミリー*

(出典：Recorded Future)

これらのC2検出におけるのもう一つの新たな傾向は、Cobalt Strikeなどの攻撃的セキュリティツール（OST）の存在感が強まったことです。これらのツールは多くの場合、正当な侵入テスト手段として使われますが、最近のサイバー攻撃への関与からも明らかなように、攻撃者による悪用が一般的になっています。例え

ば、2024年6月、Fortinetは、VBAマクロが埋め込まれたExcelファイルを使用してCobalt Strike Beaconペイロードを配信するキャンペーンについて報告しています。また、 2024年5月にリリースされた動的コード読み込みのカスタムツールであるOdinLdrなど、GitHubで当初公開されたCobalt Strikeフレームワークで使用するよう設計されたオープンソースツールも定期的に観測されています。

分析の妨害に焦点を当てるランサムウェア種

ランサムウェアの状況は、 ALPHVの撤退と、国際的な法執行機関の「Cronos」作戦によるLockBit運営の中断を受けて、2024年前半に全面的な世代交代が進みました。この2つの出来事の後、既存のランサムウェアグループと新しいランサムウェアグループはALPHVの残した穴を埋めるよう動き、LockBitから離脱するアフィリエイトを引きつけました。ただ、こうした変化にもかかわらず、ランサムウェアの能力は2024年初頭からほとんど変わっていません。

当社の観測した顕著な特徴の1つに、Fog、RansomHub、3AMといった3つの新興ランサムウェアが、分析対策としてコマンドの実行を検証するためにパスワードを使用している点が挙げられます。防御目的のパスワードの使用はランサムウェアグループの間では新しい手法ではありません。LockBit 3.0は、2022年7月以降、パスワードを使用して分析を妨害しており、ALPHVとKnightの両方のランサムウェアもこの手法を使用していることが観測されています。とはいえ、Fog、RansomHub、3AMが分析を妨害するためにパスワードを使用していることは、この手法の継続的な人気と有効性とを物語っているといえます。

- Fogは2024年5月上旬に初めて観測されました [1、2]。Recorded FutureによるFogランサムウェアサンプルの静的分析では、実行にパスワードが必要であることが示されました。

- RansomHubは2024年2月に登場し、マルチプラットフォームRaaSとして急速に注目を集めました。Insikt Groupによるランサムウェア分析により、RansomHub Windows、Linux、ESXiのバージョンでは、ランサムウェアの実行時に-pass引数を指定する必要があることが明らかになりました。指定されたこの値は埋め込み構成の暗号化を解除し、その特定のRansomHubサンプルの手順を提供します。間違ったパスワードを指定するとRansomHubサンプルは正しく実行されません。RansomHubはALPHV

やKnightと重複するコードをいくつか共有しており、未確認ではありますが、フォレンジック分析に対する保護手段として、こうしたランサムウェアからパスワード使用を受け継いでいる可能性があります。

- 3AMは2023年9月に初めて観測され、失敗したLockBitランサムウェア攻撃のマルウェアフォールバックとして展開されました。Kasperskyによると、3AMは、サンドボックスの自動実行から保護するための「アクセスキー」機能を実装しています。

2024年上半期に観察されたもう一つの傾向は、マルウェアローダーとランサムウェアの組み合わせです。2024年6月26日現在のRecorded FutureのCollective Insightsデータを確認した結果、最終的にLockBitの展開につながるGuLoaderとRemcosが関与する攻撃チェーンが特定されました。GuLoaderは2019年に初めて観測された洗練されたローダーで、さまざまなマルウェアを配信する堅牢な回避技術で知られています。これらのマルウェアには、Remcosの他、Formbook、XLoader、404Keylogger、Lokibot、Agent Tesla、Nanocore、Netwireが含まれます。一方、RemcosはコモディティRATであり、2016年後半に犯罪フォーラムで販売されていることが最初に確認されています。

この攻撃チェーンはGuLoaderを配信するフィッシングメールから始まり、GuLoaderがRemcosを取得して実行し、システムを制御できるようにしました。このアクセスは最終的にLockBitランサムウェアのインストールに使用され、身代金を要求する前にデータを盗んで暗号化する二重恐喝戦術が利用されました。Recorded Futureは、2024年6月26日までの90日間にGuLoaderとRemcosが一緒に使用された約100件の事例を記録しており、この攻撃シーケンスの蔓延が進んでいることを強調する結果となっています。

トロイの木馬、情報窃取型マルウェア、ローダーが新たな防御回避技術を導入

ランサムウェア種に関する当社の観測に並行して、2024年上半期、トロイの木馬、情報窃取型マルウェア、ローダーなどのマルウェアは、防御回避能力の向上に広く注力しました。Raspberry Robin、SocGholish、HijackLoaderなどのマルウェアは、新しいアンチエミュレーション、実行、プロセスハロウイング技術を実

装することにより、セキュリティソリューションの回避を試みました。また、ClearFake、RedLine、Coyoteは、あまり人気のないプログラミング言語やソフトウェアツールを使用した新しい配信手法を実験しました。

- 2024年5月、ReliaQuestは、ClearFakeを配布するフィッシングキャンペーンを報告しました。これは、提供されたPowerShellコードを被害者にWindowsターミナルに手動でコピーするように促し、その後このコードが自動実行されるというものです。ClearFakeは通常、ドライブバイダウンロードや偽のブラウザ更新通知を介して拡散されるJavaScriptフレームワークです。この新しい実行手法は、疑わしい親子プロセス関係、悪意のあるファイルのダウンロード、Mark-of-the-Webシグネチャなどの検出を回避しています。

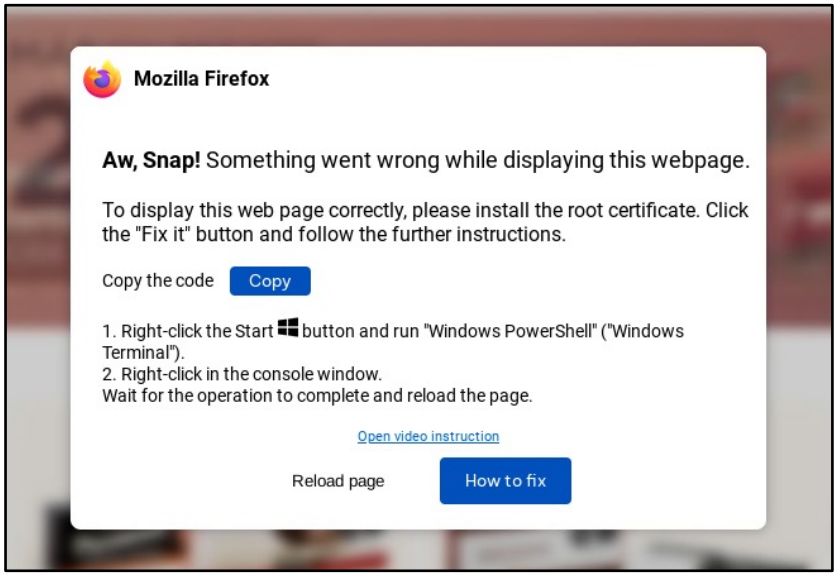

***図3**：ClearFakeのキャンペーンで被害者に悪意のあるPowerShellコードをコピーするように促すフィッシングメッセージ（出典：ReliaQuest）*

- 2024年4月、HarfangLabは、新しいRaspberry Robinの亜種がエミュレーションとサンドボックス環境を防ぐためにVDLL（仮想ダイナミックリンクライブラリ）固有の関数インポートを使用した最初のマルウェアであると報告しました。VDLLはエミュレータ環境内にのみ存在する標準のWindows DLLファイルの変更バージョンです。Raspberry Robinは、エミュレータにのみ存在することが判明している関数を動的にインポートしようとします。このインポートが成功し、サンドボックスの存在が示され

ると、Raspberry Robinは終了します。Raspberry Robinは2021年に初めて特定され、CL0P、Evil Corp、FIN11、TA505などのサイバー犯罪者と関連付けられてきました[1、2]。

- 2024年4月、McAfeeは、Luaバイトコードを使用するRedLineの新たな亜種を確認したと報告しました。攻撃者は、Microsoftの公式GitHubアカウントのvcpkghttps://github.com/microsoft/vcpkgリポジトリでホストされているZIPファイル経由でRedLineを配信しました。このMSIファイルをクリックして実行すると、compiler.exeを（Luaバイトコードのreadme.txtを引数として）実行する予定タスクが作成されます。Luaはあまり一般的ではないプログラミング言語であり、セキュリティツールにはこの分析のための機能が欠けていることがよくあります。脅威アクターはこれを利用して、悪意のある文字列を難読化し、検出を回避しました。

- 2024年2月、ReliaQuestは、少なくとも2018年初頭から活動し、TA569およびEvilCorpと関連するマルウェアで、Pythonを永続化と防御回避の目的で侵害対象の環境に導入するSocGholishの新たな亜種を観測しました[1、2]。この新たな亜種は、悪意のあるPythonスクリプト（hklib.py）を5分ごとに実行する予定タスク（pypi-py）を作成し、スクリプトが継続的に実行されるようにするものです。このSocGholishの亜種は、実行を隠すため、コンソールウィンドウを表示しないPythonインタプリタであるpythonw.exeも採用しています。

- 2024年2月、Kasperskyは、ブラジルのサイバー犯罪者によって開発されたと思われるCoyoteと呼ばれる新しいバンキング型トロイの木馬をプロファイリングしました。このトロイの木馬は、Windowsアプリケーションをインストール・更新するための比較的新しいツールであるSquirrelを、通常のMSIインストーラーではなく感染チェーンで使用しています。Squirrelを使用することで、Coyoteは初期段階のローダーをアップデートパッケージャーとして隠すことに成功し、さらに検出を回避するため、Node.jsとNIMで記述されたローダーを組み合わせ、難読化されたJavaScriptとその最終ペイロードを実行しました。

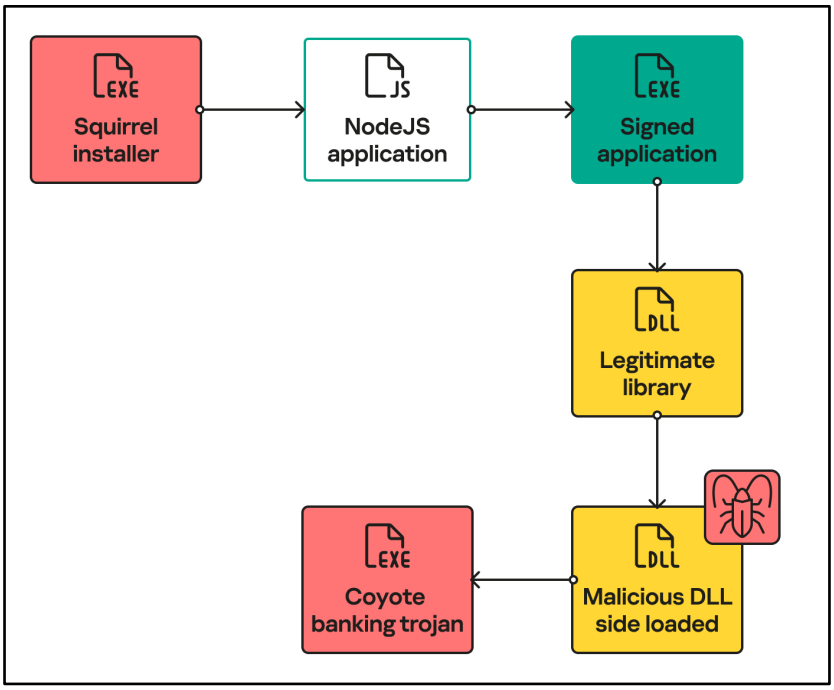

***図4**：Coyoteの感染チェーンの概要（出典：Kaspersky）*

- 2024年2月、CrowdStrikeは、HijackLoaderがプロセスハロウイングとプロセスドッペルゲンギングを組み合わせて防御回避能力を拡大したことに言及しました。これには、パイプを使用して入力/出力をリダイレクトしたり、mshtml.dllなどのロードされたDLLの.textセクションをシェルコードで変更したり、Heaven's GateやTransacted Sectionハロウイングなどの手法を活用して、cmd.exeやlogagent.exeなどのターゲットプロセスに悪意のあるペイロードを密かに挿入して実行したりする行為が含まれていました。HijackLoaderは2023年9月に初めて記録され、DanaBot、SystemBC、RedLineを配信しています。

Magecartの感染は2024年上半期に増加

2023年下半期と比較し、Magecartの感染は2024年上半期に大幅に増加しました。Recorded FutureのPayment Fraud Intelligenceの証拠によると、2023年上半期から2024年上半期にかけてMagecartの侵入件数が約103%増加したことが確認されました（**図5**）。

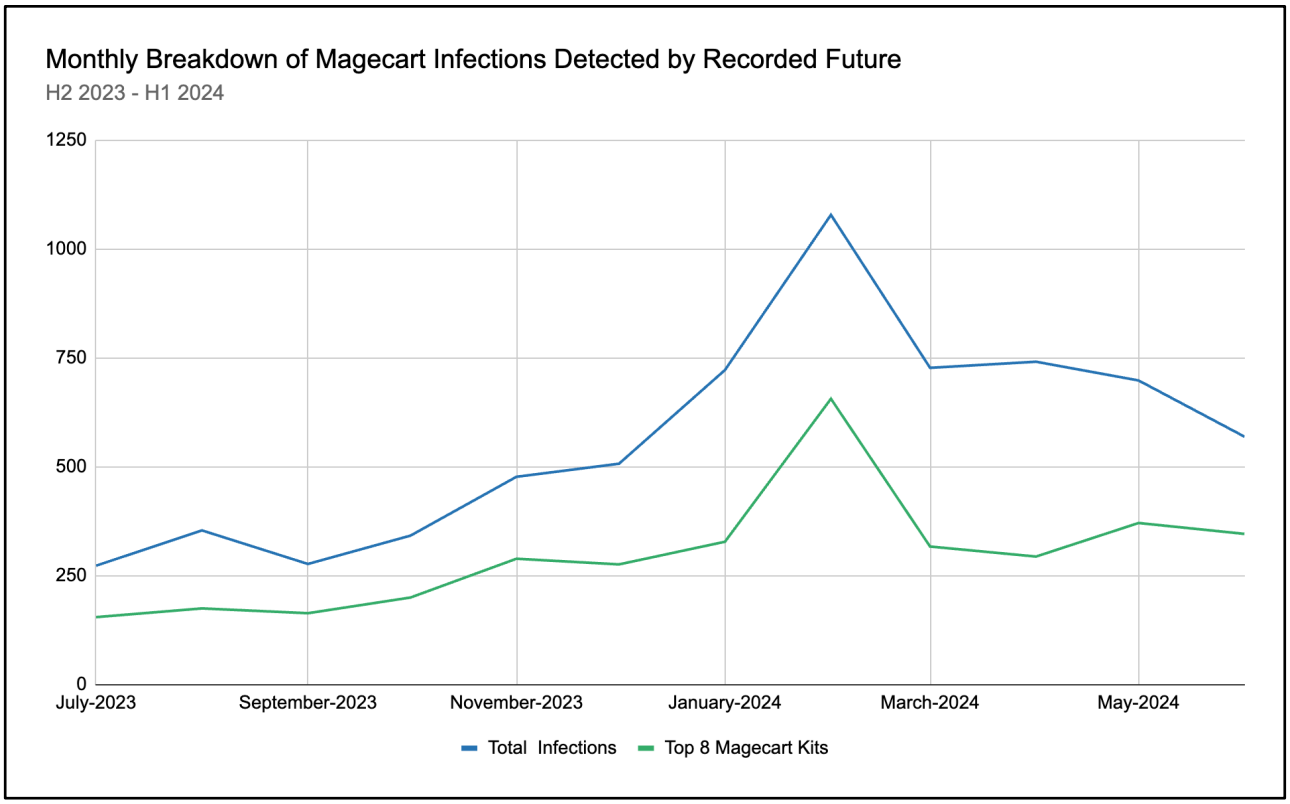

***図5**：2023年下半期から2024年上半期の間にRecorded Futureによって検出されたMagecartの侵入（出典：Recorded Future）*

観測された増加は、Recorded FutureのMagecartスキャナーに新しいIoC（侵害の指標）とeコマースドメインが追加されたことが要因の可能性もありますが、この傾向は他の要因による可能性が高いと評価しています。これには、eコマースプラットフォームに影響を与える新しい脆弱性の悪用や、脅威の状況における新しいMagecartキットの登場などが含まれます。

- 2024年4月、Sansecは報告で、脅威アクターが、2024年2月に開示されたAdobe Commerceに影響する重大な脆弱性CVE-2024-20720に脆弱なMagentoウェブサイトを狙い、偽のStripe決済スキマーに感染させているとしました。

- 2024年3月、Insikt Groupは、XSSとExploitの主要フォーラムのメンバーであり、感染したデバイス上のネットワークトラフィックとユーザー入力を傍受できる使いやすさが売りのスニファーマルウェア（別名「Sniffer By Fleras」）を1,500ドルで宣伝する「fleras」を特定しました。2024年3月から7月

にかけて、この脅威アクターはSniffer By Flerasを少なくとも488件のeコマースウェブサイトに感染させました。Sniffer By Flerasの最近の検出の増加を以下の**図6**に示します。

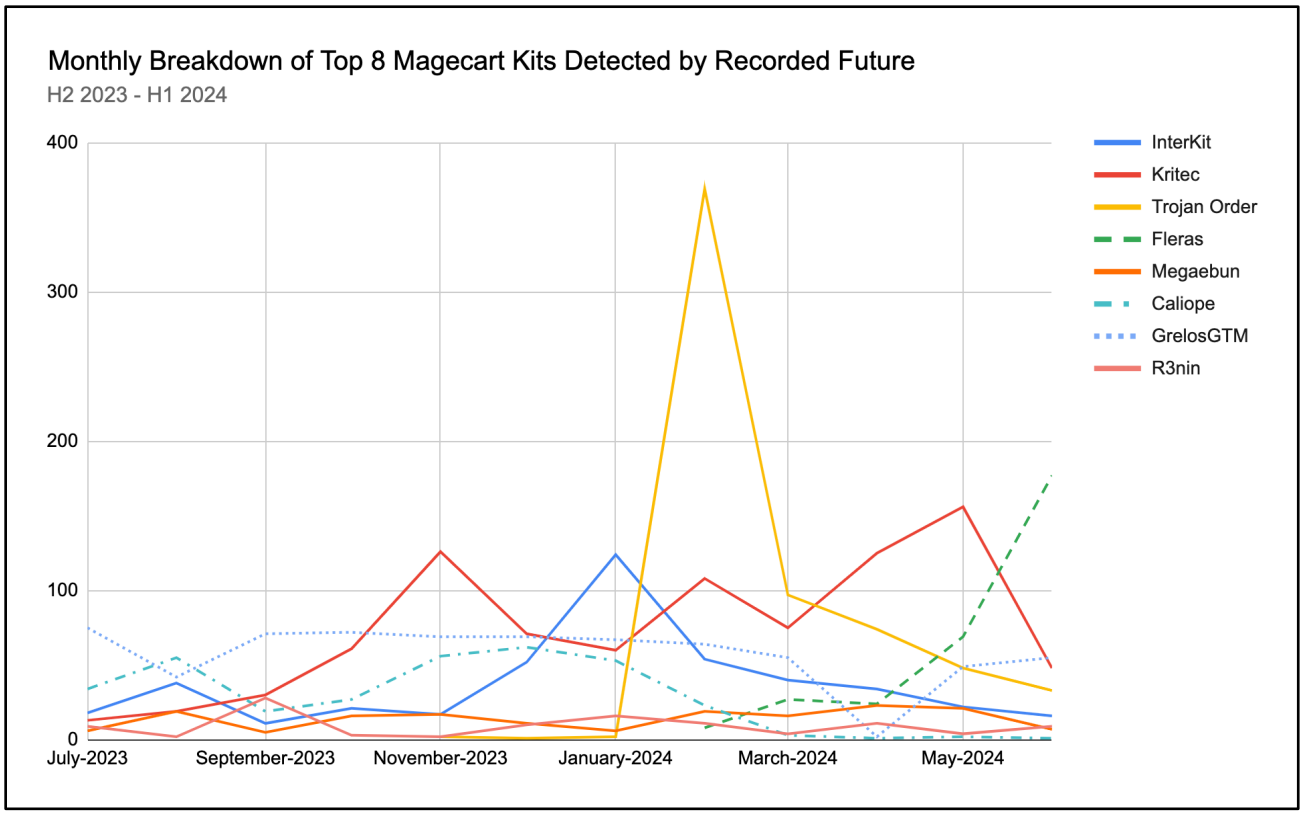

図6：2023年上半期から2024年上半期の間にRecorded Futureで検出された上位8つのMagecartキットに関連する侵入

(出典：Recorded Future)

近年のeスキミングの傾向は比較的一貫しており、サイバー犯罪者が採用する主要なスクリプト方法の進歩はわずかです。しかし、eスキマースクリプトの作成方法やそれらを偽装するための難読化技術などは順調に進歩しています。攻撃者は、eスキマーURLをウェブサイトに直接挿入することを避け、実行時にeスキマーURLの難読化を解除するローダースクリプトを選択しています。eスキマーURLをページに挿入するローダーも段階的に廃止され、eスキマーURLからスクリプトを取得して直接実行するローダーに置き換えられています。クライアント側のスクリプトを埋め込むことができるHTMLタグは、悪意のある攻撃者にとって最適なインジェクションポイントになりつつあります。Magecartの攻撃チェーン内では、Amazon CloudFront、Google Tag Manager（GTM）、Telegram Bot APIなどの無料サービスの悪用が引き続き見られます。これらのサー

ビスは、ローダーやeスキマースクリプトのホスティングに使用され、Telegramの場合は盗まれたデータの受信者として機能します。

軽減策

組織は、本レポートで説明した脅威を軽減するために、次の手段を使用できます。

脆弱性の悪用

- **インベントリスキャン**：包括的なインベントリとテクノロジースタックの定期的なスキャンを実施して使用中のサードパーティソフトウェアを特定し、古い製品やパッチが適用されていない製品の検出を支援します。リモートアクセスやセキュリティソリューションなど、脅威アクターによって最も悪用されるソフトウェアの種類に焦点を当てます。

- **堅牢なパッチ管理サイクル**：定期的なパッチ管理プロセスを確立して、ソフトウェアが迅速に更新されるようにします。ベンダーの一般的なパッチリリーススケジュールを把握し、パッチを効率的に管理・展開するための自動化ツールを実装します。PoCがオンラインで利用可能な脆弱性に対するパッチ適用を迅速化します。

- **Recorded Future Vulnerability Intelligence**：Recorded Futureのお客様はVulnerability Intelligenceを使用して特定のセキュリティニーズに合わせた公私で既知の脆弱性に関するタイムリーで包括的な洞察を得ることができ、修復措置の優先順位付けに役立てられます。

- **Recorded Future Attack Surface Intelligence**：Recorded Future のお客様はExternal Attack Surface Intelligenceを使用してネットワーク資産のリアルタイムの可視性を維持し、エクスポージャーに優先順位を付けて修復し、セキュリティ制御を強制できます。

マルウェアの侵入

- **EDR、ヒューリスティック、行動ベースの分析**：EDRソリューションを通じてヒューリスティック分析と行動ベースの分析を実装し、インタラクティブなプロセスハロウイングやLuaやNIMなどのあまり使用されていないプログラミング言語で書かれたマルウェアなど、脅威アクターのTTPを検出して対応します。

- **アプリケーションの許可リスト作成とスクリプト制御**：アプリケーションの許可リストと実行制御の厳格なポリシーを適用して、不正なスクリプトの実行を防止します。

- **従業員の教育**：新規または更新されたソーシャルエンジニアリングルアーなど、著名なマルウェアが拡散に使用する最新の配信・実行手法について従業員を教育します。

- **Recorded Future Hunting Packages**：Recorded Futureのお客様はInsikt Groupが開発したハンティングパッケージを実装して、著名なマルウェアファミリーに関連する侵入を監視できます。

Magecart攻撃

- **定期的なセキュリティ監査と脆弱性スキャン**：セキュリティ監査と自動脆弱性スキャンを定期的に実施して、eコマースウェブサイトを支えるテクノロジーに影響する脆弱性を特定して修正します。

- **コンテンツセキュリティポリシー（CSP）**：厳格なCSPを導入・更新してeコマースウェブサイトにロードされるリソースを制御し、不正なスクリプトの実行を防ぎます。

- **サードパーティ統合の監視**：eコマースウェブサイトで使用されるすべてのサードパーティスクリプトと統合を頻繁に監査し、保護します。これらの統合へのアクセスを監視・制限して、不正な変更を防止します。

- **PCI-DSS 4.0要件6.4.3コンプライアンスの進歩：**この新しい支払いカード業界標準は2025年3月に実装される予定ですが、早期のコンプライアンス達成を追求することは非常に有益です。マーチャントのウェブサイトで使用されるすべてのスクリプトを検証し、スクリプトに関する変更管理制御を行うことで、Magecartの感染を検出し、感染期間を短縮することができます。

- **Recorded Future Payment Fraud Intelligence**：Recorded Futureのお客様はPayment Fraud Intelligenceを使用して進行中のMagecartのeスキマー感染を監視し、最新のMagecart TTPを常時把握し、予防戦略を強化し、詐欺が発生する前に侵害されたカードに対して措置を講じることができます。

今後の展望

2024年末までの数か月でも、ユビキタスなエンタープライズソフトウェアやリモートアクセスソフトウェアに影響する新たに発見された脆弱性の悪用が、サイバー犯罪者や国家支援型グループに好まれる攻撃ベクトルであり続けることはほぼ間違いありません。これは主に、このような製品は広く普及していることによるものです。コロナ禍以降、企業はリモートワーク人材を維持するためにリモートアクセスソリューションへの依存度を高めました。さらに、次世代ファイアウォール（NGFW）のようなセキュリティソリューションは、セキュリティとコンプライアンスの観点からも広く採用されています。

より一般的な性質の3つの主要な要因が、こうした予測をさらに裏付けています。まず、システムへのパッチ適用は、システムをオフラインにする必要がある複雑なプロセスであることが多いため、企業は脆弱性へのタイムリーなパッチ適用に引き続き苦労しています。Skybox Securityによると、2023年に企業が脆弱性にパッチを適用するのにかかった平均時間は100日を超えています。2023年に脅威アクターが脆弱性の75%を19日以内に悪用したと報告されていることを考えると、これはかなり長い期間といえます。次に、開示・悪用されるゼロデイの数は毎年増加しており、これは主に中国の国家支援型脅威アクター、民間の警備会社の事業慣行、グレーな脆弱性マーケットプレイスによって推進されています。最後に、脅威アクターがPoC（概念実証）エクスプロイトコードの恩恵を受ける傾向が強まっており、Cloudflareが最近提示したエビデンスによると、新たに発見された脆弱性のエクスプロイトコードがオンラインで利用可能になってから22分後に攻撃が発生することが示されています。

マルウェアの開発に関しては、情報窃取型マルウェアが今後数か月にわたって脅威状況で主要な役割を果たし続けると予想しています。情報窃取型マルウェアは認証情報侵害の主因の1つであり、地下経済では非常に貴重な商品であり、後続の悪意のある活動を促進する可能性があります。例えば、2024年4月にKasperskyは、2020年から2023年の間にこうしたマルウェアの被害に遭ったデバイスの数が643%増加したと報告しました。侵害された認証情報に対する需要が根強く、それらを販売できる犯罪フォーラムや市場が存在する限り、情報窃取型マルウェアはほぼ確実に蔓延する脅威であり続けるでしょう。

また、脅威アクターは、ソーシャルエンジニアリングと防御回避能力を継続的に改善し、進化し続けるセキュリティ環境に適応して、感染を確実に成功させることが予測されます。この目的のために、脅威アクターはほぼ確実に、Luaなどのあまり一般的でないクロスプラットフォームプログラミング言語や、防御者やセキュリティソリューションがマルウェア実行チェーンに想定するようになったファイルタイプの代替手段（MSIなど）にますます目を向けるようになります。

最後に、当社では、2024年末までの期間にMagecartの侵入が大幅に減速するとは予想していません。これは、脅威アクターがeコマースプラットフォームで新たに公開された脆弱性を悪用し、新しいeスキマーを利用すると考えられるためです。他のマルウェアタイプの評価と同様に、脅威アクターはMagecart攻撃で新しい配信メカニズムを引き続き実験すると予想されます。脅威アクターは主に、検出の可能性を下げられる限り、ほぼ確実にHTMLタグや正当なサービスを悪用し続けると予想しています。

Recorded　Futureのレポートには、米国インテリジェンスコミュニティー（ICD）203：分析基準（2015年1月2日発行）と一致する可能性のある表現が含まれています。またRecorded Futureのレポートでは、米国インテリジェンスコミュニティーが採用する信頼レベル基準を使用して、分析的判断の裏付けとなる情報源の質と量を評価しています。

*Insikt Group®*について

Recorded Future の脅威研究部門である Insikt Group は、政府、法執行機関、軍、諜報機関に深い経験を持つアナリストとセキュリティ研究者で構成されています。彼らの使命は、クライアントのリスクを軽減し、具体的な成果を実現し、ビジネスの中断を防ぐインテリジェンスを生み出すことです。

*Recorded Future®*について

Recorded Futureは世界最大規模のインテリジェンス企業です。当社のインテリジェンスクラウドは、攻撃者、インフラストラクチャ、標的に関する包括的なインテリジェンスを提供します。オープンウェブ、ダークウェブ、技術ソースにわたってインターネットをインデックス化して、拡大傾向にあるアタックサーフェスと脅威状況をリアルタイムに可視化し、お客様が迅速かつ確信を持ってリスクの軽減と安全なビジネス遂行に取り組めるようにします。ボストン本社および世界各国のオフィスに従業員を擁し、75か国以上で1,800社を超える企業と政府組織と連携して、バイアスのかかっていない実用的なインテリジェンスをリアルタイムで提供しています。

詳細については、recordedfuture.comをご覧ください。