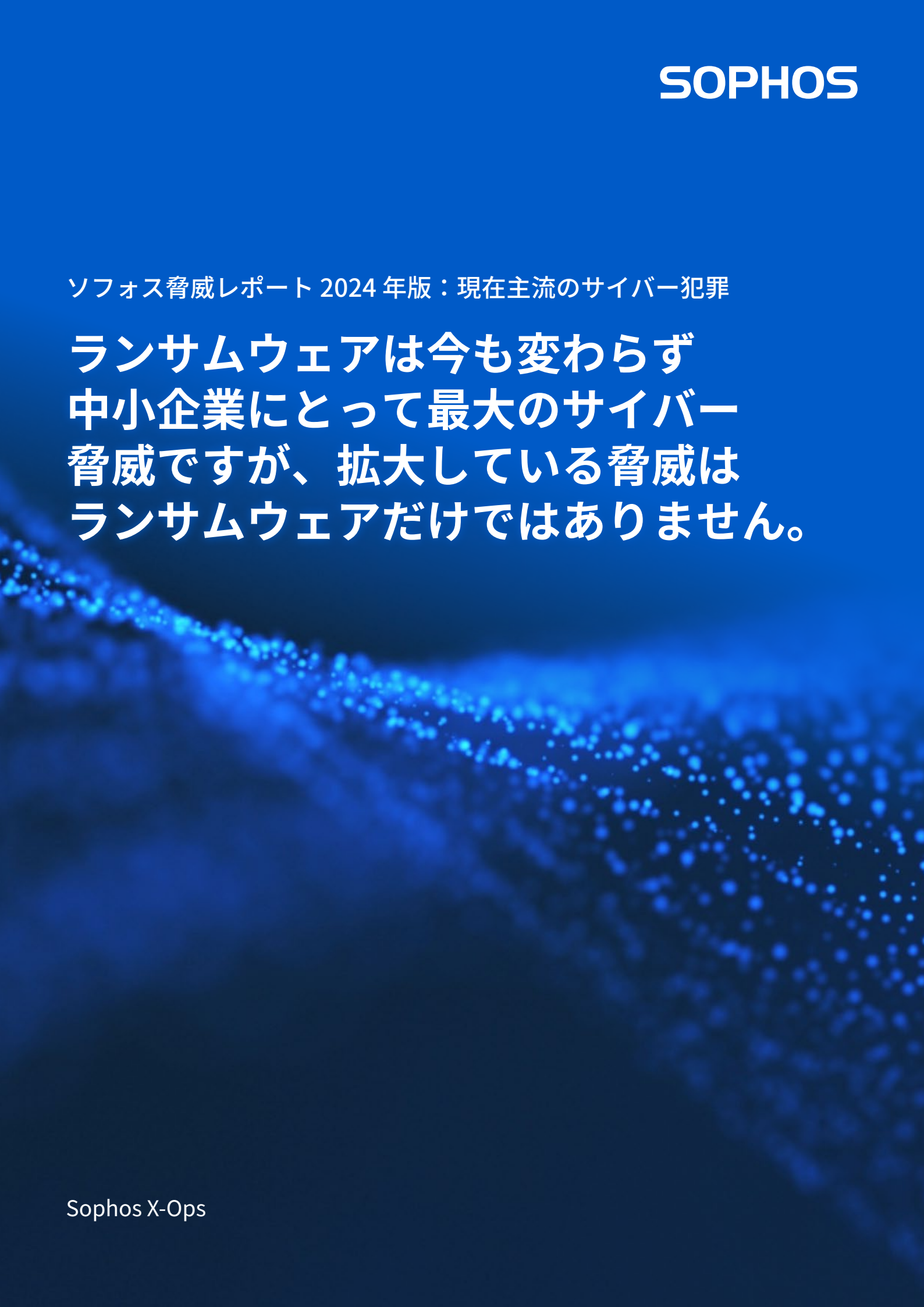
SOPHOS

ソフォス脅威レポート 2024 年版：現在主流のサイバー犯罪

ランサムウェアは今も変わらず中小企業にとって最大のサイバー脅威ですが、拡大している脅威はランサムウェアだけではありません。



Sophos X-Ops

目次

背景

サイバー犯罪はあらゆる立場の人々に影響を及ぼし、中でも中小企業が受ける被害は深刻です。大企業や政府機関に対するサイバー攻撃がニュースで大きく取り上げられる一方で、中小企業 (大まかに言って従業員 500 人 未満の組織) の方が一般的にサイバー犯罪に対して脆弱であり、より多くの被害を被っています。経験豊富なセキュリティオペレーションのスタッフが不足していること、サイバーセキュリティへの投資が不十分であること、IT (情報技術) 予算が総じて少ないことなどが、こうした脆弱性の一因となっています。また、サイバー攻撃を受けた場合、復旧費用がかかるために多くの中小企業が廃業に追い込まれることもあります。

中小企業では決して小さな問題ではありません。世界銀行によると、世界の企業の 90% 以上が中小企業であり、雇用の 50% 以上を中小企業が占めています。米国では、中小企業が経済活動全体に占める割合は 40% 以上に及びます。(本レポートでは、データ上の類似性を踏まえ、中小企業 / 組織 (small-sized business) と中堅企業 / 組織 (medium-sized business) という用語を同義で用います。)

2023 年に Sophos X-Ops Incident Response サービスが対応したお客様インシデント対応事例の 75% 以上が中小企業でした。ソフォスの中小企業向け保護ソフトウェアのお客様から収集したテレメトリに加えて、これらの事例から収集したデータからは、中小企業を常に標的としている脅威について独自の知見を得ることができます。

エグゼクティブサマリー

このデータとソフォスの脅威リサーチによると、ランサムウェアは依然として中小企業に非常に大きな影響を及ぼしています。しかし、次のような脅威も中小企業の存続を脅かしています。

- 中小企業を標的とするマルウェアの大半はデータ窃取が中心で、パスワード窃取型マルウェア、キーボードロガー、その他のスパイウェアがマルウェア検出数の約半数を占めます。フィッシングやマルウェアによって認証情報が盗まれると、クラウドプラットフォームやサービスプロバイダーに保管されている中小企業のデータが流出する可能性があります。また、ネットワーク侵害は、その中小企業の顧客企業への攻撃にも利用されます。
- 攻撃者は、マルウェア検出ツールを無効化するためにディスクイメージを使用するだけでなく、不正広告や文書内の不正なマクロがブロックされた場合に生じる問題を解消する目的で、や悪意のある検索エンジン最適化 (「SEO ポイズニング」) を介して、Web ベースのマルウェア配布を強化しています。
- セキュリティソフトウェアがインストールされていない管理対象外のコンピュータ、設定ミスがあるコンピュータ、メーカーによるサポートが終了したソフトウェアを実行しているシステムなど、組織のネットワークに接続している保護されていないデバイスは、中小企業に対するあらゆる種類のサイバー犯罪攻撃の主要な侵入口となっています。
- 攻撃者は、管理対象システム上のマルウェア対策を迂回・無効化するために、企業の脆弱なドライバや、不正に入手された証明書で署名された悪意のあるドライバを利用する傾向が強まっています。
- 電子メールによる攻撃は、以前は単純なソーシャルエンジニアリングでしたが、最近では何度もメールをやり取りして説得力を高める手法を用い、標的ユーザーとより積極的に関わるようになっています。
- サードパーティサービスやソーシャルメディアプラットフォームの悪用するソーシャルエンジニアリングベースの詐欺など、モバイルデバイスのユーザーに対する攻撃が急増しており、個人や中小企業が影響を受けています。この攻撃は、ビジネスメールやクラウドサービスの侵害から、豚の屠殺 (shā zhū pán) 詐欺まで多岐にわたります。

データについて

分析に使用したデータは、以下の情報源から取得したものです。

- カスタマーレポート — お客様のネットワーク上で実行されているソフォスの保護ソフトウェアからの検出テレメトリです。カスタマーレポートでは、検出された後 SophosLabs で分析された脅威に関する概要が記載されます (本レポートでは、これを「Labs データセット」と呼びます)。
- MDR (Managed Detection and Response) のインシデントデータ — MDR のお客様のネットワークで悪意のある活動が検出された場合に、エスカレーションの過程で収集されます (本レポートでは、これを「MDR データセット」と呼びます)。
- インシデント対応チームのデータ — 従業員数 500 人以下の企業で、MDR 保護機能がほとんど、またはまったく導入されていないお客様のネットワーク上のインシデントから収集されたデータ (本レポートでは、これを「IR データセット」と呼びます)。

ソフォスの社外向け IR チームが対応したケース (従業員数 500 名以上の企業のケースを含む) からのみ抽出したデータについては、本レポートの関連出版物である「アクティブアドバーサリーレポート (AAR)」をご覧ください。特に記載のない限り、本レポートの結論は適切な正規化を行った統合データセットに基づいています。

最大の標的はデータ

中小企業に限らず、あらゆる規模の組織が直面するサイバーセキュリティ上の最大の課題は、データ保護です。ランサムウェア攻撃、データ恐喝、不正なリモートアクセス、データ窃取など、ソフォスのお客様から報告される攻撃の 90% 以上は、何らかの方法でデータや認証情報の盗難が関与しています。

サイバー犯罪者が不正利用などの悪意のある目的でメールアカウントを乗っ取るビジネスメール詐欺 (BEC) は、中小企業において大きな問題となっています。現時点では、「アクティブアドバーサリーレポート」で BEC を取り上げていませんが、同レポートの著者らは、2023 年にインシデント対応チームが特定した BEC は、ランサムウェアを除いて他のどのタイプのインシデントよりも多かったと推定しています。

盗まれた認証情報 (ブラウザ Cookie など) は、ビジネスメール詐欺、サードパーティサービス (クラウドベースの財務システムなど) へのアクセス、詐欺などの金銭的利益のために悪用される内部リソースへのアクセスに使用される可能性があります。また、盗まれた認証情報は「アクセスブローカー」を介して、悪用を目論む攻撃者に販売されることもあります。そこでソフォスは、多くの中小企業のネットワークへのアクセスを提供すると主張する闇フォーラムを追跡してきました。

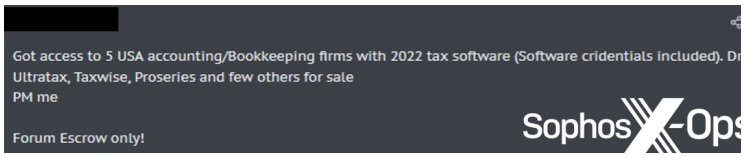


図 1：米国の小規模な会計事務所へのアクセスを宣伝する闇フォーラムの投稿

図 2：ベルギーの中小企業へのアクセスを宣伝する闇フォーラムの投稿

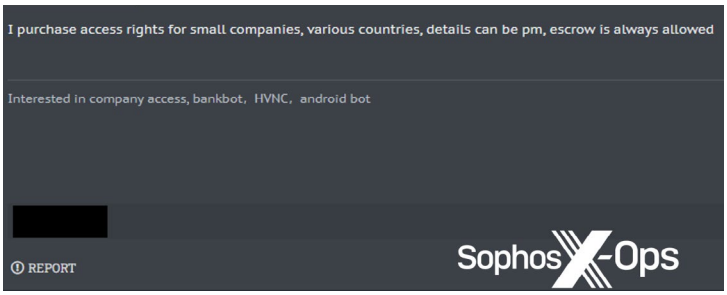


図 3：中小企業へのアクセスを購入するよう持ちかけるサイバー犯罪者

図 4：闇フォーラムで売りに出されたイタリアの中小企業へのアクセス

カテゴリ別に見ると、2023 年に検出されたマルウェアの約半数が、特定の被害者のデータを標的としていました。その大半は、ソフォスが「情報窃取型 (スティーラー)」に分類するマルウェアです。このマルウェアは、認証情報、ブラウザ Cookie、キー入力などのデータを窃取し、そのデータへのアクセス権を売却して現金に換えたり、別の攻撃に利用したりするものです。

しかし、マルウェアはモジュール化されているため、マルウェアを機能別に完全に分類することは困難です (ほぼすべてのマルウェアには、標的システムから何らかのデータを窃取する機能が搭載されています)。また、これらの検出結果には、電子メールやテキストメッセージなどのソーシャルエンジニアリングを介したフィッシング攻撃など、認証情報を窃取するその他の手法は含まれていません。さらに、macOS やモバイルデバイスなど、マルウェア、PUA (迷惑なアプリケーション)、ソーシャルエンジニアリング攻撃によってユーザーデータ、特に金銭的データが狙われるターゲットもあります。

シグネチャのアップデート数を基準に分類されたマルウェア (2023 年)

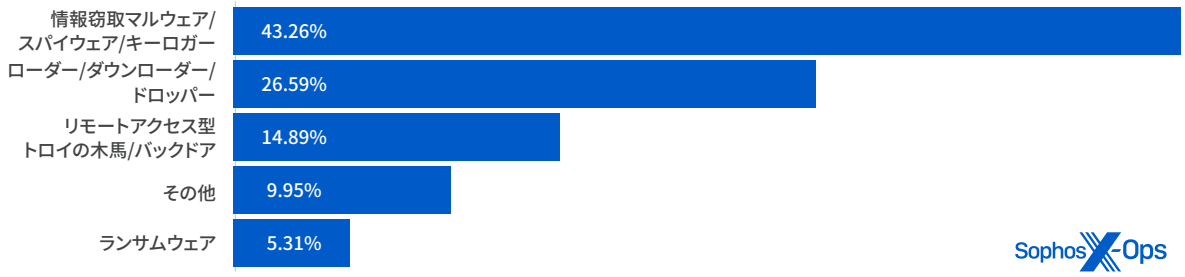


図 5：Labs および MDR データセットに見られる 2023 年のマルウェア検出数 (タイプ別)

検出されたマルウェアの約 10% は、上記の主要な 4 カテゴリに分類されていません。「その他 (Other)」のカテゴリには、ブラウザに広告を挿入したり、検索結果をリダイレクトしてクリック報酬を得たり、データを改ざんまたは収集してマルウェア開発者に利益をもたらしたりするマルウェアなどが含まれます。

情報窃取型マルウェアの中には、標的が非常に限定的なものもあります。Discord の「トークン」を盗むマルウェアは、Discord のメッセージングサービスの認証情報を盗むことを目的としており、多くの場合、チャットサーバーや Discord のコンテンツデリバリネットワークを介して他のマルウェアを配信するために利用されます。しかし、Strela、Raccoon Stealer、そして息の長い RedLine ファミリといった他の主要な情報窃取型マルウェアは、オペレーティングシステムやアプリケーションからパスワードストアを収集するだけでなく、ブラウザ Cookie などの認証情報データを収集するなど、標的をより貪欲に絞っています。Raccoon Stealer にはまた、クリッパーが配備されています。これは、クリップボードにコピーされた暗号通貨ウォレットアドレスを、マルウェアオペレーターが管理するウォレットアドレスと交換する機能です。

2023 年に顧客からの報告件数が上位であった情報窃取マルウェア

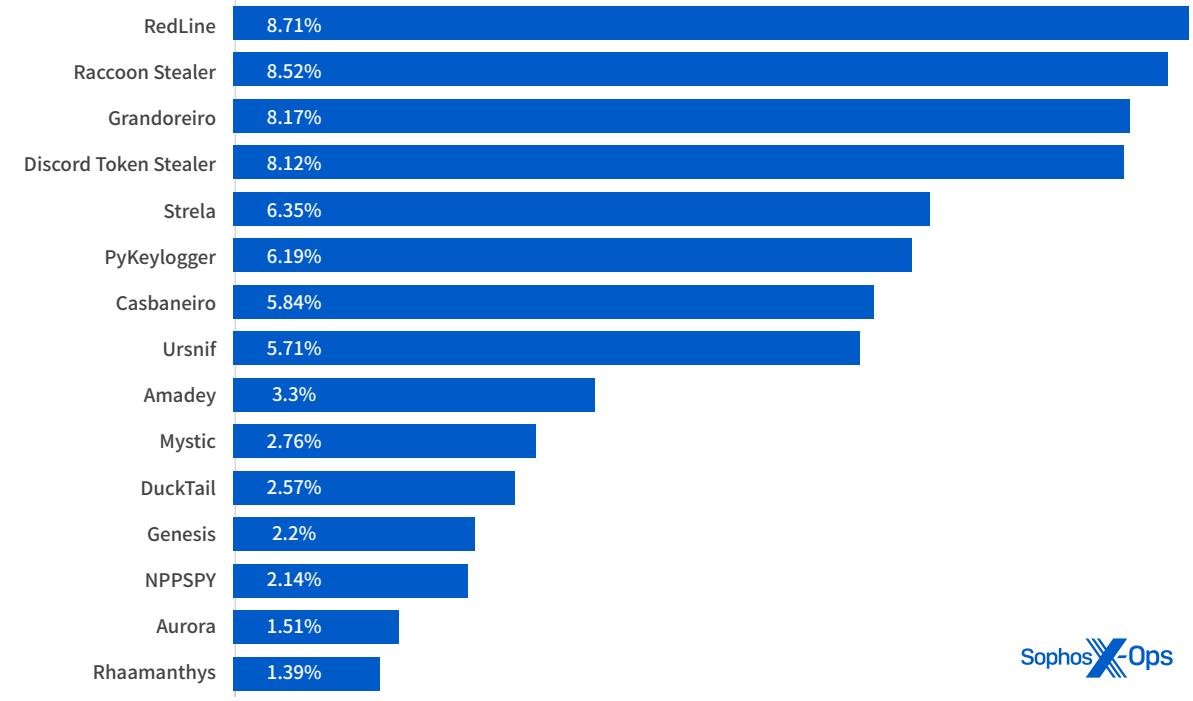


図 6：2023 年における情報窃取マルウェアの検出数 (SophosLabs データセットの顧客テレメトリから抜粋)

ソフォスでは、macOS を標的とした情報窃取マルウェアの増加を確認しており、今後もこの傾向は続くと考えています。これらのマルウェアは、闇フォーラムや Telegram チャンネルで最高 3,000 ドルで販売されており、システムデータ、ブラウザデータ、暗号通貨ウォレットを収集することができます。

中小企業にとって最大の脅威であり続けるランサムウェア

ランサムウェアがマルウェア検出件数全体に占める割合は比較的小さいものの、その影響力は依然として最大です。ランサムウェアはあらゆる業種と規模の企業に影響を及ぼしますが、被害を受ける頻度が最も高いのは中小企業であることがすでに確認されています。2021 年、Institute for Security and Technology 社のランサムウェアタスクフォースは、ランサムウェア攻撃の 70% が中小企業を標的にしていることを明らかにしました。ランサムウェア攻撃の総数は毎年異なりますが、この割合はソフォス独自の指標でも裏付けられています。

LockBit ランサムウェアは、2023 年にソフォスのインシデント対応チームが担当した中小企業のセキュリティ事例で最も多い脅威でした。LockBit は、数多くのアフィリエイトが提供する RaaS (サービスとしてのランサムウェア) であり、2022 年に最も展開されたランサムウェアでした (図 7 参照)。

ソフォスのインシデント対応チームが処理した小規模企業で発生したランサムウェアインシデント (2023 年)

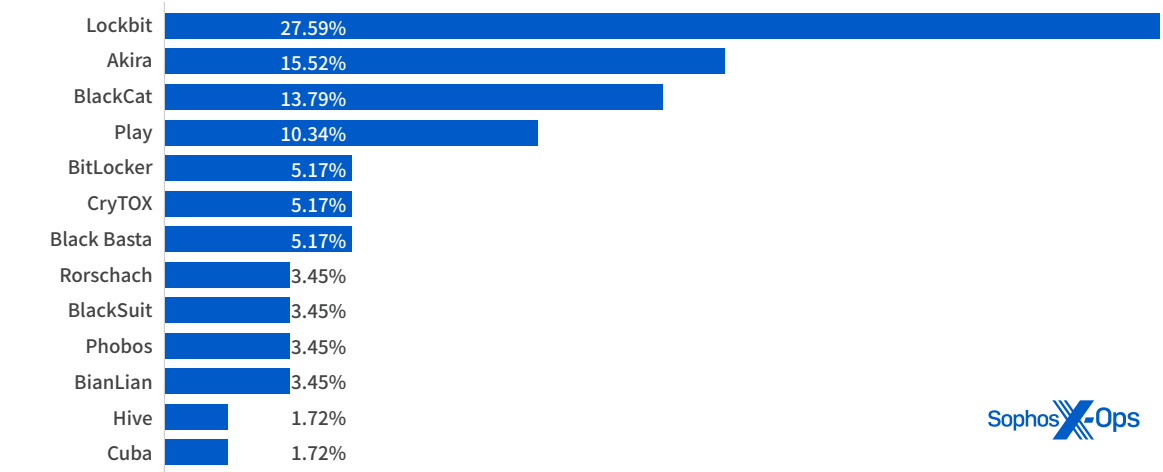


図 7：2023 年にソフォスのインシデント対応 (IR) チームが調査した中小企業のインシデントの背後にあるランサムウェアの内訳。これらの割合は、通常ソフォスの保護機能を導入していなかったお客様における実地調査のデータセットが反映されている

2023 年に顧客からの報告件数が上位 20 のランサムウェア

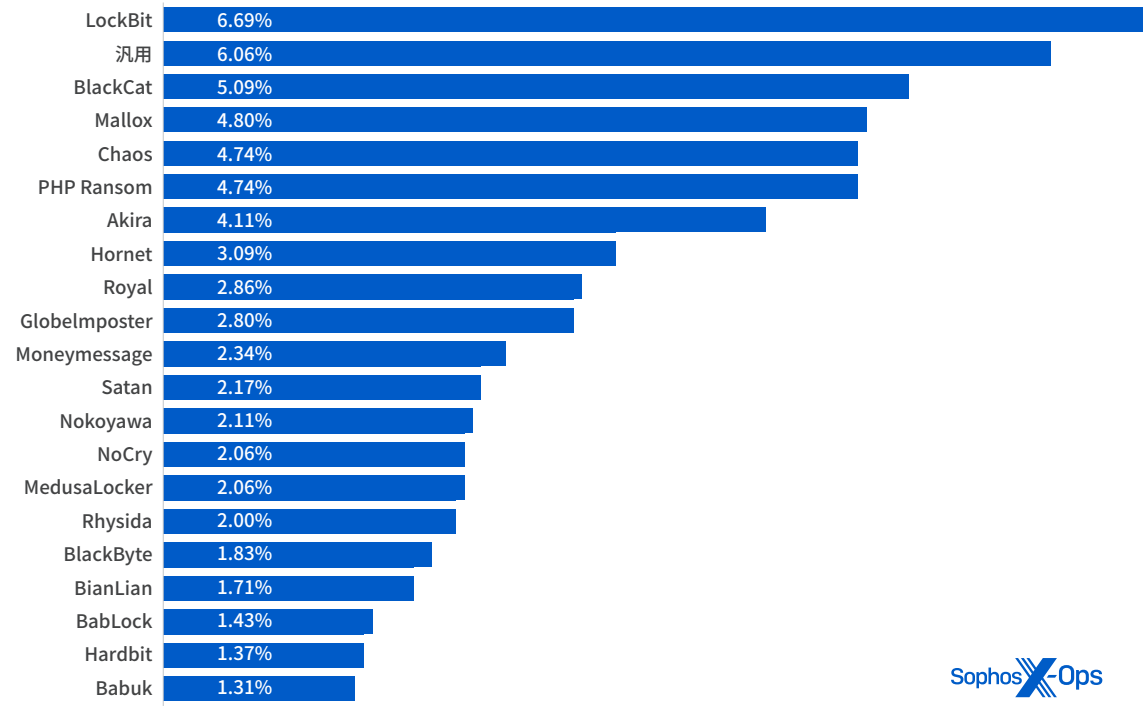


図 8：2023 年に Sophos Endpoint Protection ソフトウェアによって検出され、Labs データセットに存在するランサムウェア展開の試行件数の上位を、検出されたランサムウェア全体に占める割合で示したもの。「Generic」とは、別の定義では検出されなかったが包括的シグネチャで検出されたさまざまな種類のランサムウェアを示す

LockBit は、ソフォスの Managed Detection and Response (MDR) グループ (インシデント対応チームとそのデータを含む) が最も多く確認したマルウェアで、ランサムウェアの展開が試みられたインシデント件数は、同種のランサムウェアである Akira の約 3 倍でした。

2023 年に MDR が担当したインシデントで最も多く確認されたマルウェア (インシデント数別)

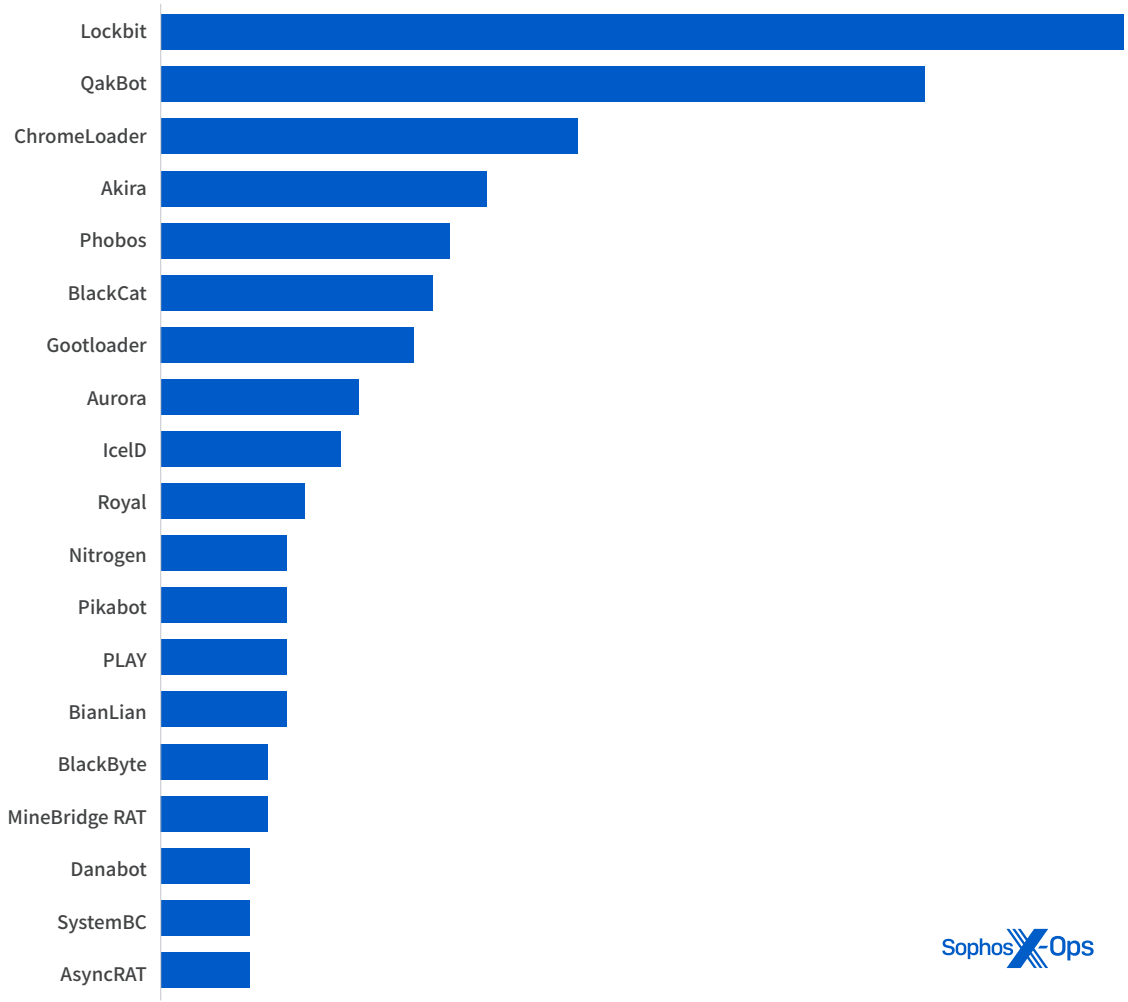


図 9：2023 年に Sophos Managed Detection and Response が担当したインシデントで最も多く確認されたマルウェア (MDR データセットに基づく)。このグラフと図 8 のグラフの違いに注目。2023 年に LockBit が優勢であったことを除けば、多岐にわたるランサムウェアファミリがシステムへの感染を試みていることがわかる。MDR による現場支援を必要とする段階まで進行するのは、そのうちのごく一部。1 件のインシデントで複数検出される可能性がある点に留意。

2023 年に入ると、ランサムウェアのリモート実行 (組織のネットワーク上で管理されていないデバイスを使用し、ネットワークファイルアクセスを通じて他のシステム上のファイルを暗号化する手法) が増加しました。

リモートランサムウェアのインシデント数 (2022 ～ 2023 年)

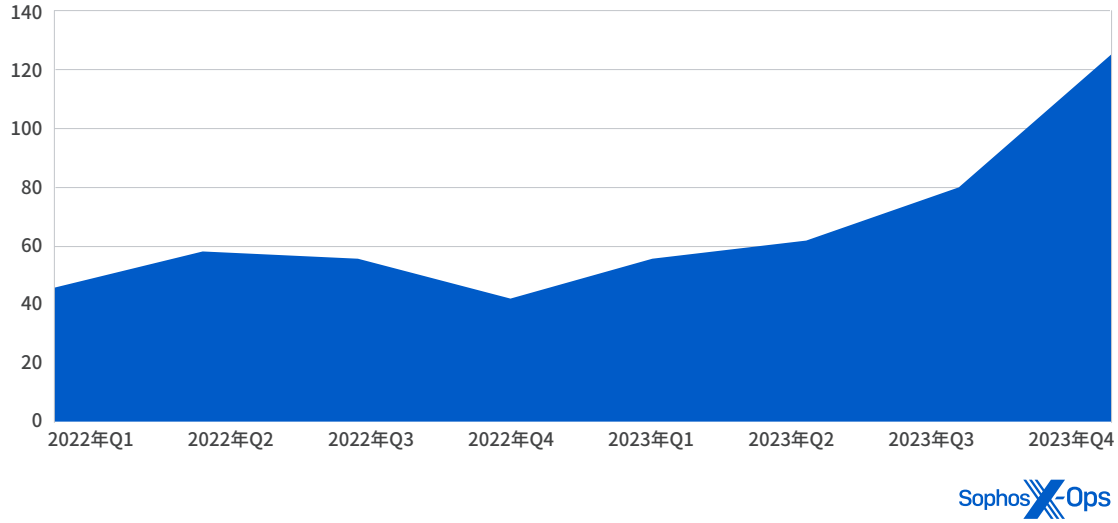


図 10：ソフォスが収集した顧客テレメトリの過去 2 年分のデータでは、リモートランサムウェアが関与しているランサムウェア攻撃 (未遂に終わったもの) の割合が全体的に増加している。リモートランサムウェアは現在進行中の問題であり、2023 年後半には新たな動きを見せている。

この種の攻撃は、組織の Windows ベースのネットワークに接続する無防備なサーバー、個人デバイス、ネットワークアプライアンスを悪用することで、足掛かりを築くことができます。多層防御を導入すれば、こうした攻撃によって組織全体がオフラインになることは防止できますが、データ流出や盗難の被害を受けやすい組織であることに変わりはありません。

ランサムウェアの標的になっているのは Windows システムだけではありません。ランサムウェアなどのマルウェアの開発者は、クロスプラットフォーム言語を使用して、macOS や Linux オペレーティングシステム、および対応するハードウェアプラットフォーム向けのバージョンを開発するケースが増えています。2023 年 2 月には、Cl0p ランサムウェアの Linux バージョンが 2022 年 12 月の攻撃で使用されていたことが確認されました。それ以来、ソフォスは Apple 独自のプロセッサ上の macOS と複数のハードウェアプラットフォーム上の Linux を標的とする LockBit ランサムウェアのリークバージョンを観測しています。

サービスとしてのサイバー犯罪

マルウェアの環境で依然として主流となっているのは、「MaaS (サービスとしてのマルウェア)」です。MaaS とは、サイバー犯罪者が闇マーケットプレイスを通じて他のサイバー犯罪者に提供するマルウェア配信フレームワークです。しかし、プラットフォームセキュリティの向上と、業界や法執行機関による取り締まりが行われたことで、MaaS を取り巻く状況は変化しています。

Emotet は、マルウェア配信ビジネスにおいて 10 年間支配的な地位にありましたが、2021 年 1 月に欧州警察機構 (Europol) と欧州司法当局 (Eurojust) によって取り締まられて以来、その地位は後退しています。また、Emotet 程ではありませんが、2023 年 8 月に法執行機関によって活動を停止させられた Qakbot と Trickbot も同様です。Qakbot は一部復活したものの、その後継者となる Pikabot と DarkGate にほぼ取って代わられましたた。

このいずれも、MaaS 市場のトップに躍り出た息の長いリモートアクセス型トロイの木馬 AgentTesla には影響を与えていません。AgentTesla は、2023 年エンドポイント全体においてエンドポイントプロテクションによって最も多く検出されたマルウェアであり (汎用的な悪意のある .LNK ファイルや難読化されたマルウェアを除く)、2023 年のソフォステレメトリにおけるマルウェア配信フレームワークの検出件数の 51% を占めます。

2023 年に顧客からの報告件数が上位であったマルウェア配信のためのフレームワーク

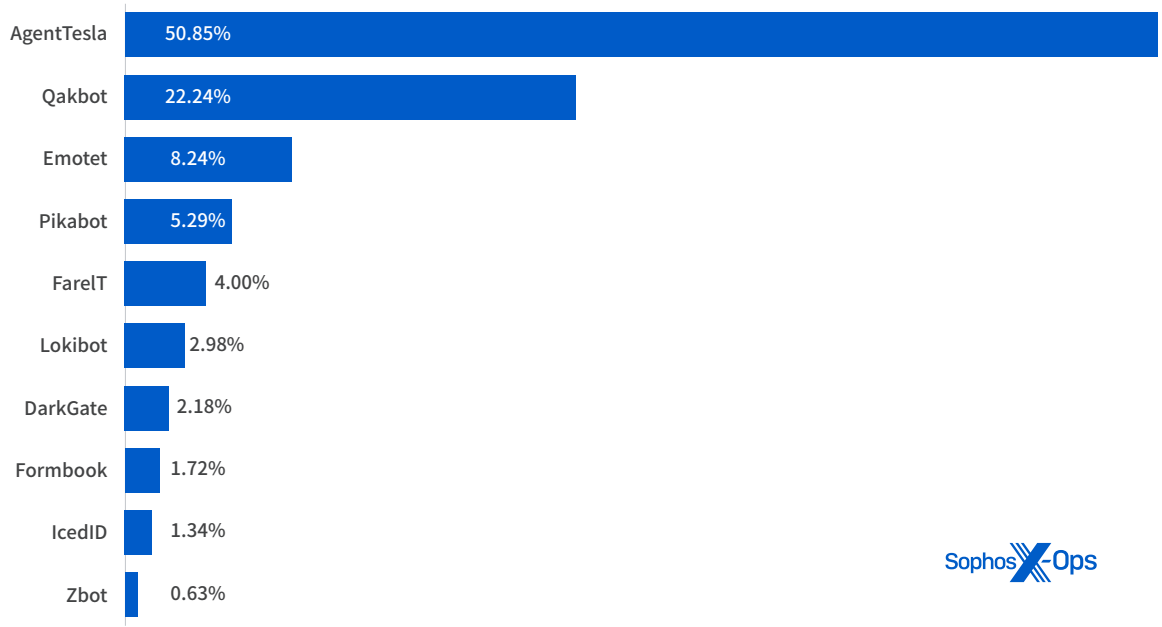


図 11：攻撃者がマルウェアの配信に使用する一般的フレームワークの内訳 (ソフォス製品で保護された顧客ネットワークでのエンドポイント検出数に基づく)。Qakbot の検出数は、そのインフラストラクチャに対する 2023 年 8 月の国際的取り締まり以前の検出数

新たな配信ルート

マルウェア攻撃には、何らかの形での初期アクセスが必要です。通常、次のいずれかを通じて初期アクセスが行われます。

- フィッシングメール
- 悪意のあるメールの添付ファイル
- オペレーティングシステムやアプリケーションの脆弱性の悪用
- 偽のソフトウェアアップデート
- リモートデスクトッププロトコル (RDP) の悪用
- 認証情報窃取

MaaS のオペレーターはこれまで、最初の足がかりを獲得する手段を悪意のある電子メールの添付ファイルに頼ってきました。しかし、Microsoft Office プラットフォームのデフォルトセキュリティが変更されたことの影響は、MaaS 市場にも及んでいます。Microsoft が Office アプリケーションに変更を加え、インターネットからダウンロードされた文書に含まれる Visual Basic for Applications (VBA) マクロをデフォルトでブロックするようになったことで、MaaS オペレーターが好んでいたマルウェア拡散の方法は使用し難くなりました。

そのため、攻撃者が使用する添付ファイルの種類にも変化が見られ、PDF ファイルの添付ファイルへの移行が進んでいます。ただし、注目すべき例外も存在します。Qakbot のオペレーターは 2023 年初め、Excel や Word に加えられた変更を回避するために、悪意のある OneNote 文書を使用するようになりました。この文書には、標的が OneNote ノートブックファイル内のボタンをクリックすると起動するスクリプトファイルへのリンクが隠されていました。

2021 年には、RaccoonStealer バックドアなどの MaaS 製品が Web 配信を利用するようになり (リンク先 : 英語)、検索エンジン最適化 (SEO) を小細工して標的を騙し、マルウェアをダウンロードさせていることをソフォスは指摘しています。2022 年には、SolarMarker の情報窃取キャンペーンの一環として「SEO ポイズニング」が使用されたことが確認されています。このような手口が再び増加しており、より巧妙化しています。

ソフォスは、悪意のある Web 広告や SEO ポイズニングを使用して被害者を狙う注目すべき攻撃キャンペーンをいくつか確認しました。そのうちの 1 つは、ソフォスが「Nitrogen」と名付けたマルウェアを使用した攻撃グループによるものです。このグループは、特定のキーワードに関連付けられた Google や Bing の広告を使用して、正規ソフトウェア開発者のブランドアイデンティティを使った偽サイトからソフトウェアインストーラーをダウンロードするよう標的を誘導していました。ボットネットエージェントの Pikabot 、情報窃取型マルウェアの IcedID、バックドアマルウェアファミリの Gozi など、数多くの初期アクセス用マルウェアに関しても、同じ不正広告手法が使用されています。

Nitrogen の場合、広告の対象ユーザーは IT ジェネラリストであり、エンドユーザーサポート用の有名なリモートデスクトップソフトウェアやセキュアなファイル転送ユーティリティなどのダウンロードを提供していました。このインストーラーは、広告だけでなく悪意のある Python ペイロードも配信しており、インストーラーによって起動されると、Meterpreter リモートシェルと Cobalt Strike ビーコンをダウンロードします。他の研究者らの調査結果によると、これは BlackCat ランサムウェア攻撃の最初のステップである可能性が高いようです。

正規の目的と攻撃の両方に使用される「デュアルユース」ツール

Cobalt Strike は、「攻撃シミュレーション / レッドチームオペレーション」ソフトウェアキットであり、正規のセキュリティテスト組織だけでなく、攻撃者にも使用され続けています。しかし、Cobalt Strike は、攻撃者が使用する唯一の市販ソフトウェアではなく、他にも広くされているものがあります。

リモートデスクトップツール、ファイル圧縮ツール、一般的なファイル転送ソフトウェア、その他ユーティリティ、そしてオープンソースのセキュリティテストツールは、中小企業が使用するのと同じ理由で攻撃者に使用されています。

Sophos MDR では、「デュアルユースツール」と呼ばれる以下のユーティリティが、侵入後のプロセスの一部として攻撃者に悪用されていることを確認しています。

- **探索：**Advanced IP Scanner、NetScan、PCHunter、HRSword
- **永続化 (常駐化)：**Anydesk、ScreenConnect、DWAgent
- **認証情報へのアクセス：**Mimikatz、Veeam Credential Dumper、LaZagne
- **ラテラルムーブメント：**PsExec、Impacket、PuTTy
- **データ収集・持ち出し：**FileZilla、WinSCP、megasync、Rclone、WinRar、7zip

Sophos MDR がインシデントで確認した件数は、Cobalt Strike よりも AnyDesk と PsExec のほうが多くなっています (下図参照)。

2023 年に MDR が担当したインシデントで最も多く確認された「デュアルユースツール」(インシデント数別)

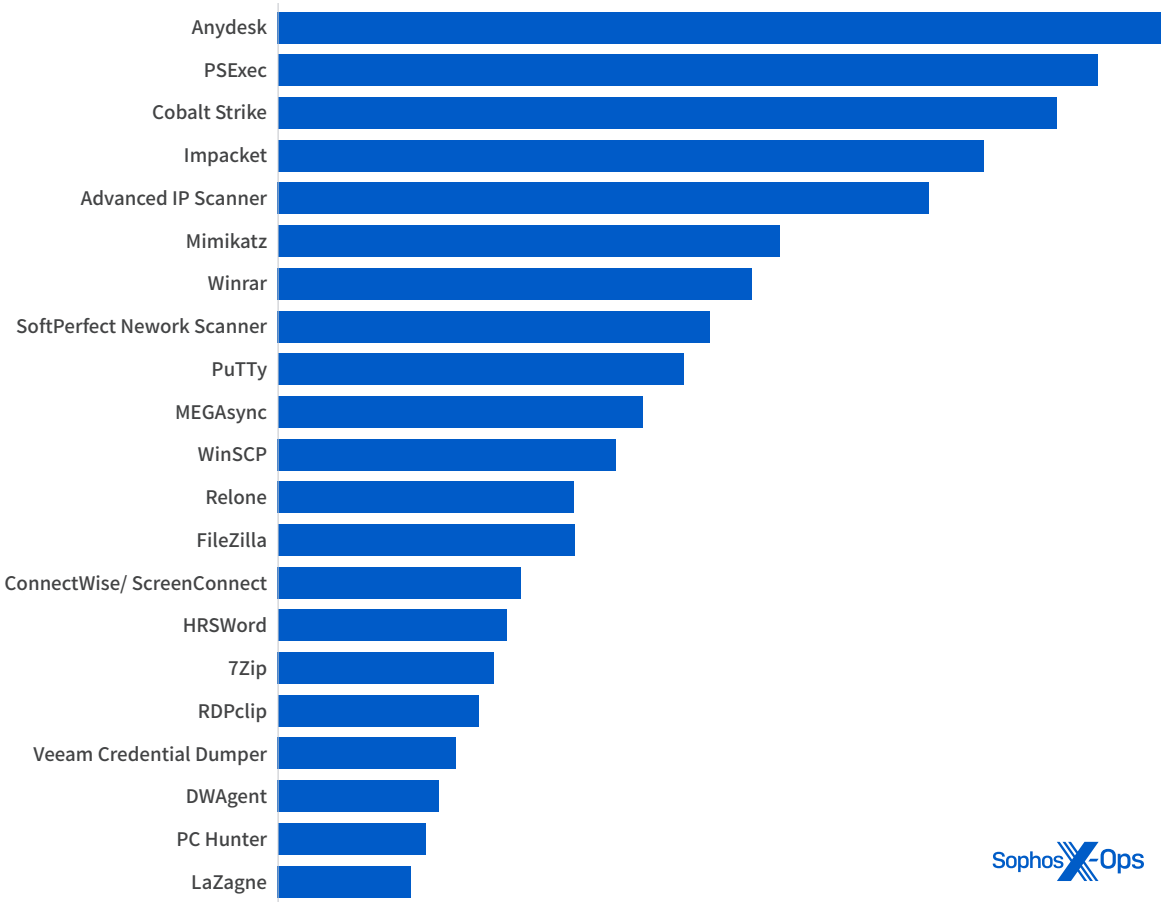


図 12：Sophos MDR データセットで確認された件数に基づき、サイバーセキュリティインシデントで最も頻繁に遭遇した「デュアルユース」ツール

ゼロデイ攻撃と非ゼロデイ攻撃

2023 年 5 月、Progress Software 社は、広く使用されている同社のセキュアマネージドファイル転送プラットフォーム「MOVEit」の脆弱性を報告しました。報告された脆弱性には、少なくとも 1 組の攻撃者が悪用したものが含まれていました。その後、同社は別の脆弱性を複数明らかにし、それらを修正する複数のパッチを公開しました。

この攻撃は、Cl0p ランサムウェアグループと関連のある攻撃者によるものでした。攻撃者らはこの脆弱性を利用して、MOVEit Transfer サーバーの一般向け Web インターフェイスに Web シェルを展開しており、Progress ユーザーによって脆弱性にパッチが適用された後も Web シェルが常駐しているケースもありました。

MOVEit は、2023 年に企業・組織を悩ませた数多くの「ゼロデイ」脆弱性の 1 つに過ぎません。 別のマネージドファイル転送システムである GoAnywhere は、2 月に脆弱性を公表しましたが、この脆弱性の悪用を CL0p 関連の別グループが試みていました。 また、PaperCut MF および PaperCut NG プリントサーバーソフトウェア製品に存在するリモートコード実行の脆弱性は、1 月に開発者に報告された後、3 月と 4 月に Bl00dy ランサムウェアグループに悪用されています。

これらの脆弱性には、パッチを適用できないこともあります。たとえば、6 月に検出された Barracuda Email Security Gateway アプライアンスの脆弱性は、パッチが適用できないほど深刻であり、物理アプライアンスまたは仮想アプライアンスを完全に交換する必要がありました。中国の脅威グループは、2023 年中はそれ以降も脆弱性のあるアプライアンスを悪用し続けました。

攻撃者が利用するソフトウェアやデバイスの脆弱性は、新しいものである必要はありません。パッチが提供されないことを知っている攻撃者は、古いネットワークファイアウォールや Web サーバーソフトウェアなど、サポートが終了したソフトウェアを探し出します。

サプライチェーン攻撃とデジタル署名されたマルウェア

中小企業は、業務や IT インフラストラクチャの管理に利用しているサービスのセキュリティについても常に気に掛けている必要があります。 サプライチェーン攻撃は、国家的攻撃グループだけが実行するものではありません。実際、マネージドサービスプロバイダーに対する攻撃が、ランサムウェアの常套手段となっているのを目の当たりにしてきました。

ソフォスの MDR (Managed Detection and Response) チームは、MSP のリモート監視管理 (RMM) ソフトウェアを悪用する攻撃を受けた中小企業の 5 件のインシデントに対応しています。これらの攻撃者は、標的組織のコンピュータ上で実行されている NetSolutions RMM エージェントを使用して、標的ネットワーク上に新しい管理者アカウントを作成した後、市販のリモートデスクトップツール、ネットワーク探索ツール、ソフトウェアデプロイメントツールを展開しました。うち 2 件の攻撃者は、LockBit ランサムウェアの展開に成功しました。

信頼されているソフトウェアを利用した攻撃、中でもエンドポイント保護を無効にできてしまう攻撃では、防御は困難です。中小企業とそれをサポートするサービスプロバイダーは、アラートに注意を払い、ネットワーク上のシステムでエンドポイント保護がオフになっていないか確認する必要があります。なぜなら、攻撃者がサプライチェーンの脆弱性 (あるいは、一見すると正規のものに思われるソフトウェア) を通じて特権アクセスを獲得したことを示すサインかもしれないからです。

たとえば、2023 年には、攻撃者が有効なデジタル署名が残っている古いソフトウェアの脆弱なカーネルドライバを使用したり、不正に入手したデジタル署名 (Microsoft の Windows Hardware Compatibility Publisher (WHCP) プログラムを通じてデジタル署名された悪意のあるカーネルドライバを含む) を使用して、セキュリティツールによる検出を回避し、マルウェア保護を無効にするコードを実行する悪意のあるソフトウェアを作成したりする事例が多数見られました。

カーネルドライバは、オペレーティングシステム内の非常に下位のレベルで動作し、通常、オペレーティングシステムの起動時に他のソフトウェアよりも先にロードされます。つまり、多くの場合、セキュリティソフトウェアが起動する前に実行されます。デジタル署名は、いわば運転免許証のようなものです。Windows 10 version 1607 以降、Windows の全バージョンでカーネルドライバには有効なデジタル署名が必要となっており、有効なデジタル署名がなければ、セキュアブートが有効になっている Windows オペレーティングシステムではロードされません。

2022 年 12 月、ソフォスは Microsoft に対し、Microsoft の署名入り証明書を持った悪意のあるカーネルドライバを複数発見したことを通知しました。 これらのドライバには Microsoft の署名入り証明書が付属していたため、デフォルトで無害なソフトウェアとして受け入れられ、インストール、およびインストール先のシステムのエンドポイント保護の無効化が可能になりました。Microsoft はセキュリティアドバイザリを発表し、2023 年 7 月には WHCP を通じて取得された数多くの悪意のあるドライバの証明書を取り消しました。

ドライバ自体が不正なものでなくても、悪用される可能性があります。ソフォスはこれまで、旧バージョンだけでなく現行バージョンのソフトウェア製品のドライバやその他のライブラリが、マルウェアをシステムメモリに「サイドロード」しようとする攻撃者に悪用される事例を見てきました。

また、Microsoft のドライバが攻撃に利用されるケースも確認されています。Microsoft の Process Explorer ユーティリティ用ドライバの脆弱なバージョンが、エンドポイントプロテクション製品を無効化しようとするランサムウェアオペレーターによって複数回使用されています。ソフォスが 2023 年 4 月に報告したツール「AuKill」は、このドライバを使用して、Medusa Locker ランサムウェアと LockBit ランサムウェアの展開を試みていました。

脆弱性が存在するドライバが悪用される前に、ソフォスが運良く発見することもあります。7 月には、他社のセキュリティ製品用のドライバのアクティビティによって、ソフォスの動作検知ルールがトリガーされました。 このアラートは、お客様が独自に行った攻撃シミュレーションテストによってトリガーされたものでしたが、このイベントを調査した結果、3 つの脆弱性が発見されました。ソフォスはこれらの脆弱性をソフトウェアベンダーに報告し、その後パッチが適用されました。

スパマー (スパム送信者) が生み出す新たなソーシャルエンジニアリングの手法

暗号化されたエンドツーエンドのモバイルチャットが主流の今、電子メールは古いコミュニケーション手段のように思えるが、スパマーはそのことに気付いていない (あるいは気にしていない) ようです。従業員のふりをして別の従業員にギフトカードの送付を要求するという従来の BEC 手法は根強く残っていますが、スパマーが用いる手法ははるかに独創的になってきています。

この 1 年の間、ソフォスのメッセージングセキュリティチームは、従来の電子メール制御を回避するよう設計された、新しいソーシャルエンジニアリングの手法や技術の数々に遭遇しました。攻撃者が唐突に添付ファイルやリンクを送り付けてくるメールは、もはや過去のものです。より効果を上げているスパマーは、まず会話を始め、その後のフォローアップメールでとどめを刺す傾向があります。

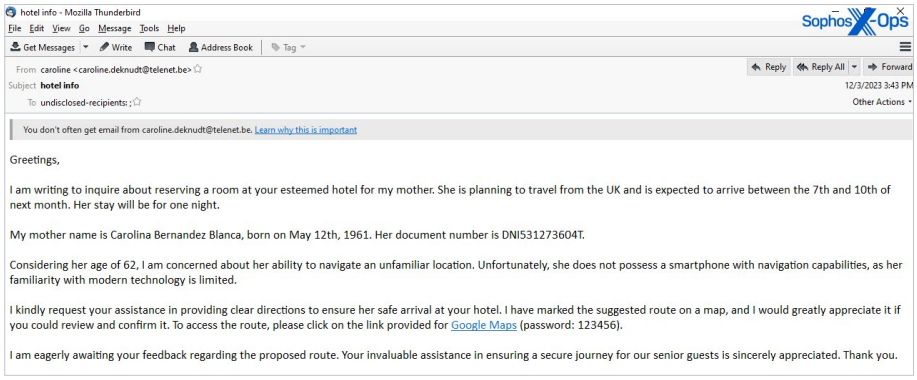


図 13：標的から返信を受け取ったスパマーは、パスワードで保護された Zip アーカイブ内の悪意のあるファイルへのリンクが含まれているメールを標的に送信する

この手法が使用されていた攻撃では、宅配便の配達員を装ったスパマーが企業に電話をかけ、武器化された電子メールを開くよう依頼していました。また、2023 年に幅広い業界を狙った攻撃で、スパマーが最初に勧誘や苦情の電子メールを送信し、その後、企業が最初のメールに返信すると、武器化された偽ファイルをダウンロードさせるためのリンクが送信されることも確認されています。

従来のスパム対策は、メッセージの内容を検査し、その内容に基づいて判断します。スパマーは、メッセージ内のあらゆるテキストコンテンツを埋め込み画像に置き換えるさまざまな方法を試していました。文字で書かれたメッセージが画像になっていることもあれば、検出を回避しようとして、QR コードや請求書のような画像 (攻撃者が被害者に電話をかけるよう促す電話番号が記載されている) を使用する方法も用いられていました。

図 14：スパムメールに添付された PDF ファイルには、不鮮明で読み取れない請求書のサムネイルと、悪意のあるペイロードをホストする Web サイトへのリンクが埋め込まれている

悪意のある添付ファイルはさらに進化し、悪意のあるスクリプトやサイトにリンクしている武器化された PDF ファイルが利用されるようになっています (埋め込まれた QR コードが使用されることもあります)。Qakbot マルウェアファミリは、Microsoft OneNote の文書フォーマットであるノートブック (.one ファイル) を悪用し、ペイロードを配信していました (同年後半、複数機関が連携した取り締まりにより活動停止)。攻撃者はまた、検出を回避する方法として、Microsoft が Windows App Store 経由でのアプリ配布に使用するアーカイブファイル形式の一種である MSIX ファイル形式にも目を付けました。

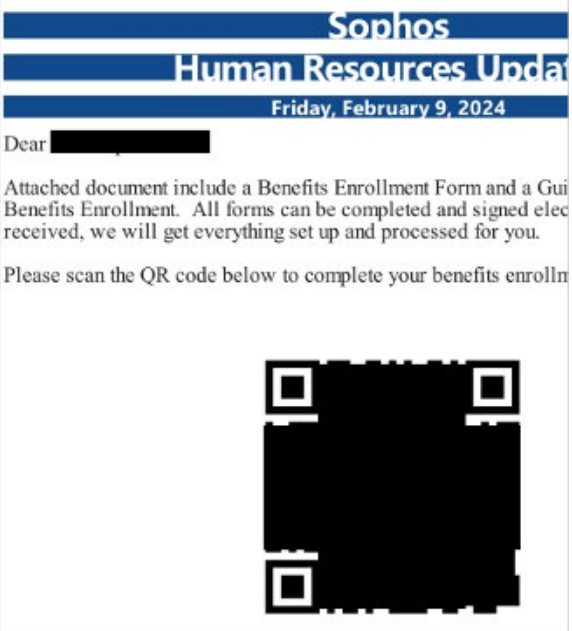


図 15: ソフォスの従業員に電子メールで送信された悪意のある PDF 添付ファイルには、フィッシングページに誘導する QR コード画像が埋め込まれていた

攻撃者は Microsoft のサービスも悪用していました。年末までにソフォスがブロックしたスパムの約 15% は、Microsoft のビジネス向けメッセージングシステム onmicrosoft.com で作成されたメールアカウントを使用して送信されたものでした。

モバイルマルウェアとソーシャルエンジニアリングの脅威

中小企業は、承認された情報システムやアドホックな情報システムの一部として、モバイルデバイスに大きく依存しています。テキストメッセージ、メッセージング / 通信アプリケーション、クラウドサービスに接続するアプリケーション (モバイル POS アプリケーションなど) は、分散型の中小企業にとってミッションクリティカルなシステムです。サイバー犯罪者はそのことを知っており、モバイルデバイスユーザーを標的にして、データへの不正アクセスや詐欺を行う方法を発見し続けています。

スパイウェアおよび金融機関を狙う「バンカー」は、特に懸念されている Android 用マルウェアであり、今後も脅威であり続けると考えられます。スパイウェアは、携帯電話上のデータを収集するために使用されますが、時には金銭的利益を直接得るために、そのデバイスのユーザーをプレミアム料金のサービスに加入させることさえあります。スパイウェアは、感染したデバイスから SMS メッセージや通話ログなどの個人データを抜き取り、詐欺師に売ったり、脅迫に使ったりします。スパイウェアオペレーターから脅迫を受けた末、被害者が自ら命を絶ったケースもいくつかあります。

このような悪意のあるモバイルアプリケーションは、さまざまな方法で配布されています。Google Play のアプリストアやサードパーティのアプリストアのサイトで正規のアプリケーションを装い、モバイル融資アプリケーションとして提供されることもあります。また、テキストメッセージで送信されるリンクを通じて拡散されることもあります。

バンカーとは、暗号通貨ウォレットなどの金融アプリケーションを標的として、資金にアクセスする目的で口座データを採取するマルウェアで、機密データへのアクセスにはアクセシビリティ許可を使用します。

そして、「豚の屠殺」(Sha zhu pan) という仮想通貨詐欺も流行しています。ソフォスは、2021 年初めに「CryptoRom (暗号通貨恋愛詐欺)」と名付けた詐欺と関連がある、iOS と Android 両プラットフォーム上の偽アプリケーションを追跡し始めたが、それ以降、CryptoRom 詐欺はますます巧妙化しています。

Sha zhu pan 詐欺組織は、実質的にその犯罪に誘拐された人々が配置されている施設で運営されることが多く、世界中の被害者から奪った金額は数十億ドルに上ります。また、多くの場合、標的となるのは中小企業と関わりのある人々です。2023 年、カンザス州の小さな銀行が経営破綻し、米連邦預金保険公社 (FDIC) に差し押さえられました。これは、この銀行の CEO が、Sha zhu pan 詐欺で奪われたとされる資金を取り戻すために、預金から 1,200 万ドル以上を詐欺師に送金したために起こりました。この悲劇的な事件が示しているのは、標的の私生活に関わる詐欺が、中小企業にどれだけ影響を及ぼすかということです。

Sha zhu pan 詐欺の実行者たちは、ソーシャルメディアサイトや出会い系アプリ、その他アプリやコミュニティプラットフォーム、さらにはうっかり反応してしまった SMS メッセージを通じて、被害者を誘い出します。このような詐欺師は、ロマンチックなつながりや友情を求めている人を標的にする傾向があります。まず、標的を WhatsApp や Telegram のような安全なメッセージングアプリに移動させてから、信頼を獲得し、内部情報を持っているとする金儲けのアイデア (通常は暗号通貨に関するもの) を紹介します。

この 1 年間で、Sha zhu pan 詐欺に使われる偽アプリが Google Play や iOS アプリストアに出回っています。こうした偽アプリは、審査プロセスが終了するまでは無害なアプリを装ってストアのセキュリティ審査を回避し、その後、リモートコンテンツを変更して偽の暗号取引アプリに変身します。アプリを通じて入金された暗号通貨は、即座に詐欺師の懐に入ります。

最近では、偽アプリを必要としない別のタイプの暗号通貨詐欺の手口も確認されています。それは、偽アプリの代わりに、暗号通貨ウォレットのモバイルアプリの「Web3」機能を使い、被害者が作成したウォレットにアクセスする方法です。ソフォスは、こうした「DeFi (分散型金融) マイニング」の亜種である Sha zhu pan と関連のある数百のドメインを特定し、(偽アプリを特定した場合と同様に) 通報して閉鎖させる作業を続けています。

結論

中小企業が直面する脅威は枚挙にいとまがなく、多くの場合、その高度な技術は大企業や政府機関に対する攻撃で使われるものと同等です。窃取される金額は大企業に比べれば小さいものの、犯罪者たちは盗めるだけ盗み、金額の小ささを被害者の数で補っています。

犯罪組織は、中小企業の防御力が低く、ユーザーや資産を保護する最新の高度なツールを導入していない状況につけ込んでいます。このような脅威を阻止するには、攻撃者のその思い込みが間違っていることを証明する必要があります。従業員を教育し、外部に面している全資産に多要素認証を導入し、サーバーとネットワークアプライアンスに最優先でパッチを適用し、Microsoft Exchange サーバーのような管理し難い資産を SaaS メールプラットフォームに移行することを検討してください。

ソフォスの経験上、サイバー攻撃の影響が最も大きかった企業と最も小さかかった企業の最大の違いは、対応に要する時間です。セキュリティ専門家が 24 時間 365 日体制で監視・対応することが、2024 年において効果的な防御を行うための必須条件となります。安全な状態を維持することは不可能ではありません。包括的な計画を策定し、何重もの防御策を講じることで、対応する時間を確保し、被害を最小限に抑えることができます。

ソフォス株式会社営業部
Tel: 03-3568-7550
Email：partnersales@sophos.co.jp

24-04-11 JA（NP）

SOPHOS