Digital Security
Progress. Protected.

ESET 脅威レポート

2024 年下半期

2024 年 6 月～ 2024 年 11 月

(eset):research

目次

エグゼクティブサマリー

情報窃取型マルウェア MaaS（サービスとしてのマルウェア）

2 つの窃取型マルウェアについてのストーリー：情報窃取型マルウェアの脅威環境の激変

RedLine Stealer が解体された一方で、Lumma Stealer の検出が急増しています。

情報窃取型マルウェア メールの脅威

Formbook の復活

Formbook が Agent Tesla に代わって、ESET のテレメトリデータで情報窃取型マルウェアの首位に立ちました。

クリプトスティーラー macOS Windows Android

デジタルトレジャーハンター：ビットコインの高騰で活気づくクリプトスティーラー

ビットコインの交換レートが史上最高値を更新したことで、クリプトスティーラーがいずれも増加しました。

Android iOS 金融関連の脅威

アプリか、Web サイトか？モバイルバンキングの認証情報をすばやく窃取する方法

モバイルデバイスを攻撃する新たな手法により、モバイル OS の従来型のセキュリティ対策を回避し、ユーザーを騙して Android や iOS のデバイスを侵害できるようになっています。

Web の脅威 詐欺 ディープフェイク

裕福なセレブと共に投資し、最終的に Nomani に感染

新たな投資詐欺広告がソーシャルメディアのニュースフィードに次々と表示され、偽の動画や有名企業の投稿を使って被害者を騙して金銭やデータを窃取する攻撃が発生しています。

Web の脅威 詐欺 フィッシング

オンラインマーケットプレイスの詐欺が多様化。偽のホテル予約サイトから観光客を騙すケースも

2024 年下半期には、人気の宿泊予約プラットフォームのユーザーを標的にする新たな詐欺が増加しました。攻撃者は、オンラインマーケットプレイスでの詐欺を目的に開発されたツールキットである Telekopye を使用しています。

ランサムウェア

RaaS の勢力争いに明確な勝者：RansomHub

LockBit が 2024 年上半期に解体された後、RaaS（サービスとしてのランサムウェア）市場のトップの座を競う戦いが勃発しています。サイバー攻撃グループ間の関係が変化し、スキルの低いグループがこの市場に参入しています。

序文

2024 年下半期の ESET 脅威レポートをご覧いただきありがとうございます。

2024 年下半期もサイバー犯罪者は防御側との終わりのない戦いを続ける中で、セキュリティの抜け穴や攻撃対象を拡大する革新的な方法を見つけています。新たな攻撃手法やソーシャルエンジニアリングの方法が登場し、ESET のテレメトリ（監視データ）でも新たな脅威が急増した一方で、いくつかの解体作戦（テイクダウン）が実施されたことで、サイバー犯罪のこれまでの順位も大きく変動しました。

情報窃取型マルウェアは、順位が大きく変動したカテゴリの 1 つであり、その要因は、長期にわたって圧倒的な支配を続けてきた Agent Tesla マルウェアが、さまざまな機密データを窃取するために設計された Formbook マルウェアに首位の座を奪われたためです。Formbook は、発見から 10 年近くが経過したにもかかわらず、MaaS（サービスとしてのマルウェア）モデルの採用と継続的な開発により、多くのさまざまな犯罪者に利用され続けています。

Lumma Stealer は、情報窃取型マルウェアのカテゴリに新たに加わったもう 1 つの MaaS であり、サイバー犯罪者にこれまで以上に利用されるようになっています。2024 年下半期にいくつかの注目すべき悪意のあるキャンペーンで利用され、ESET のテレメトリでは、本レポートの対象期間中に検出数が約 400% 増加しました。RedLine Stealer も、MaaS モデルの情報窃取型マルウェアですが、全く異なる運命を辿りました。2024 年 10 月に国際的な捜査機関によって解体されて、その活動は終焉を迎えたと考えられます。しかし、RedLine Stealer の終焉によって同様の脅威が拡大し、その空白を埋めようとすることも予想されます。

予想通り、2024 年後半に暗号通貨の価値が過去最高を記録したことで、暗号通貨ウォレットのデータが悪意のある攻撃者の主要な標的の 1 つになりました。ESET のテレメトリは、クリプトスティーラーの検出が複数のプラットフォームで増加したことを示しています。注意が必要なのは、macOS で最も顕著な増加が見られ、暗号通貨ウォレットの認証情報を執拗に標的にするいわゆるパスワード窃盗ツールが上半期と比較して 2 倍以上になりました。さらに、銀行アプリや暗号通貨ウォレットを標的にする金融関連の Android の脅威が 20% 増加しました。

Android あるいは iOS のどちらのユーザーも、2024 年下半期に ESET の研究者が分析した新たな攻撃手法に警戒する必要があります。これらの新たな攻撃では、サイバー犯罪者は PWA（プログレッシブ Web アプリ）や WebAPK を利用して、モバイルアプリの従来型のセキュリティ対策を回避します。PWA も WebAPK も、不明なソースからのアプリインストールをユーザーが明示的に許可する必要はないため、銀行の認証情報を窃取する悪意のあるアプリをモバイルユーザーが知らぬ間にインストールしてしまう恐れがあります。そして、モバイルプラットフォームのこれらのテクノロジーへのアプローチが変わらない限り、フィッシングキャンペーンがこれまで以上に高度化および多様化し、PWA や WebAPK を悪用するようになると考えられます。

ソーシャルメディアでは混迷が続いており、ディープフェイク動画や企業ブランドの投稿を使ってユーザーを詐欺投資スキームに誘導する新たな手法が次々と登場しています。ESET が HTML/Nomani として追跡しているこれらの詐欺の検出が本レポートの期間中に 335% 増加しましたが、今後も増加の勢いが鈍化することはないでしょう。

2024 年下半期には、Booking.com や Airbnb などの人気の宿泊予約プラットフォームのユーザーを標的にする新たな詐欺も増加しました。この詐欺は、オンラインのマーケットプレイスの詐欺を目的に最初に開発された Telekopye というツールキットを使用し、正規の宿泊施設プロバイダーの侵害されたアカウントを使って最近宿泊を予約した人を特定し、詐欺目的で作成した支払いページに誘導します。

これまでランサムウェア市場を寡占してきた LockBit が解体されたことで、ランサムウェアの状況が変動し、他のランサムウェアがその空白を埋めることになりました。RansomHub は、2024 年上半期に初めて発見された RaaS（サービスとしてのランサムウェア）ですが、2024 年下半期末までに数百件の被害が発生しており、新たにトップの座を確かなものにしました。

本書が読者の皆様に貴重な知見をもたらすことを願っています。

ESET 脅威検出部門ディレクター
Jiří Kropáč

脅威環境の動向

情報窃取型マルウェア MaaS（サービスとしてのマルウェア）

2 つの情報窃取型マルウェアについてのストーリー：情報窃取型マルウェアの脅威環境の激変

RedLine Stealer が解体された一方で、Lumma Stealer の検出が急増しました。

RedLine Stealer と Lumma Stealer は、過去の ESET 脅威レポートでも何度も取り上げたことがあり、どちらの情報窃取型ツールも MaaS（サービスとしてのマルウェア）モデルを採用しています。

RedLine Stealer は、保存されているクレジットカード情報からローカルの暗号通貨ウォレットまでのさまざまなデータの収集に使用されており、2020 年の発見後に短期間で、ESET テレメトリで最も検出された情報窃取型マルウェアの 1 つになりました。

Lumma Stealer も 2022 年に発見されてから短期間に検出順位を上げ、2024 年下半期に ESET 製品が検出した情報窃盗型マルウェアのトップ 10 に入りました。このマルウェアは、ブラウザの二要素認証拡張機能やユーザー認証情報、さらには、RedLine Stealer と同様に暗号通貨ウォレットなどのさまざまな情報を標的にします。

これら 2 つの情報窃取型マルウェアは、MaaS モデルを採用して多くの犯罪者をその顧客として獲得したことで、当面はその勢力を維持すると思われていました。しかし、Lumma Stealer は存続しましたが、RedLine Stealer は法執行機関によって年末までに解体されています。

国際的な捜査機関によって解体された RedLine Stealer

オランダ国家警察が 2024 年 10 月に実施した Magnus 作戦によって、RedLine Stealer とそのクローンである META Stealer を解体しました。この作戦には、FBI、欧州司法機構、その他の複数の法執行機関も参加しています。この捜査では数人を逮捕し、RedLine Stealer のインフラストラクチャを破壊しただけでなく、RedLine と META の顧客である犯罪者のデータベースも押収しました。

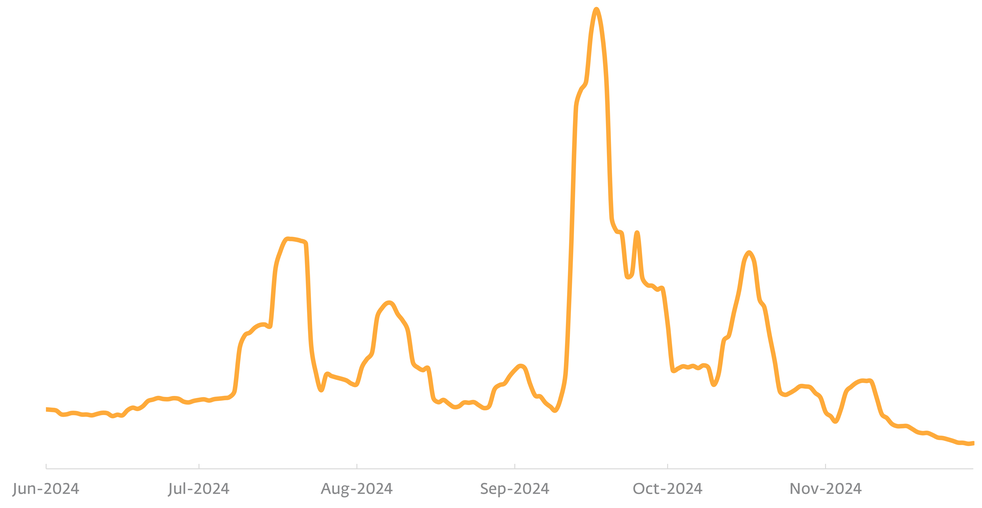
Magnus 作戦によって RedLine Stealer は確実に終焉を迎えることになりました。RedLine の開発者は逮捕されていないものの、このマルウェアを復活させようとする可能性は低いでしょう。理論的には、新しいサーバーを購入またはレンタルし、既存のコードを使って新しいインフラストラクチャを構築し、アフィリエイトにパネルを配信することも可能ですが、法執行機関に特定され、起訴されたことを考えれば、おそらく目立った活動はしないと考えられます。

RedLine のアフィリエイトも、自らのユーザー名と最後に使用した IP が記録されたデータベースを法執行機関に押収されたことから、他のツールへの移行を検討することになるでしょう。これらの情報でそのユーザー名を使用している人物を完全に特定できるわけではありませんが、「警察に重要人物として」マークされたことに変わりありません。RedLine の解体で生まれた空白を埋める形で、他の MaaS モデルの情報窃取型マルウェアの活動が活発化することになると考えられます。

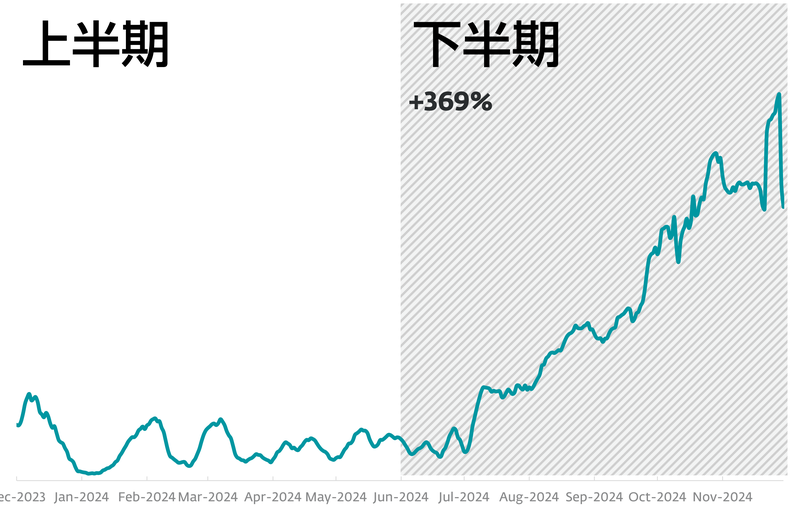
Alexandre Côté Cyr、ESET マルウェア研究者

ESET は Magnus 作戦の後に、**Flare** の研究者と協力して 2023 年に実施した RedLine のバックエンドモジュールに関する調査の結果を**発表しました**。ESET のブログでは、2023 年の結果に加えて、オランダ国家警察から解体後に提供されたソースコードから得られたいくつかの新しい情報も紹介しています。

統計が示すように、RedLine Stealer の検出数は減少したものの、完全に消滅したわけではありません。その主な理由は、RedLine のサンプルが今も多く存在するためです。アフィリエイトが積極的に拡散しなかったとしても、YouTube のコメントや GitHub のリポジトリを通じて RedLine を配信する受動型のフィッシングキャンペーンは数多く存在します。検出が続いているもう 1 つの原因は、クラッキングされた旧バージョンの RedLine Stealer が存在していることです。そのような古いバージョンであっても動作しているマルウェアがあるはずです。RedLine Stealer や META Stealer にシステムが侵害されたことが疑われる場合、これら 2 つの脅威に特化した ESET の**オンラインスキャナー**を利用できます。



2024 年下半期の **RedLine Stealer** の検出傾向、7 日移動平均線



2024 年上半期～下半期の **Lumma Stealer の検出傾向**、7 日移動平均線

Lumma Stealer の検出はかつてないほど増加

Lumma Stealer に対するサイバー犯罪者の需要がますます高くなっています。前述のとおり、2024 年下半期には、ESET 製品が検出した情報窃取型マルウェアのトップ 10 に初めてランクインしました。前半期比の増加率も過去最高の 369% となり、2024 年下半期に合計で 50,000 近くの検出を記録しました。

報道されているように、2024 年下半期に注目されたいくつものキャンペーンで Lumma Stealer が使用されています。例えば、この情報窃取型マルウェアは、複数の GitHub リポジトリの数千のプロジェクトコメントで偽の修正プログラムとして**配信されていた**だけでなく、AI 画像・動画エディタである EditPro に**なりすましていました**。10 月に確認された別の**キャンペーン**では、攻撃者が、独創的な方法でユーザーを騙して偽の CAPTCHA サイトにリダイレクトしていました。検証ステップが完了すると、Lumma Stealer が被害者のシステムに配信されます。

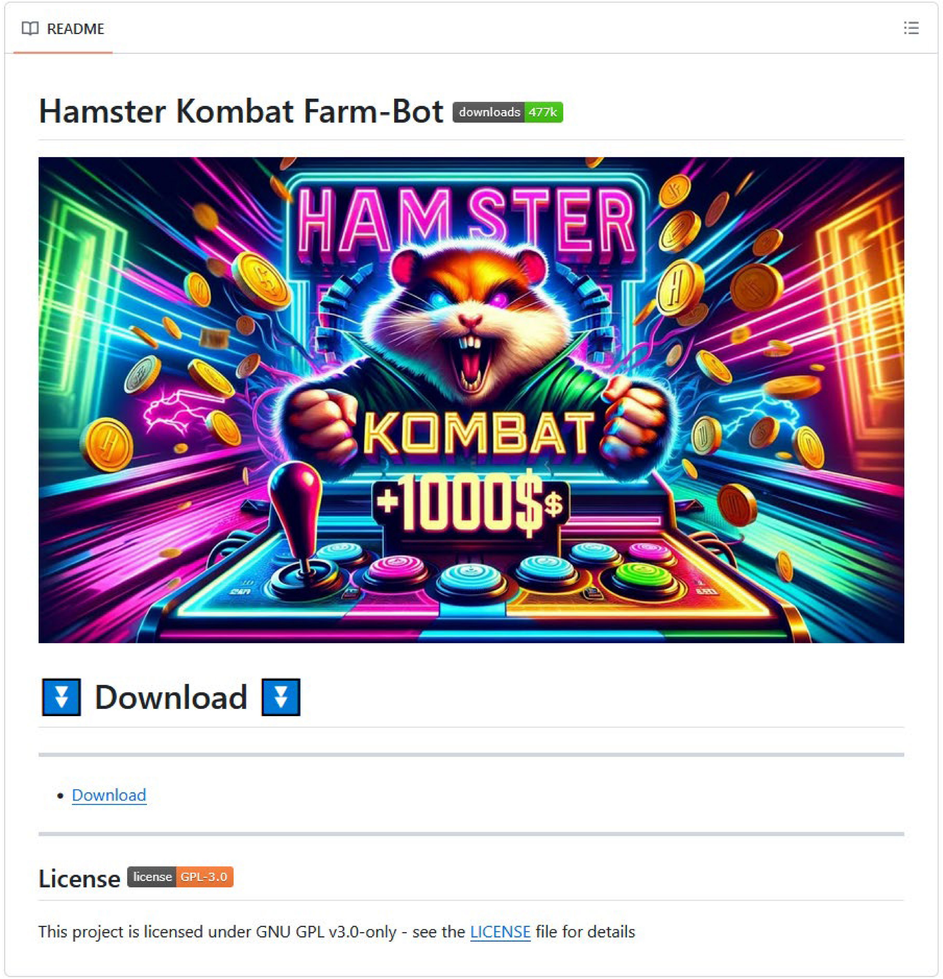
ESET のテレメトリデータによると、Lumma Stealer は 2024 年下半期にさまざまな攻撃で利用されていることが確認されています。クリプトスティーラー（暗号通貨を窃取する

マルウェア）のカテゴリでは、Win/PSW.Agent.OGR トロイの木馬として検出され、このマルウェアが 2024 年下半期の検出数の 4 分の 3 を占めました。この窃取型マルウェアは、7 月から 10 月に特に活発に活動し、その期間中、主に Windows の不正コピーをアクティベートするためのキー管理サービス（KMS）アクティベーターとして、人気のあるファイルやインストーラーにパッチが適用されて配布されています。

Win/Rozena.ADZ インジェクターのキャンペーンも検出され、その多くが Lumma Stealer を配信していました。このキャンペーンは、アダルトコンテンツを扱うオンラインマーケットプレイスや Web サイトの侵害されたビデオを通じて拡散しており、主に 10 月と 11 月に確認されました。

ESET が 7 月に発表したブログで説明したように、ESET の研究者は、モバイル画面をクリックして遊ぶ Hamster Kombat というゲームのプレイヤーを標的にした、Lumma Stealer が埋め込まれたクリプターを発見しました。Hamster Kombat のプレイヤーが最大限の特典を得ることのできるファームボットやオートクリッカー（どちらもゲームの操作を自動化して得点を速く稼ぐためのツール）を提供すると宣伝する GitHub リポジトリがいくつか見つかりました。これらのリポジトリには実際には、リリースファイルに直接埋め込むか外部のファイル共有サービスにリンクするという形で Lumma Stealer が埋め込まれたクリプターが隠されていました。

2024 年下半期に ESET のテレメトリで Lumma Stealer 攻撃の試行数が最も多かったのは、ペルー、ポーランド、スペイン、メキシコ、スロバキアでした。



Lumma Stealer を拡散していることがわかった GitHub リポジトリの 1 つ

情報窃取型マルウェア メールの脅威

Formbook の復活

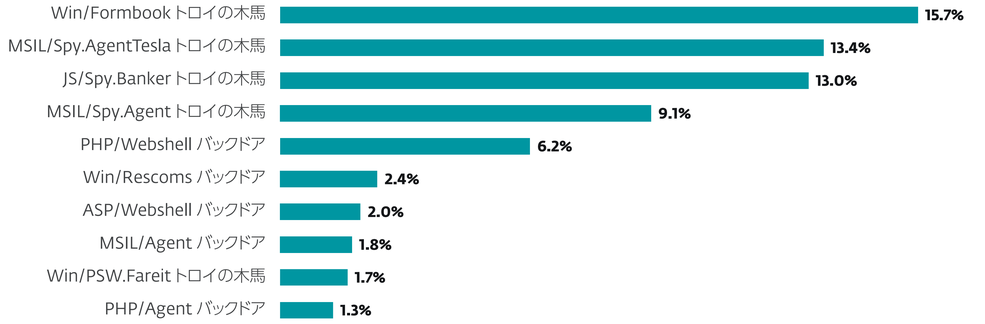
Formbook が Agent Tesla に代わって、ESET のテレメトリデータで情報窃取型マルウェアの首位に立ちました。

2024 年下半期の情報窃取型マルウェアのトップ 10 の重要な変動は、Formbook マルウェアが悪名高い Agent Tesla から**首位の座**を奪ったことです。ESET のテレメトリによると、2024 年上半期から下半期にかけて Agent Tesla の検出数が 26% 減少したのに対し、Formbook の検出数は 200% 以上増加しました。

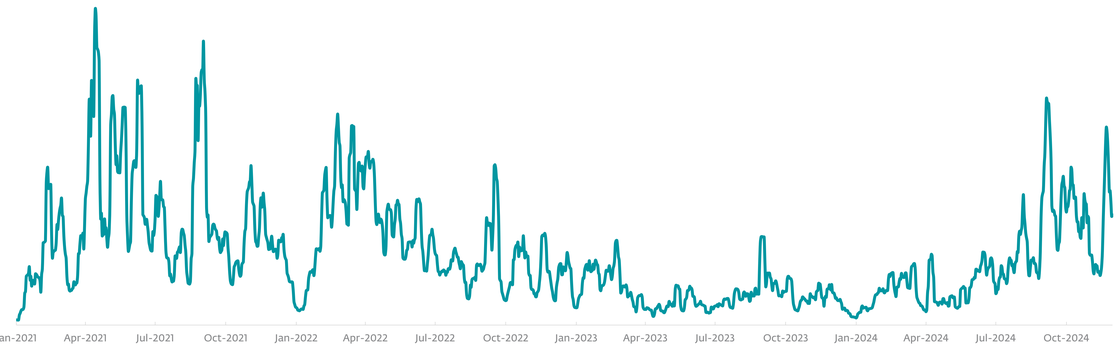
2021 ～ 2024 年の Formbook の検出傾向データに注目すると、この脅威の活動は **2021 年に特に活発**となっており、1 日あたりのヒット数が 10,000 件を超えた日もありました。その後に件数が徐々に減少しましたが、強力な脅威であり続けており、ESET が検出した情報窃取型マルウェアのトップ 5 に常にランクインしています。2024 年下半期に Formbook が復活し、2022 年の検出数のレベルに戻りました。1 日あたりの検出数で最多である 7,000 以上を 9 月 5 日に記録し、その約半数が日本で検出されました。

Formbook は、ModiLoader ダウンローダーの大規模キャンペーンのペイロードにも見つかっており、7 月の**ブログ**で説明したように、その多く（検出された攻撃の試行の 80%）が

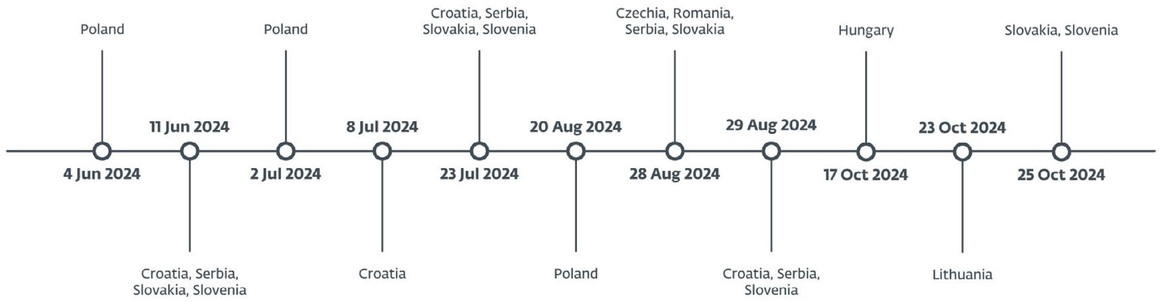
Formbook は 2016 年に初めて発見され、その後広範に拡散しています。この情報窃取型マルウェアは、クリップボードのデータ、キーストローク、スクリーンショット、キャッシュされたブラウザデータなどを収集します。地下フォーラムで販売されているこの MaaS（サービスとしてのマルウェア）ソリューションは、フィッシングメールの悪意のある添付ファイルとして拡散します。この情報窃取型マルウェアは 2020 年以降に XLoader とも呼ばれるようになりましたが、このマルウェアの macOS バージョンにこの名前が使われることもあるため、ESET は引き続き、この Windows の脅威である Formbook を Win/Formbook トロイの木馬という名前で追跡しています。



2024 年下半期の**情報窃取型マルウェア検出のトップ 10**



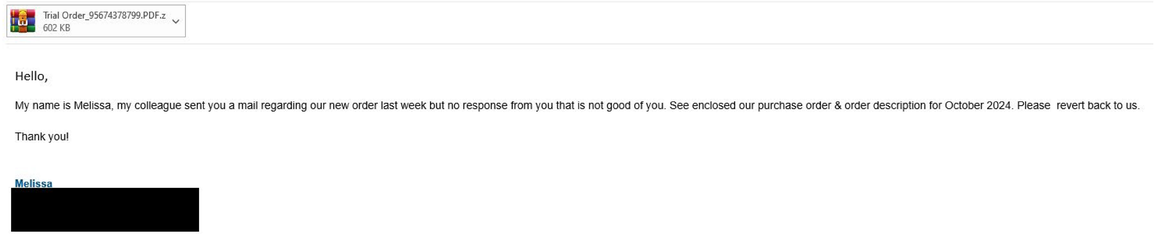
2021 年上半期～ 2024 年下半期の **Formbook の検出傾向**、7 日移動平均線



Formbook を配信する中欧と東欧における最も重大な ModiLoader と AceCryptor キャンペーンのタイムライン

ポーランドを標的にしていました。これらのキャンペーンでは、攻撃者が現存する会社やその従業員を装ったフィッシングメールの悪意のある添付ファイルを使って ModiLoader を拡散します。Formbook 以外で頻繁に配信されたペイロードは、情報窃取型マルウェアの Agent Tesla と Rescom（Remcos とも呼ばれます）でした。

最近の ESET の調査結果によると、Formbook は、他の ModiLoader に加えて複数の AceCryptor キャンペーンでも配信され続けています。ESET 製品は 6 月～10 月に、東欧と中欧で 34,000 近いユーザーを ModiLoader 攻撃や AceCryptor 攻撃から保護しました。この期間に合計 24 件のキャンペーンが確認され、2024 年下半期の初めは主に Rescoms や Agent Tesla を配信していましたが、その後は主に Formbook がペイロードに含まれるようになりました。ポーランドは、これらの攻撃の最大の標的になり続けています。



2024 年下半期に確認された、ModiLoader を配信するファイルが添付されたフィッシングメールの 1 つ

ModiLoader などの大規模キャンペーンに注目すると、2024 年に情報窃取型マルウェア全体の活動が非常に活発だったことがわかります。2021 年末から最近までのどのレポートの期間も、このマルウェアの検出数が常に減少していました。このカテゴリの検出が 2024 年上半期に増加に転じましたが、その増加率はわずか 4% でした。この増加の傾向が 2024 年下半期に加速し、情報窃取型マルウェアが 12%増加しました。

Agent Tesla の検出は大幅に減少しましたが、この情報窃取型マルウェアが完全に活動を停止したと考えるべきではありません。このマルウェアのオペレーションは解体されたわけではなく、活動が小康状態になっているのは、おそらく Agent Tesla を操っているオペレーターが新しい改良した悪意のある機能を開発しているためです。したがって、Agent Tesla は間違いなく完全に復活することになるでしょう。

現段階で検出数が多い情報窃取型マルウェアが何であるかにかかわらず、常に不審なメールに注意し、最新のセキュリティソリューションでデータを保護する必要があります。Formbook などの情報窃取型マルウェアはユーザーのパスワードを標的にすることが多いため、ブラウザに認証情報を保存するのではなく、専用のパスワードマネージャーを利用することをお勧めします。

ESET のエキスパートの解説

Formbook は比較的古いマルウェアであるにもかかわらず、MaaS（サービスとしてのマルウェア）として開発を継続しているため、多くのサイバー犯罪者に利用され続けています。2024 年下半期には、この脅威がさらに高度な難読化手法を採用し、分析や自動的な検体収集を著しく困難にしていることがわかりました。

ESET マルウェアアナリスト、Juraj Horňák

クリプトスティーラー macOS Windows Android

デジタルトレジャーハンター：ビットコインの急騰で活気づくクリプトスティーラー

ビットコインの交換レートが史上最高値を更新したことで、クリプトスティーラーがいずれも増加しました。

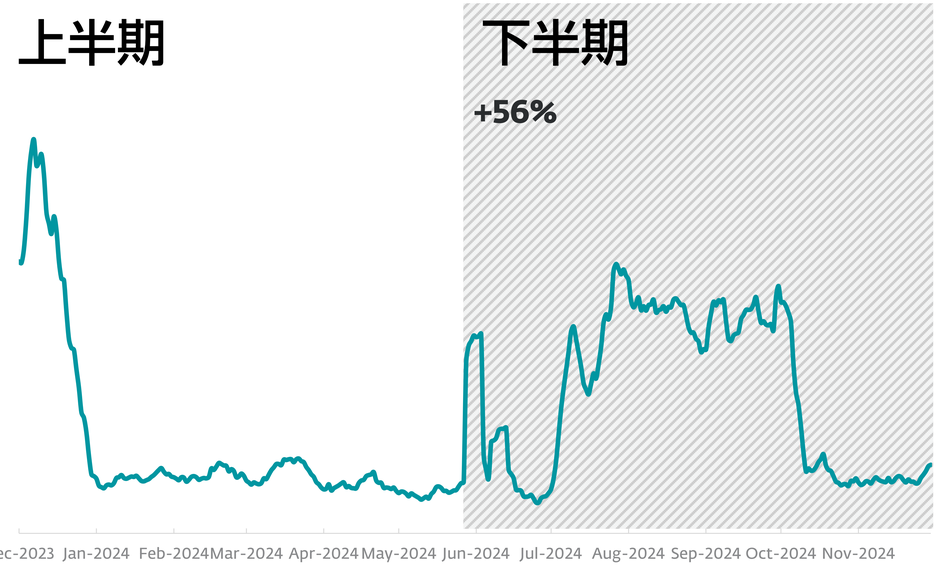
2024 年、特に下半期に、暗号通貨の交換レートが驚異的に上昇しました。ビットコインは 3 月までにすでに史上最高値の 69,000 米ドルを超え、その後もさらに上昇し続けましたが、2024 年 11 月のアメリカ大統領選挙でドナルド・トランプが勝利したことで急騰し、90,000 米ドル以上で取り引きされました。予想通り、サイバー犯罪者もこの好機に乗じて競って利益を得ようとしており、クリプトスティーラーが大幅に増加しました。

2024 年下半期の ESET のテレメトリデータによると、Windows、macOS、Android プラットフォームでクリプトスティーラーの検出数が増加しました。macOS で最も大幅に増加し、暗号通貨ウォレットを標的にするパスワードスティーラーの検出数が上半期の倍以上になりました。これに対し、Windows のクリプトスティーラーは 56% 増加し、Android の金融関連の脅威は 20% 増加しました。

macOS

ESET のテレメトリによると、macOS プラットフォームでの暗号通貨ウォレットなどに関連する認証情報を標的にすることが多いパスワード窃取ツール（PSW）の検出が 127% 増加しました。これらの脅威には広範な機能があるため、クリプトスティーラーだけに分類することはできませんが、macOS での暗号通貨を窃取する活動は増加傾向にあります。

この急増に大きく貢献したのが、**AMOS**（Atomic Stealer とも呼ばれます）とその複数のバージョンや模倣したバージョンです。AMOS は、当初は Mac デバイスから機密データを収集するマルウェア系統として設計され、MaaS（サービスとしてのマルウェア）として Telegram で販売されました。2023 年に確認されて以来、AMOS のさまざまな亜種や模倣したバージョンがブラックマーケットで販売され、実際に使



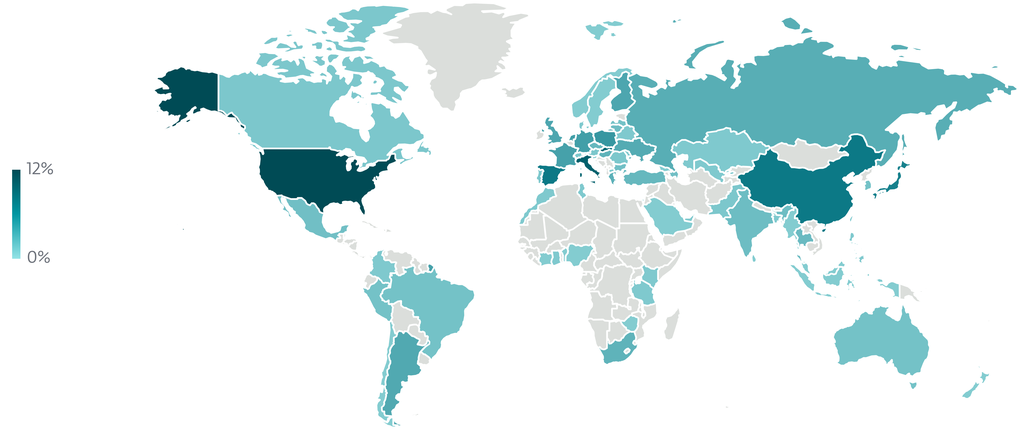
2024 年下半期の**クリプトスティーラーの検出傾向**、7 日移動平均線

われています。ESET はこれらの脅威を、OSX/PSW.Agent トロイの木馬の亜種として検出します。

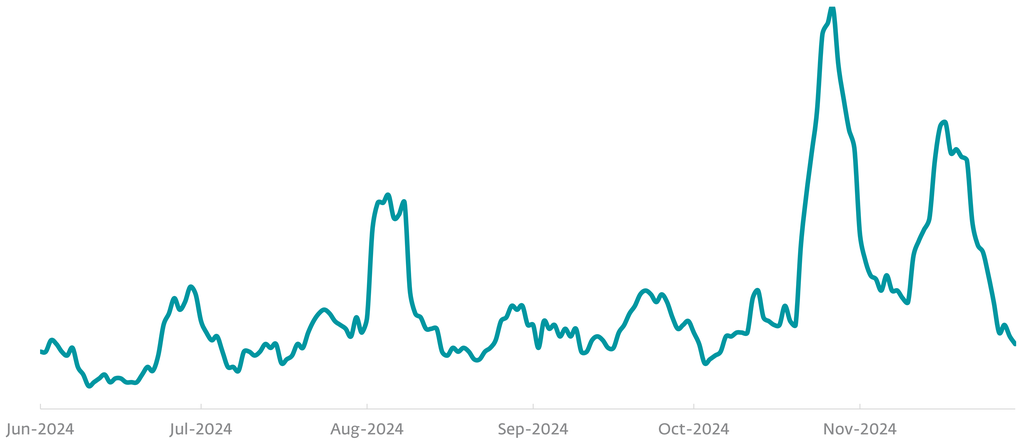
通常、Google の偽の広告やソーシャルエンジニアリングによってデバイスが AMOS に感染します。攻撃者は Google のネットワークで正規のように見せかけた不正な広告でユーザーをサイトに誘導し、正規のソフトウェアを装うマルウェアをダウンロードさせます。また、暗号通貨投資会社の社員を称する個人から接触されたとソーシャルメディアやオンラインフォーラムで報告した被害者もいます。被害者が信用すると、テレビ会議アプリなどの特定のソフトウェアをインストールするように提案されますが、実際にインストールされるのは AMOS です。

ESET のテレメトリで 2024 年下半期に PSW が最も多く検出されたのは、米国、イタリア、中国、スペイン、日本です。

注意が必要なのは、macOS でクリプトマイナーが大幅に増加し、検出数が 320% 以上も増加しましたが、特に前述の PSW に比べると、その絶対数は比較的少なくなっています。PSW の増加とは異なり、この増加は特定のクリプトスティーラーの検出が macOS で増加した結果ではありません。ESET のテレメトリによると、ほぼすべての macOS クリプトマイナー系統で均等に増加傾向が見られており、これは、ビットコインの交換レートの変動の影響によるものと考えられます。



2024 年下半期の **macOS PSW 検出の地理的分布**



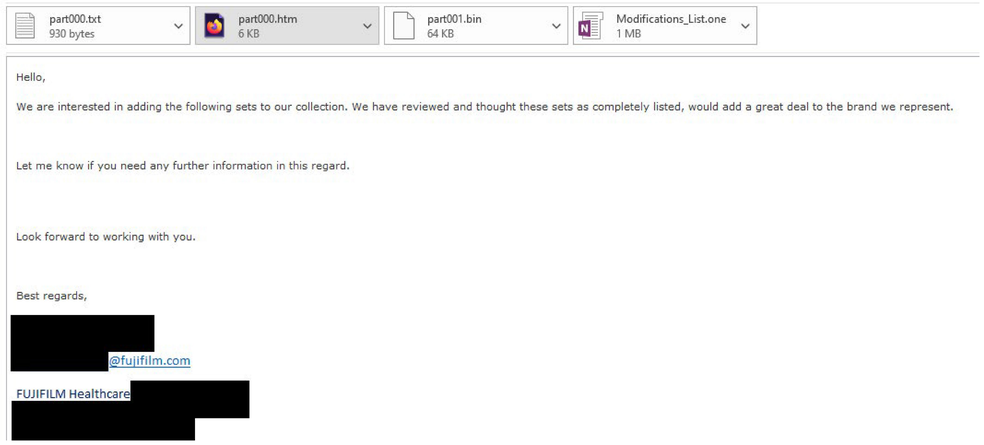
2024 年下半期の **OSX/PSW.Agent トロイの木馬の検出傾向**、7 日移動平均線

Windows

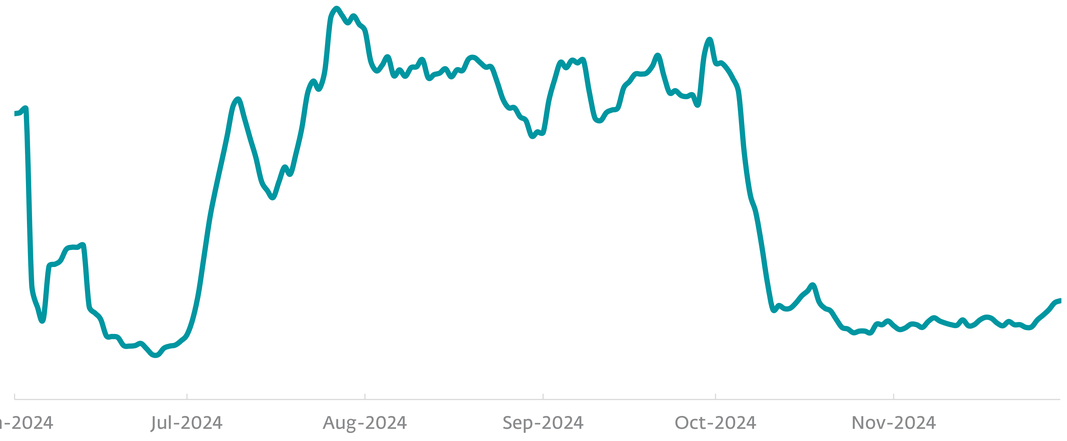
PSW の脅威も、Windows プラットフォームを標的にするクリプトスティーラーが増加した原因の 1 つです。このカテゴリで最も多く検出された 2 つのマルウェアグループは Win/PSW.Agent トロイの木馬と Win/PSW であり、Delf トロイの木馬が 2024 年下半期に検出されたクリプトスティーラーの 90% 近くを占めました。

2024 年上半期の数百件であった Win/PSW.Agent の検出数が、2024 年下半期には数千件へと大幅に増加しました。検出した検体を調査したところ、最も多かった Win/PSW.Agent グループが実際には悪名高い MaaS（サービスとしてのマルウェア）である Lumma Stealer の多数の亜種の 1 つであることがわかり、そのために検出数が増加していました。Lumma Stealer に関する ESET の最新の調査結果は、本レポートの情報窃取型マルウェアのセクションの「**2 つの情報窃取型マルウェアについてのストーリー：情報窃取型マルウェアの脅威環境の激変**」を参照してください。

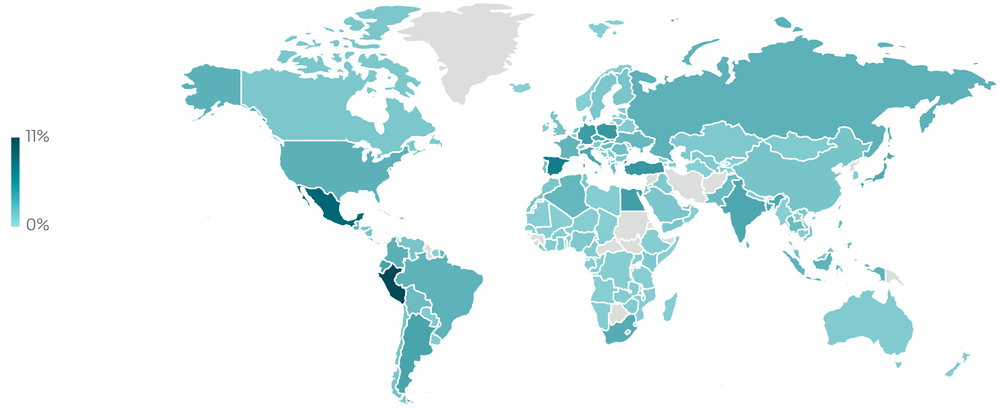
Win/PSW.Agent とは異なり、Win/PSW.Delf トロイの木馬の検出数は 2024 年下半期には増加しませんでした。しかし、6 月 7 日と 9 月 2 日にこのマルウェアの活動が急増し、トルコが主な標的になりました。9 月には、富士フイルムになりすましたスパムキャンペーンで、このマルウェアが配信されています。



Win/PSW.Delf トロイの木馬を配信する、富士フイルムになりすましたフィッシングメール



2024 年下半期の **Windows プラットフォームを標的にするクリプトスティーラーの検出傾向**、7 日移動平均線



2024 年下半期の **Windows プラットフォームを標的にするクリプトスティーラー検出の地理的分布**

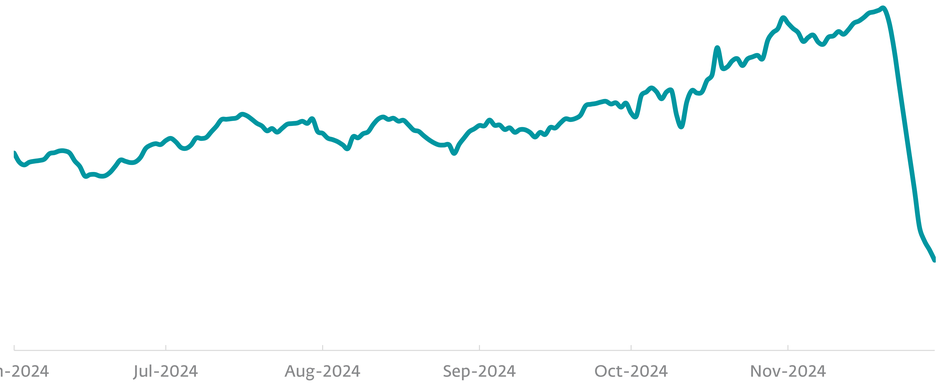
このレポートの期間中に Windows 攻撃の試行回数が最も多かった国は、ペルー、メキシコ、スペイン、トルコ、ポーランドでした。

Android

Android プラットフォームでは、クリプトスティーラーは、Android バンキングマルウェアが含まれるさらに広範な金融関連の脅威のカテゴリの一部に属します。このカテゴリの脅威が拡大していることは、暗号通貨ウォレットや金融取引アプリ、秘密鍵、暗号通貨のリカバリフレーズに関連する認証情報がデバイスに見つかった場合にそれを窃取する機能が多くの金融関連のトロイの木馬に組み込まれるようになっていることを示しています。

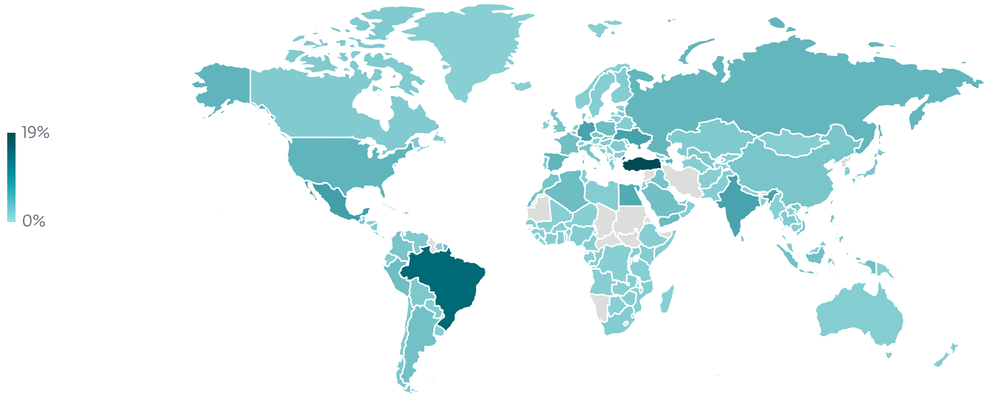
ESET のテレメトリによると、Android の金融関連の脅威は 2024 年下半期に 20% 増加しました。それほど大きな増加ではありませんが、次ページのグラフを見ると、上昇傾向にあることがわかります。この増加の主な要因である Cerberus は、バンキングアプリを主に標的としつつ、暗号通貨ウォレットや取引所も標的にする機能を備えた高度なトロイの木馬です。

Cerberus は、正規のアプリに偽のログイン画面を重ねて表示し、被害者が標的のアプリにログインしようとすると、入力した認証情報を取得して攻撃者に送信します。ESET のテレメトリで、2024 年下半期に Cerberus の検出数が 56% 増加しましたが、重要なのは、Android デバイスが最初に侵害され、その後、Cerberus（またはその他の脅威）によってドロッパーを通じて追加の悪意のあるコードがインストールされる可能性があるという点です。



2024 年下半期の**金融関連の Android の脅威の検出傾向**、7 日移動平均線

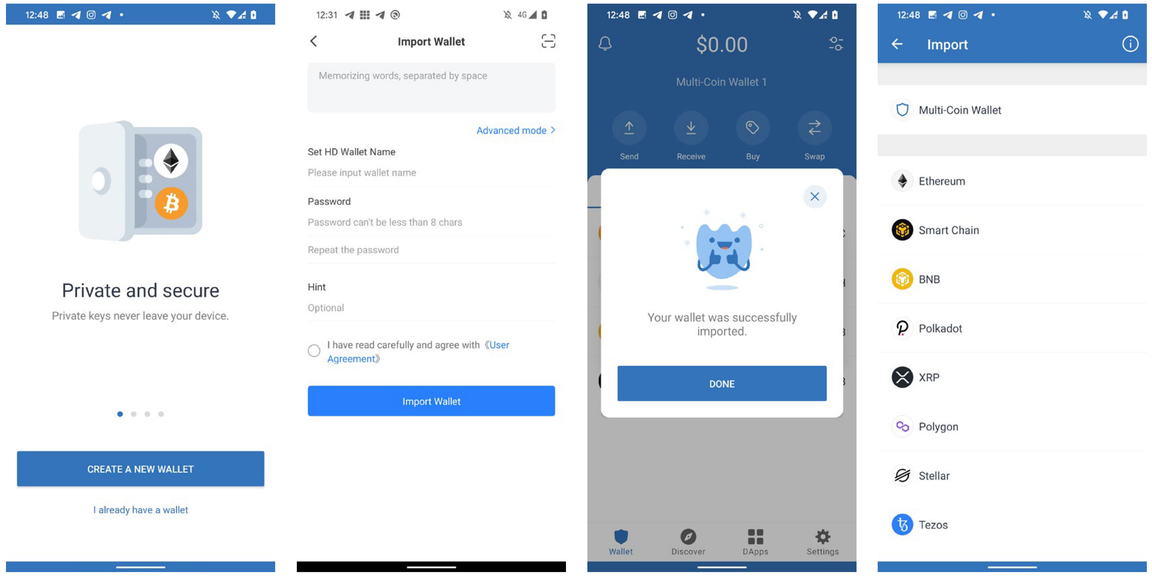
ESET のテレメトリによると、Android の金融関連の脅威の検出の 53% 以上がドロッパーによるものです。ESET 製品が 2024 年下半期に金融関連の Android の脅威を最も多く検出した国は、トルコ、ブラジル、メキシコ、インド、ドイツ、ウクライナでした。



2024 年下半期に検出された **Android の金融関連の脅威の地理的な分布**

研究者が特定した注意が必要な Android クリプトスティーラーの 1 つが **WalletConnect** です。WalletConnect は、暗号通貨ウォレットと分散型アプリケーション（DApp）のプロキシとして機能する正規のツールに見せかけた悪意のあるアプリです。WalletConnect がインストールされると、詐欺のための Web サイトにユーザーが誘導され、取引を承認するように指示され、結果としてウォレットの機密情報やデジタル資産が窃取されます。ESET はこの脅威を、Android/FakeWallet.KH として検出します。

研究者はさらに、OCR（光学式文字認識）を使ってデバイスに保存されているスクリーンショットから暗号通貨ウォレットのリカバリフレーズを抽出するマルウェアを**発見しました**。ユーザーによっては、リカバリフレーズのスクリーンショットを撮影してモバイルデバイスに保存することで、クリップボードやメモから盗まれないようにしている場合もあります。マルウェアは、これらのリカバリフレーズを手に入れることで、被害者の暗号通貨ウォレットを復元して乗っ取り、ウォレットの暗号資産をすべて窃取できます。ESET 製品はこの脅威を、Android/Spy.OcrSpy.A と Android/Spy.Banker.CTP として検出します。



リカバリフレーズを攻撃者のコマンド & コントロールサーバーに送信する、トロイの木馬化された暗号ウォレットアプリの例

Android iOS 金融関連の脅威 攻撃手法

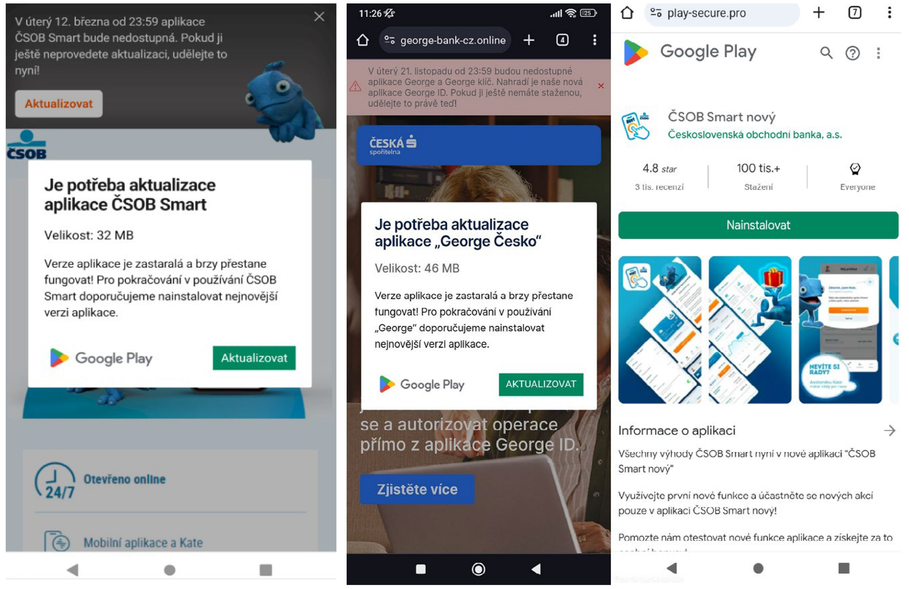
アプリか、Web サイトか？モバイルバンキングの認証情報をすばやく窃取する方法

モバイルデバイスを攻撃する新たな手法により、攻撃者は従来のモバイル OS のセキュリティ対策を迂回し、ユーザーを騙して Android や iOS のデバイスを侵害しています。

ESET の研究者は、モバイルデバイスを標的にする新しい攻撃手法を利用したキャンペーンを分析しました。この方法は多くのサイバー犯罪者に悪用される可能性が高く、プログレッシブ Web アプリ（PWA）や WebAPK（Chrome ブラウザで生成される Android パッケージキット）を利用します。これらのテクノロジーを利用することで、ユーザーはブラウザを使用してアプリを Web サイトから直接インストールできます。要するに、PWA（プログレッシブ Web アプリ）と WebAPK を使用すると、ユーザーはネイティブアプリに似たアイコンを通じて、スマートフォンの画面から Web ベースのサービスにアクセスできるようになります。

この手法が極めて危険なのは、PWA も WebAPK も、不明なソースからアプリをインストールしたりブラウザが不明なアプリをインストールしたりすることをユーザーが明示的に許可する必要がないことです。結果として、信頼できないソースからデバイスが知らぬ間にアプリをインストールする恐れがあります。ESET の研究者が分析した悪意のあるアプリは、インストール後に、モバイルバンキングマルウェアのように動作し、偽の銀行ログインインターフェースを表示して認証情報の入力を要求します。ログイン情報、パスワード、二要素認証コードなどの窃取した認証情報が攻撃者のコマンド & コントロールサーバーに送信され、結果として、攻撃者が被害者のアカウントへのアクセス権限を不正に入手します。

2024 年に ESET の調査で、チェコの大手銀行、ハンガリーの銀行、グルジアの銀行の顧客を標的にするキャンペーンが明らかになりました。しかし、この戦略は、ポーランドの銀行に対する攻撃の後の 2023 年 7 月に、ポーランドの金融分野のコンピュータセキュリティインシデント対応チーム（CSIRT KNF）によって最初に報告されました。チェコで発生したあるキャンペーンでは、攻撃者が窃取したデータを使用し、侵害したスマートフォンから攻撃者のルート化されたモバイルデバイスに中継された NFC データを使用して ATM から預金を引き出しています。この NFC データリレー機能を使用する Android マルウェアが実際に確認されたのはこれが初めてです。



偽のダウンロード Web サイトの例、右側は Google Play の外観の模倣

地方銀行の顧客を標的にする悪意のある PWA や WebAPK が ESET の調査と CSIRT KNF で検出された国

最初のフィッシングメッセージは、SMS、自動音声通話、ソーシャルメディアの不正な広告などのさまざまな方法で配信されました。被害者は、モバイルバンキングアプリケーションの更新が必要であったり、税金の払い戻しを受けられる可能性があったりすることを知らせるメッセージや電話を受け取りました。これらのメッセージは、おそらく無作為に選択された電話番号に送信されており、被害者を正規のバンキングサイトを模倣するフィッシングサイトに誘導するリンクが含まれていました。Facebook や Instagram の不正な広告で偽のバンキングアプリを宣伝し、公式アプリは廃止されるとユーザーを騙していました。

フィッシングサイトに移動すると、Android ユーザーには WebAPK をインストールするように指示され、iOS ユーザーにはネイティブシステムに似た画面で PWA をホーム画面に追加するよう指示されます。いずれの場合も、公式のロゴやデザイン要素を使った、見かけも挙動も正規のバンキングアプリのように見えるアプリケーションがインストールされます。このプロセスでは通常、信頼できないソースからのインストールであることを示す警告が表示されないため、フィッシングであると判断することがさらに困難になっています。

ESET の研究者はこれらの脅威を積極的に監視および分析していますが、PWA や WebAPK を利用するモバイル脅威の傾向のグラフ（本レポートの他のセクションに示したグラフなど）にまとめるのは簡単なことではありません。従来のアプリとは異なり、これらの悪意のある PWA や WebAPK は基本的には正規のアプリケーションに見せかける目的でパッケージ化されたフィッシング Web サイトです。行動や特性は一般的なマルウェアとは異なっています。特に問題なのが、モバイルオペレーティングシステムの従来型のセキュリティ警告を回避でき、アプリストアの審査プロセスを完全にすり抜けてしまうことです。そのため、モバイルプラットフォームが PWA や WebAPK に対するアプローチを変えない限り、PWA や WebAPK を利用したより巧妙で多様なフィッシングキャンペーンが今後も発生することが予想されます。

PWA/WebAPK とネイティブアプリの相違点

PWA は基本的には Web ページのローカルコピーであり、ネイティブアプリと機能はほとんど同じです、HTML、CSS、JavaScript などの標準の Web テクノロジーを使用して構築されています。複数のプラットフォームに対応しており、ブラウザから直接インストールできるため、アプリストアやその審査を回避できます。WebAPK はこの点がさらに進化したもので、Chrome ブラウザが PWA から生成するネイティブ Android アプリケーションであり、PWA の一般的なアイコンのようにブラウザの小さいロゴが重なって表示されないため、正規のアプリであるように見えます。

チェコのある銀行の正規のアプリ（左）、悪意のある WebAPK（中）、悪意のある PWA（右）

インストールの過程でサードパーティアプリに対する明示的な許可は必要なく、アプリそのものが信頼されないものであることを示す通常の警告も表示されません。このため、ユーザーがこれらを悪意のあるアプリと判断するのは困難です。さらに、これらのアプリがデバイスのオペレーティングシステムにシームレスに統合されることで、見た目がさらに本物らしくなり、正規のアプリと悪意のあるアプリを区別するのが困難になります。

ESET のテレメトリは、チェコ、ハンガリー、ポーランド、グルジアで Android/Spy.NGate（亜種 .A、.B、.C）と Android/Spy.Banker（亜種 .CIC、.CLW、.BWW）としてこれらの攻撃を検出しています。

ESET のエキスパートの解説

サイバー犯罪では継続的に技術開発が行われており、PWA や WebAPK が悪意のある目的で利用されることが増加することになるはずです。これらのテクノロジーは攻撃者にとって、アプリストアの承認を必要とすることなくフィッシングアプリケーションを配信する便利で効果的な手段です。PWA は複数のプラットフォームに対応しており、攻撃者がより多くのユーザーを標的にでき、スケーラブルで汎用性の高い攻撃になります。既存のセキュリティツールを利用することに加えて、アプリを正規のアプリストアからのみインストールし、実績のあるセキュリティアプリを利用するなどのアドバイスに従うことで、このような新たな脅威から身を守ることができます。

Lukáš Štefanko、ESET シニアマルウェア研究者

Web の脅威 詐欺 ディープフェイク

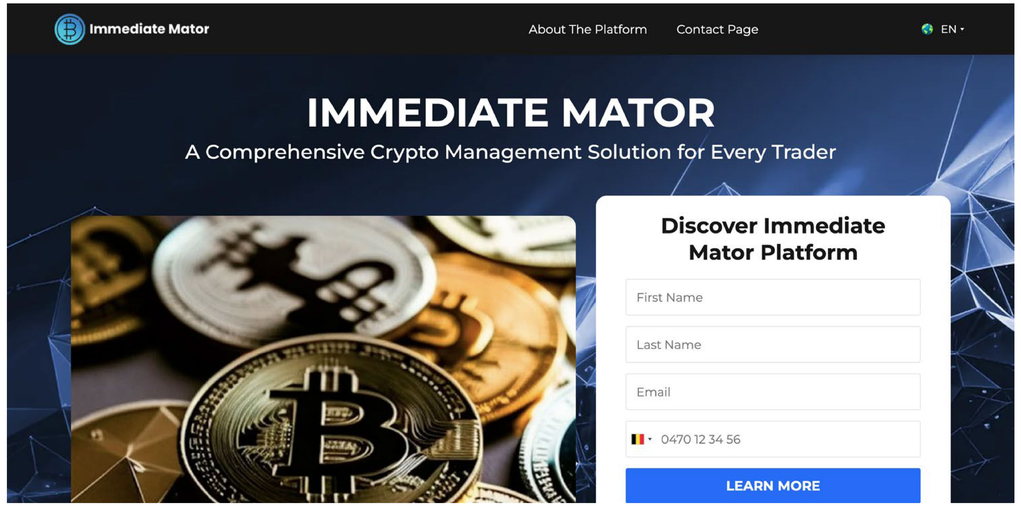
裕福なセレブと共に投資し、最終的に Nomani に感染

新たなタイプの投資詐欺広告がソーシャルメディアのニュースフィードに溢れています。ディープフェイク動画や企業ブランドを装った投稿によって多くの犠牲者を引き寄せ、金銭的な損失や個人情報の漏洩といった被害を引き起こしています。

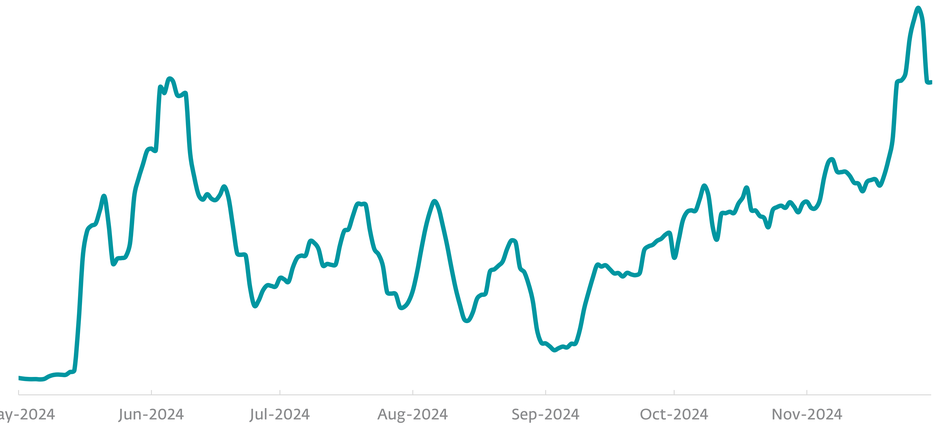
2024 年のソーシャルメディアには、「限定公開」の投資機会、奇跡を起こすサプリメント、法的支援や捜査機関の援助を謳う詐欺広告が溢れました。犯罪者は、このような広告を信用できるように見せるために、その国の企業やグローバル企業のブランドを悪用したり、広告商品の正当性を有名人が保証しているように見せる AI 生成のディープフェイク動画を使用したりしています。

これらの詐欺師の主な目的は、被害者をフィッシングサイトやフィッシングフォームに誘導し、ユーザーの個人情報を収集することです。これらの Web サイトの内容は、偽の広告と同様に、地元のニュースメディアのサイトそっくりに模倣したり、特定の企業や組織のロゴ、ブランディング、カラーを悪用し、Quantum Bumex、Immediate Mator、Bitcoin Trader など名前を次々へ変えながら、投資、取引、暗号通貨などの一般的な金融テーマのビジュアルを使用したりしています。

ESET はこの脅威を HTML/Nomani トロイの木馬として検出しています。Nomani という名前は、ESET の検出エンジニアによって「no money（お金を失う）」という英単語から派生した名前として選ばれました。ESET のテレメトリ（監視データ）によると、HTML/Nomani は 2024 年 5 月に急増し、2024 年上半期から下半期にかけて 335%以上増加しました。2024 年 5 月から 11 月にかけて、ESET は 8,500 件以上のドメインと、これらのドメインへの何万ものアクセス試行をブロックしました。ESET のシステムは、平均して、毎日 100 件以上の新しい URL を検出しています。2024 年上半期にこのマルウェアの検出が最も多かった国は、日本（11.5%）、スロバキア（11%）、カナダとスペイン（いずれも 9%）、チェコ（7%）でした。



存在しない投資商品を宣伝する偽の Web サイト（HTML/Nomani として検出される）



HTML/Nomani の検出傾向 2024 年 5 月から 2024 年 11 月までの 7 日移動平均線

詐欺師はフィッシングドメインから収集したデータを使って、被害者に直接電話をかけ、驚異的な利益を上げることができると謳った詐欺商品に投資させるように誘導します。被害者の中には、騙されてローンを組まされたり、デバイスにリモートアクセスアプリをインストールされたりした人もいます。これらの被害を受けた「投資家」が、約束された利益の支払いを求めると、詐欺師は追加料金の支払いを要求し、さらに個人情報（身分証明書やクレジットカード情報など）を提供するように強要します。最終的に、詐欺師は金銭とデータを両方とも奪い、姿をくらまします。これは典型的な「豚の屠殺詐欺」の手口です。

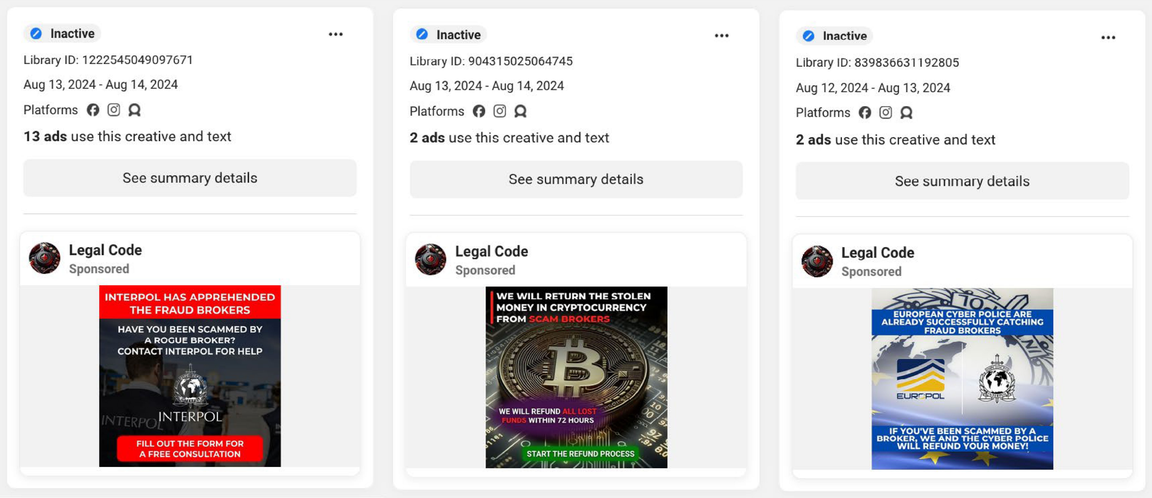
ローカライズされ継続的に更新されるコンテンツ

注意深いユーザーであれば、いくつかのレッドフラグに基づいて Nomani 関連の広告であることを見極めることができます。広告の動画は低解像度になっていますが、これはレンダリングの不具合を隠すための「特徴」です。しかし、このような不具合は、スマートフォンの小さな画面では発見しづらくなっています。文章構造が不自然であることが多く、生成された人物の呼吸が不自然であったり、キーワードがしつこく繰り返されたり、音声と映像が正しく同期されていないことも多くあります。しかし、ユーザーの注意力が低下しており、Cookies や利用規約、その他の確認画面の内容を読まずに承諾する習慣が広がっているため、多くのユーザーがこれらの広告をほぼ自動的にクリックしてしまうリスクがあります。

数百件にわたるこれらの詐欺広告を分析した結果、攻撃者が各国ごとにコンテンツを高度にローカライズしたバージョンを使用していることが明らかになりました。スロバキアでは、現職の国家元首やエネルギー企業、また ESET のような企業が、なりすましの重要な対象となっています。ドイツでは、攻撃者はドイツの政党「キリスト教民主同盟（CDU）」の党首や、ルフトハンザの企業ブランドを悪用した偽の投資に注力しています。アメリカやカナダの多くの人は、イーロン・マスク氏が暗号通貨への投資を呼びかけているディープフェイクを見たことがあるのではないでしょうか。

Meta（Facebook）の広告、X、YouTube、および Google の偽のレビュー

これらの偽広告の主に配信されるのは、Facebook と Instagram ですが、Meta Ad Library を通じて確認できる広告の詳細によると、多くの投稿は Messenger や Threads でも配信されていました。X（旧 Twitter）と YouTube は以前、主に「投資プラットフォーム」の偽のレビューやディープフェイク動画の広告に使用されていましたが、最近では詐欺広告が動画プラットフォームにも登場しています。



Meta Ad Library にリストされている詐欺的な Nomani 広告の例。皮肉なことに、これらの広告は以前に詐欺に遭ったユーザーを標的にしている。

Google 検索でも、欺瞞的で肯定的なレビューが溢れており、検索上位に表示されています。TikTok ではこのような詐欺コンテンツは確認されていません。

Meta プラットフォームにおけるリーチを増やすために、詐欺師は偽のプロフィールと窃取した正規のプロフィールを組み合わせて広告を掲載しています。ハッキングされたアカウントには、小規模企業のページや政府機関、フォロワーが数万人いるマイクロインフルエンサーのアカウントが含まれています。ESET の調査で確認された一例は、フォロワーが 30 万人以上いる人気俳優のアカウントでした。欧州連合（EU）が広告の透明性を確保するために公開している情報によると、この攻撃は数十か国から管理され、ヨーロッパの異なる地域で数百件の偽広告を拡散していました。

Nomani 広告を頻繁に広めているもう一つの大きなグループは、覚えやすい名前で新しく作成されたプロフィールで、フォロワーが少なく、投稿も非常に少ないアカウントです。既存の正規の企業やニュースメディアのいくつかのアカウントがコピーまたは軽微に変更されたバージョンが攻撃者に悪用されており、通常はこれらの企業ブランドのカラーやロゴ、さらには過去のソーシャルメディアコンテンツが悪用されています。

サイバー攻撃者で進む担当の分業制

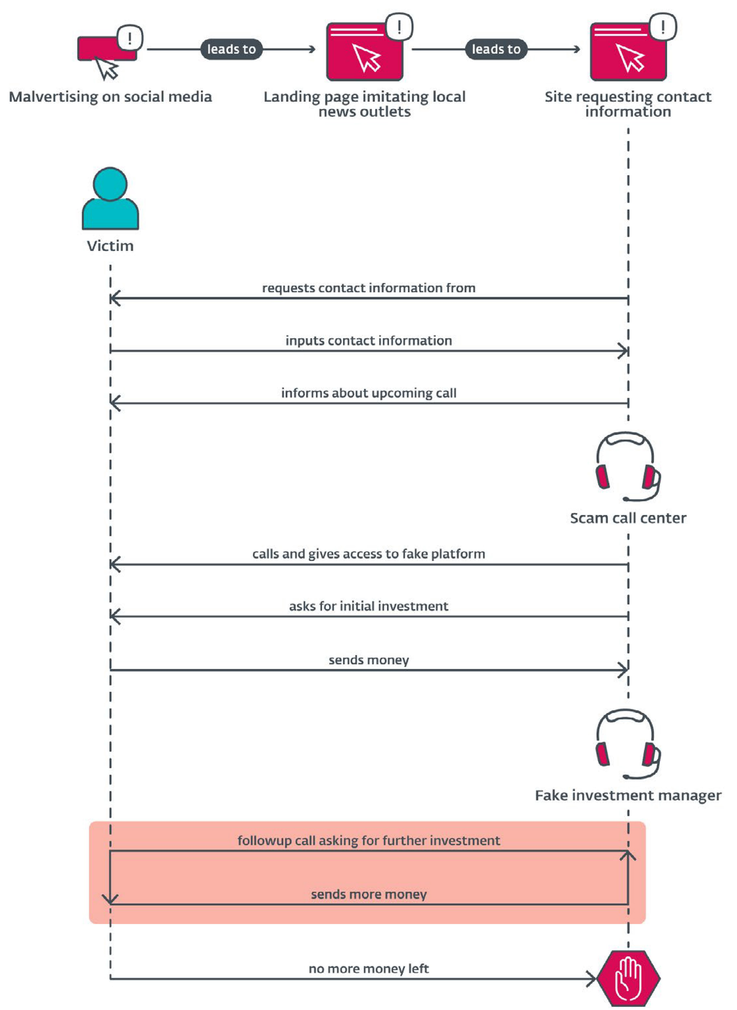
HTML/Nomani の検体を分析した結果、いくつかのアーティファクトから、このサイバー攻撃者はロシア語圏の国を拠点としていると考えられます。検出された多くのフィッシングサイト（投資、偽商品、法律関連、その他のテーマを含む）で、

テンプレートが共通しており、同じロシアのサーバーにコールバックしていました。これらのページで使用されていたスクリプトとコードには、キリル文字のコメントが含まれており、訪問者を追跡するためにロシアの大手 IT 企業である Yandex のツールが使用されていました。通信に Telegram を使用しているのが確認されていますが、これは典型的な手法ですが、ロシア語を話すサイバー犯罪者だけが利用しているわけではありません。

HTML/Nomani の詐欺では、攻撃チェーンのさまざまな部分を異なるグループが担当している兆候があり、分業制の特徴が見られます。例えば、あるグループは Meta アカウントや広告の窃取や悪用を担当し、他のグループはフィッシングページや偽の投資プラットフォームを構築したり、コールセンターを運営したり、マネーロンダリングを担当したりしています。それぞれが作業を分業する組織構造になっているため、追跡と特定が複雑になり、将来的に法執行機関による摘発の範囲や効果が限定される可能性があります。

いくつかの金融機関は、このような不正な攻撃が増加傾向にある、あるいは最も多く頻発するシナリオになっていることを公表しています。言い換えれば、Nomani のような詐欺は、サイバー犯罪者が被害者の認証情報を窃取し、取引を自ら行おうとする「従来型」のフィッシングのシナリオに取って代わりつつあります。

詐欺師は、ソーシャルエンジニアリングの手法を使用して被害者との信頼関係を築くこともあり、銀行が不正防止のために使用する認証メカニズムや確認電話さえも巧妙に回避することも多くあります。



Nomani 詐欺の概要

Web の脅威 詐欺 フィッシング

オンラインマーケットプレイスの詐欺が多様化。偽のホテル予約サイトから観光客を騙すケースも

2024 年下半期には、人気の宿泊予約プラットフォームのユーザーを狙った新たな詐欺が発生しました。この詐欺師は、オンラインマーケットプレイスでユーザーを騙すために開発したツールキット「Telekopye」を使用しています。

冬休みの旅行の宿泊をオンラインで予約したとしましょう。ホテルからの連絡を受け取ったとき、あなたはすでに居心地の良いホテルで過ごすまでの日数を数えていました。しかし、支払いに問題が発生しており、ホテルのメッセージに含まれるリンクから解決するように求められました。少し不審な感じがしますが、とにかくリンクをクリックして問題の内容を確認することにしました。

開いたページは本物のように見えます。Web サイトのデザインに不審な点がなく、あなたの情報はすべて正しく記載され、支払い金額を含む予約の詳細も記載されています。

このページの支払いフォームに情報を記入することは、合理的なように思われます。しかし、入力した情報は、組織的な詐欺師グループによって窃取されることになります。

予想外の展開を見せる厄介な詐欺

では、この詐欺は一体どのような内容なのでしょうか？ESET の研究者は、「スイスアーミーナイフ」のようなツールキット、**Telekopye** を使って行われ、オンラインマーケットプレイスで買い手と売り手の両方を狙ったさまざまな詐欺を報告しています。

2024 年、ESET の研究者は、これらの詐欺グループが、Booking.com や Airbnb などのホテルや短期滞在用の宿泊施設の予約を扱う人気のオンラインプラットフォームのユーザーを狙った**新たな手口を追加**したことを発見しました。

この新しい詐欺には、厄介な要素があります。それは、詐欺のための支払いページに提供される情報が標的ユーザーの実際の予約と一致していることです。

Telekopye

- Telegram ボットとして動作するツールキットは、フィッシングを簡単に行える機能を提供し、オンラインマーケットプレイスの詐欺を組織的な違法ビジネスに変えるための非常に汎用的で多目的な「スイスアーミーナイフ」のように機能します。
- Telekopye は、2023 年に ESET Research によって発見され、少なくとも 2016 年から使用されていることが確認されています。このツールの発生源はロシアだと考えられます。
- ヨーロッパや北アメリカのさまざまなオンラインサービスを標的にするよう設計されており、被害者は世界中に広がっています。

マンモス：詐欺師が標的とする買い手と売り手の呼称。

ネアンデルタール：ESET Research が詐欺師に付けた名前 - Telekopye を利用する Telegram グループのメンバー。

オンラインマーケットプレイス詐欺には、詐欺師が売り手を装う場合（より一般的）と買い手を装う場合の主に 2 つのシナリオがあります。どちらのシナリオでも、決済ゲートウェイを装ったフィッシングページにユーザーを誘導します。

宿泊予約詐欺は、Telekopye 詐欺に追加された最新の方法です。

詐欺師は、信憑性を高めてユーザーを騙すことができるように、プラットフォームの正規のホテルや宿泊施設プロバイダーのアカウントを乗っ取り、購入または窃取したであろう認証情報を使ってアクセスします。詐欺師は次に、そのプロバイダーから最近宿泊を予約し、まだ支払いをしていない、あるいは最近支払ったユーザーを選び出し、プラットフォームのチャットで連絡を取ります。プラットフォームや被害者の設定によっては、宿泊予約プラットフォームからメールや SMS を受け取る場合もあります。

この記事の冒頭で説明したように、この仕組みによって詐欺を見破ることが非常に困難になっています。提供される情報は、被害者個人に関連しており、想定される通信方法で届けられ、リンクされている偽の Web サイトも想定通りに見えます。では、手遅れになる前に騙されていることに気づくにはどうすればいいのでしょうか？

ドメインに潜む悪魔

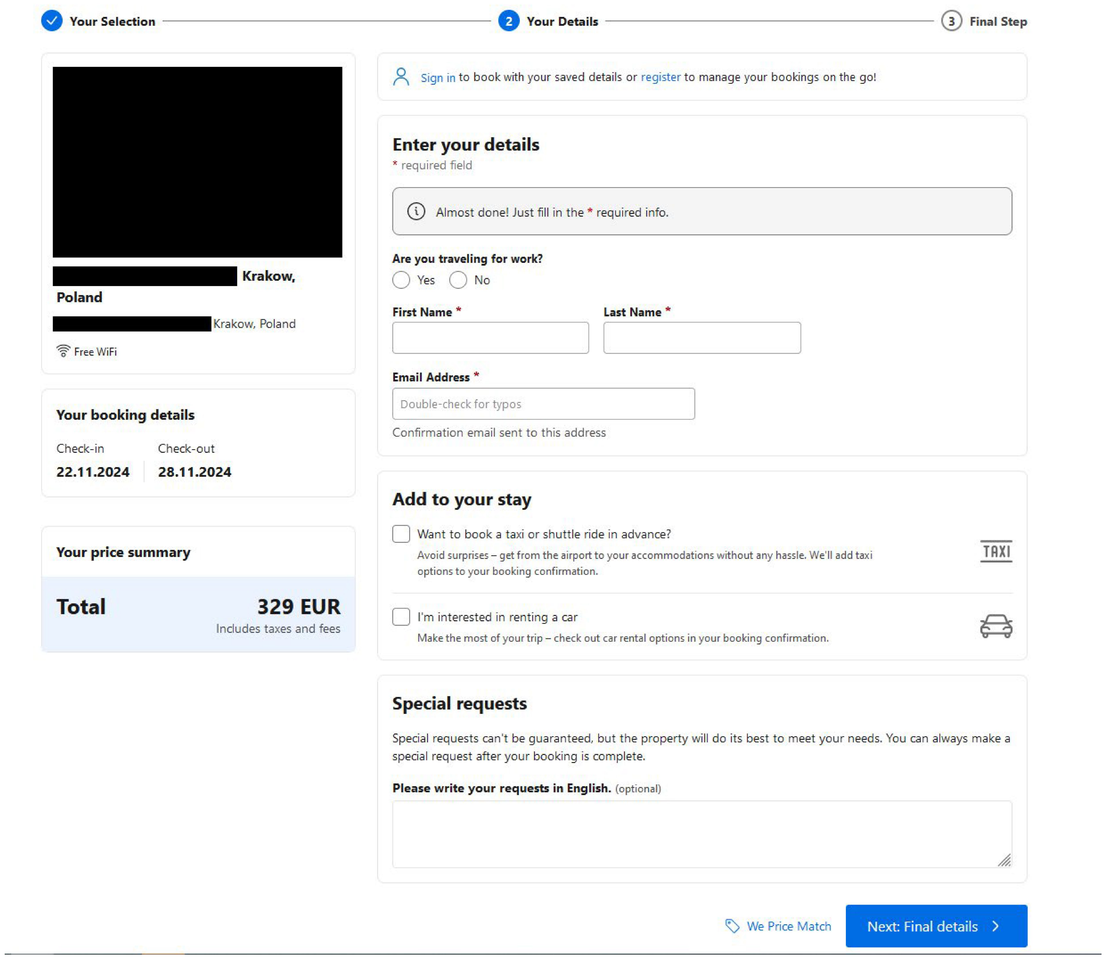
多くの場合、問題があることを示す唯一の目に見える兆候は、Web サイトの URL のドメイン名であり、それが偽装された正規の Web サイトのドメイン名と一致しないことです。しかし、ここでも詐欺師は正規の URL のように見せかけるためにいくつかの手間をかけています。標的となっているプラットフォームの名前がサブドメインとして頻繁に使用され、実際のドメイン名は支払いプロセスの次のステップを示すような、一般的な名前になっています。ESET のテレメトリデータで確認された、Booking.com を装ったそのような URL の例を以下に示します。[1]

- `https://booking.support-ticketapp[.]com/confirm/login`
- `https://booking.com-extra-check[.]quest/confirm/login`
- `https://booking.processord-user[.]com/order`

例えば、このような目的のために Booking.com の専用ドメインを作成した場合、既存のドメインのサブドメインとして作成され、`<task_name>.booking.com` のような形式になり、例えば、この場合は `support-ticketapp.booking.com, extra-check. booking.com` のような URL が作成されます。

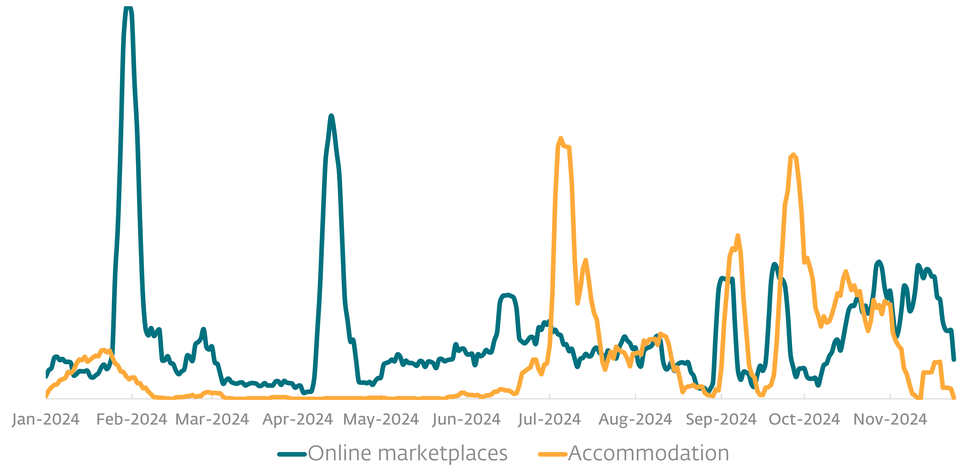
標的ユーザーがフィッシングページのフォームに記入すると、「予約」の最終段階である支払いカード情報の入力を要求するフォームに誘導されます。フォームに入力されたカード情報は詐欺師によって収集され、被害者から金銭を奪うために使用されます。

ESET のテレメトリによると、このような詐欺は 2024 年に流行し始めています。傾向チャートに見られるように、宿泊施設に便乗した詐欺は 7 月に急増し、初めて元の Telekopye オンラインマーケットプレイス詐欺を超え、その月の検出数は元の詐欺の 2 倍以上となりました。10 月にも上昇を記録しました。検出のピークは、休暇シーズンと連動している可能性がありますが、活動の増加がランダムである可能性も考えられます。



Telekopye によって作成された偽の Booking.com フォームの例で、実際の予約詳細が事前に入力されています。

[1] 元の URL には、URL パスの最後に標的ごとの一意の英数字識別子が含まれていますが、これらはサンプルの URL からは削除されています。



2024 年に Telekopye が標的にしたオンラインサービスのタイプの検出傾向、7 日移動平均線

ESET のエキスパートの解説

この新しい予約詐欺により、Telekopye のツールキットを使用する犯罪者は、既に確立されている詐欺の手口をまったく新しい分野に拡大させることに成功しており、被害者の範囲が広がる恐れがあります。

詐欺師は、試行錯誤を重ねたツールやプロセスをすぐに利用できるようにしており、今後このような詐欺が増えることが予想されます。また、ESET の傾向データから、宿泊予約プラットフォームを標的にした詐欺がさらに蔓延する可能性が示されていますこのような詐欺が広く拡散しており、その手口が比較的巧妙であることから、オンライン活動を安全に維持するためにはセキュリティ意識を高めることが極めて重要です。

法執行機関との協力に関する最近の Telegram のポリシー[2] 変更が、これらの詐欺グループにどのような影響を与えるか、今後の状況を注視する必要があります。

ESET マルウェア研究者、Radek Jizba

自分を安全に守る方法

Telekopye による詐欺から身を守る最善の方法は、詐欺師の手口を認識し、攻撃の影響を受けているプラットフォームで注意を払うことです。

- 予約に関連するフォームを記入する前に、必ずプラットフォームの公式 Web サイトやアプリを離れていないことを確認してください。予約や支払いを進めるために外部の URL に誘導される場合、詐欺の可能性が高いことを示しています。
- この詐欺は宿泊予約サービスで顧客のアカウント（物件の所有者）が乗っ取られているため、物件所有者に直接連絡して支払い要求が正当であるかどうかを確認しても、詐欺を見破ることはできません。不審な点がある場合は、宿泊予約に利用した予約サービスプロバイダ（**Booking.com**、**Airbnb**）のカスタマーサポートに連絡するか、またはセキュリティの問題を報告してください。
- 宿泊施設を予約する場合も、賃貸する場合も、自分のアカウントが侵害されないように保護するために、強力なパスワードを使用し、利用可能な場合は二要素認証を有効にしてください。

警戒すべきレッドフラグを理解し、さらに、フィッシングサイトに誘導されてしまった場合に備えて、信頼できるマルウェア対策ソリューションをデバイスに導入することを強くお勧めします。

Telekopye とその詐欺グループの手口の詳細については、このテーマを取り上げた最近の**ホワイトペーパー**をご覧ください。

[2] https://thehackernews.com/2024/09/telegram-agrees-to-share-user-data-with.html

ランサムウェア

RaaS の勢力争いに明確な勝者：RansomHub

2024 年上半期に LockBit が解体された後、RaaS（サービスとしてのランサムウェア）での勢力争いが始まり、犯罪グループ間での提携も変化し、技術力の低い新たな参入者もこの争いに割って入るようになりました。

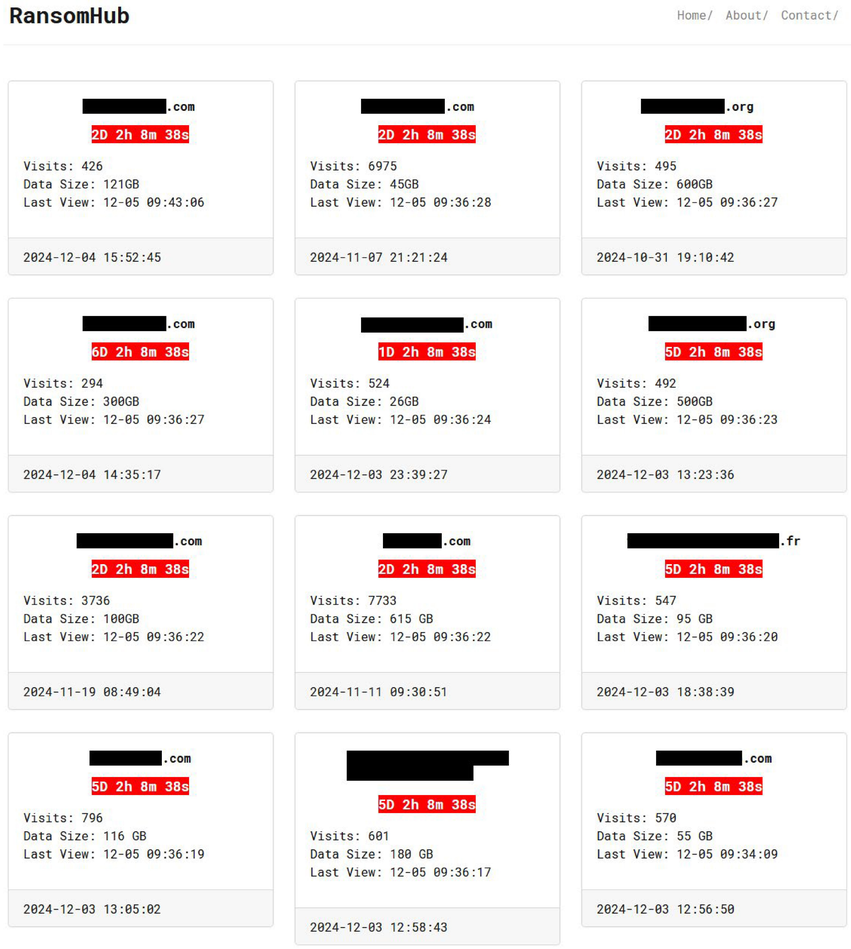
2024 年上半期は、RaaS（サービスとしてのランサムウェア）市場で当時覇権を握っていた LockBit を解体したクロノス作戦のニュースが大きな話題となりましたが、2024 年下半期には法執行機関による後続の対応がいくつか行われました。これには、**1 人の開発者、1 人の防弾ホスティングの管理者、その他 2 人の逮捕**に加え、LockBit の**暗号化専門家**の逮捕も含まれていました。さらに、FBI は **7,000 個の復号鍵**の回収に成功し、多くの被害者が暗号化されたファイルを復号できるようになりました。

LockBit の背後にいる犯罪グループは、築いてきた王国を簡単に手放したくはなく、インフラを再構築し、リークサイトを再開しています。しかし、この犯罪グループの評判とビジネスの関係性は大きく崩れたため、自己顕示のために、あえて偽の被害者をリークサイトに投稿して、依然として影響力があるかのように見せかけるようにしています。

これまで最も大きな影響力があった RaaS が突然崩壊したことで、勢力の空白が短期間生じることとなり、多くのランサムウェアグループがなだれ込むことになりました。最も大きな力を付けたのが RansomHub であり、2024 年 7 月以来、RaaS グループの中でトップの座を占めています。劇的な出来事が起こらなければ、このグループは年末まで首位を維持することになるでしょう。

先頭を切る RansomHub

RansomHub は比較的新しい RaaS グループであり、2024 年 2 月に初めて発見されたが、すぐに最もアクティブなグループにランクインしました。その後の 6 か月間で、RansomHub のリークサイトには **200 以上の被害者**が掲載されるようになり、現在ではその数は 500 近くに上り、Halliburton や Kawasaki Europe などの著名な企業も含まれています。



RansomHub のリークサイト

RansomHub の主なペイロードは Go で記述されており、Linux と Windows の両方のシステムを標的にしています。他の高度なランサムウェアの攻撃者と同様に、RansomHub は EDR（エンドポイント検出および応答）対策を無効化するツールを使用しており、標的システムの検出および保護機能を無力化します。その目的を達成するために、この犯罪グループは Kaspersky のルートキット対策ツールである TDDSKiller など、非常に下位レベルで常駐するソフトウェアを削除するために設計された正規のツールを悪用するか、自ら作成したマルウェアである EDRKillShifter を使用します。

RansomHub の活動が急増し、その被害者が増加していることから、この RaaS は現在解体された LockBit や廃止された BlackCat サービスから、階層の上位に位置していたアフィリエイトを引き寄せた可能性が非常に高いと考えられます。RansomHub がそのブランド力を高めるために、経験の浅いランサムウェアの犯罪グループにも門戸を開いていると ESET は考えています。

ESET のエキスパートの解説

2024 年、RansomHub は、解体された LockBit に取って代わり、市場をリードする RaaS グループとしての地位を確立しました。RansomHub は 2025 年までこの地位を維持することが予測されます。しかし、RaaS は非常に競争の激しいサイバー犯罪界隈であり、犯罪グループはより多くのパートナーを引き付け、収益性を高めようと、アフィリエイトプログラムを変更することも多くあります。競合グループの方がより多くの利益を上げることができることがわかれば、熟練のアフィリエイトは提携先を変更する可能性も十分にあります。

ESET シニアマルウェア研究者、Jakub Souček

CosmicBeetle が敗者となり、RansomHub が勝者か？

後者の例として CosmicBeetle（別名：NONAME）が挙げられます。CosmicBeetle は、2020 年から活動しているスキルレベルが比較的低い犯罪グループです。ESET の調査によると、このグループは当初、古い Scarab ランサムウェアを拡散していましたが、2023 年には GUI での操作が可能な Delphi ベースで独自に開発したランサムウェア ScRansom に切り替えました。

コードにはバグが存在しているほか、攻撃時にマルウェアを手動で制御しなければならず、暗号化ルーチンも複雑すぎるため、ScRansom マルウェアが攻撃に成功する確率は著しく制限されています。

CosmicBeetle は、重要な標的を侵害できた場合でも、暗号化されたデータに対して信頼できる復号ツールを提供することはできませんでした。それが、LockBit になりすまし、身代金要求のメモや、被害者の一部やリークサイトのデザインをコピーして、イメージを磨こうとした理由と考えられます。

RansomHub と CosmicBeetle の関連が ESET に特定されたのは、2024 年 6 月にインドの製造業者に対する攻撃を行ったときでした。このインシデントでは、CosmicBeetle のオペレーターは ScRansom を展開しようとしたが失敗しています。CosmicBeetle のオペレーターはこの失敗を受け、さまざまなサードパーティの EDR 無効化ツールを試すようになりました。これらの試みも徒労に終わると、他の選択肢を模索するようになり、数日後には RansomHub の EDR 無効化ツールとペイロードを利用するようになりました。

特に注意が必要な点は、C:\Users\Administrator\Music\1.0.8.zip に保存されたアーカイブから EDR 無効化ツールを手動で抽出したことでした。これは RansomHub のアフィリエイトが一般に用いる方法ではありませんが、CosmicBeetle が多用しているアプローチです。

ランサムウェアは、通常、フィッシング、脆弱性の悪用、ブルートフォース攻撃、窃取された認証情報、ダウンローダー、またはカスタムマルウェアなどの他の脅威によって侵害された後に利用される最終的なペイロードです。ランサムウェア攻撃の多くは、攻撃のライフサイクルの早い段階で検出されます。攻撃者が被害者の防御機能を回避し、最終的にランサムウェアを展開した場合にのみ、セキュリティ製品はこれらの攻撃をランサムウェアとして分類します。

Embargo が EDR を無効する手段を確立

2024 年下半期に ESET の研究者の注目を集めた RaaS の新たな競合グループが Embargo です。このランサムウェアは 2024 年 6 月に初めて確認され、ランサムウェア界隈で検出される傾向が増加しています。このランサムウェアは、Rust で記述されています。

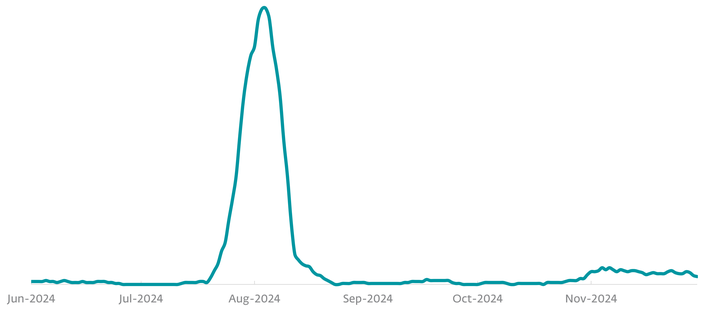
主なツールキットは、MDeployer という名前のローダーと、MS4Killer という名前の EDR 無効化ツールで構成されています。特に注意しなければならないのは、MS4Killer が被害者の環境に合わせてコンパイルされており、被害者が利用するセキュリティソリューションを標的としていることです。MS4Killer は、カーネル内で実行されているセキュリティ関連プロセスを確実に終了させるために、Embargo は脆弱なドライバの持ち込み（BYVOD）と呼ばれる手法を使用しています。

Embargo の際立った特徴は、オペレーターが侵入時でも、ツールをすばやく変更できることです。Embargo が同じインシデントで MDeployer の複数のバージョンを使用したことで、この能力が実証されています。おそらく最初の目的を達成できなかった以前のバグが多いバージョンを置き換えるために異なるバージョンを展開したと考えられます。

企業ではなく一般ユーザーを狙う Magniber

ESET のテレメトリによると、2024 年下半期におけるランサムウェアの検出数は、上半期と比較して世界全体で 23% 以上減少しました。

ESET はまた、2024 年 7 月と 8 月に活動の異常な増加を観察しています。この期間、Magniber ランサムウェアは企業を侵害して膨大な金額を狙うのではなく、エンドユーザーから数千ドルを恐喝するキャンペーンを展開しました。これは前例のないことではなく、CryptoWall、DejaVu（STOP）、または LockBit など、流出したビルダーを使って構築された他の大規模な拡散攻撃が定期的に現れています。



Win/Filecoder.Magniber が 2024 年 7 月と 8 月に急増

Magniber のキャンペーンが非常に異例なのは、その攻撃規模と広範な配信にあります。世界中のユーザーのデータを暗号化しようと試みているものの、多くの検出はポーランド、スロバキア、台湾、ハンガリー、チェコに集中しています。

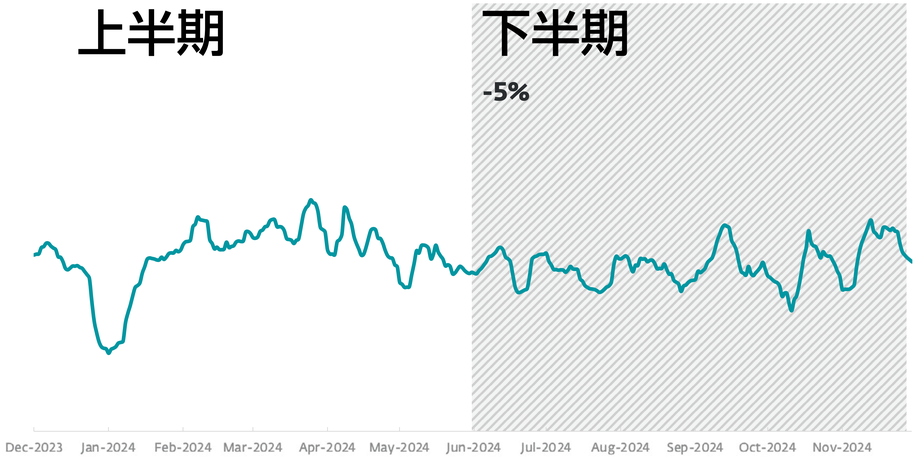
APT グループがランサムウェアを利用する仕組み

2024 年下半期には、国家が支援するサイバースパイグループがランサムウェア攻撃への関与を深めているさらなる証拠も明らかになりました。いくつかのグループは、北朝鮮が支援するサイバー攻撃グループ Moonstone Sleet が使用する FakePenny ランサムウェアのような独自のマルウェアを展開しています。

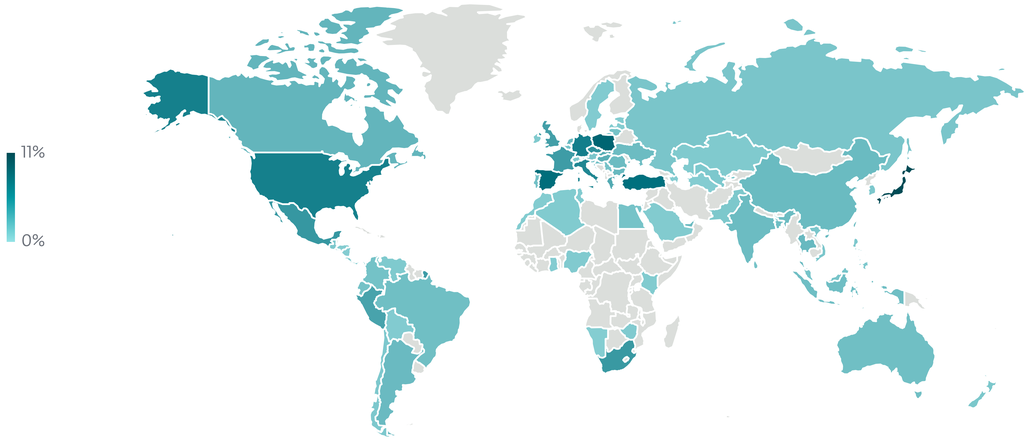
他のグループ、例えば中国と関連する ChamelGang は、暗号化マルウェアを使用してそのスパイ活動から目を逸らさせています。また、副収入の獲得を狙っているグループもあります。その一つはイランと関連する Pioneer Kitten で、初期アクセスブローカー（IAB）として活動し、Ransomhouse や現在は活動を停止している NoEscape、BlackCat などのいくつかのグループと協力していました。北朝鮮とつながりのある Andariel も、サイバー攻撃グループ Play に初期アクセスやアフィリエイトサービスを提供している疑いがあります。Andariel によって以前に侵害された標的のシステムに Play ランサムウェアが展開されているのが確認されています。興味深いことに、Play は公式に RaaS として活動していることを否定しています。そのため、北朝鮮のサイバー攻撃グループと関連があることが、奇妙に感じられます。

脅威テレメトリ（監視データ）

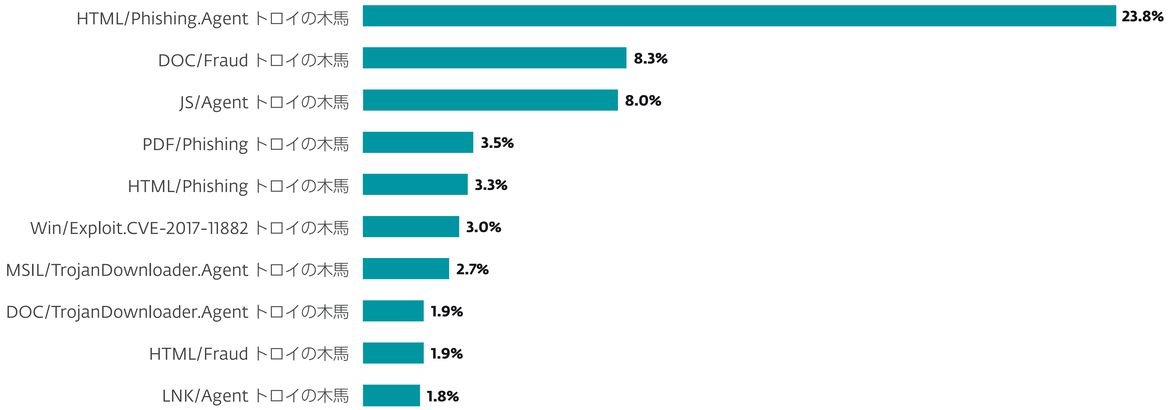
すべての脅威



2024 年上半期～ 2024 年下半期の**脅威全体の検出傾向**、7 日移動平均線

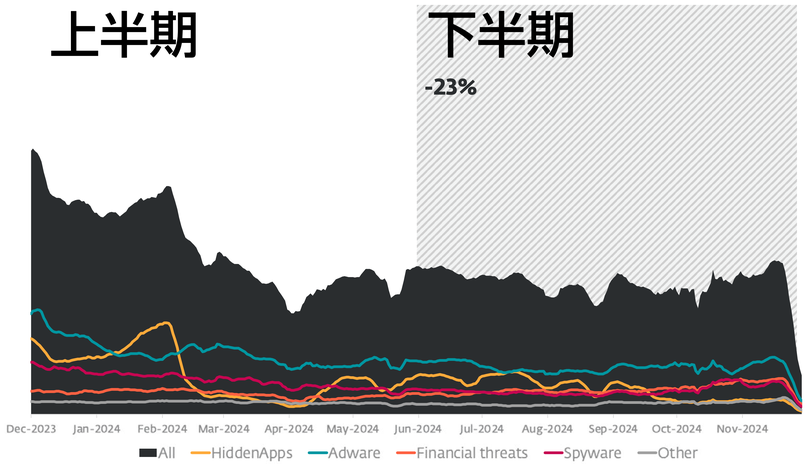


2024 年下半期における**マルウェア検出の地理的な分布**

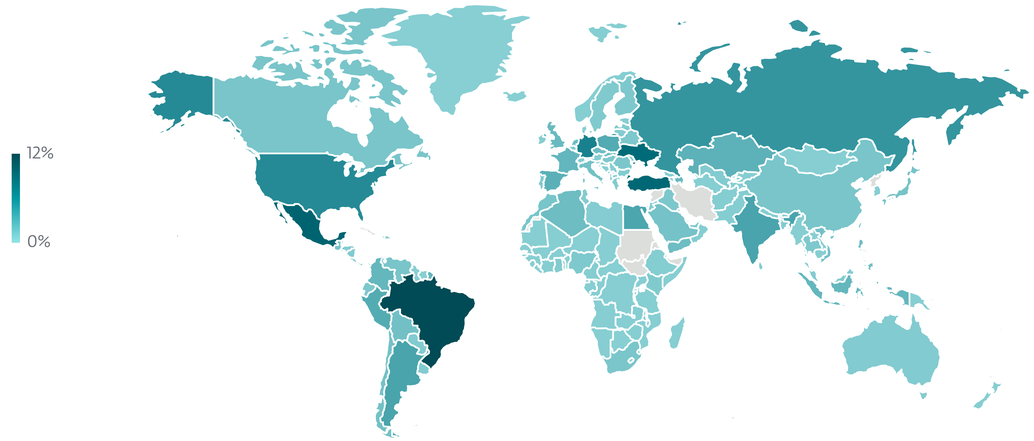


2024 年下半期の**マルウェア検出トップ 10**（マルウェア検出数に占める割合）

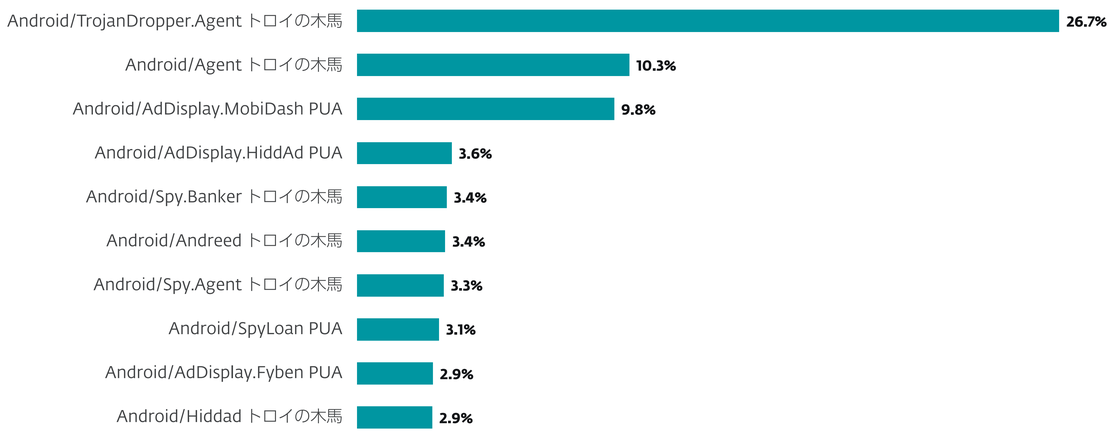
Android



2024 年上半期～ 2024 年下半期の **Android の脅威カテゴリの検出傾向**、7 日移動平均線
（クリッカー、クリプトマイナー、ランサムウェア、詐欺アプリ、SMS トロイの木馬、ストーカーウェアの傾向は、「その他」の傾向線に統合）

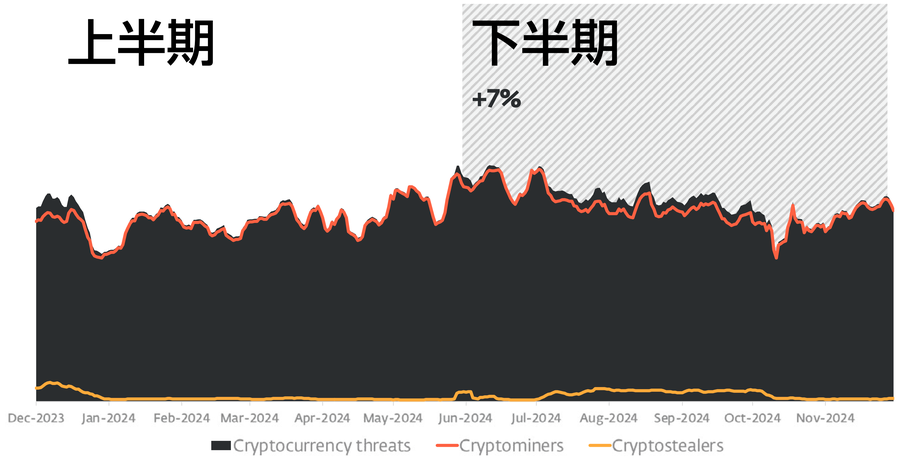


2024 年下半期における **Android の脅威検出の地理的な分布**

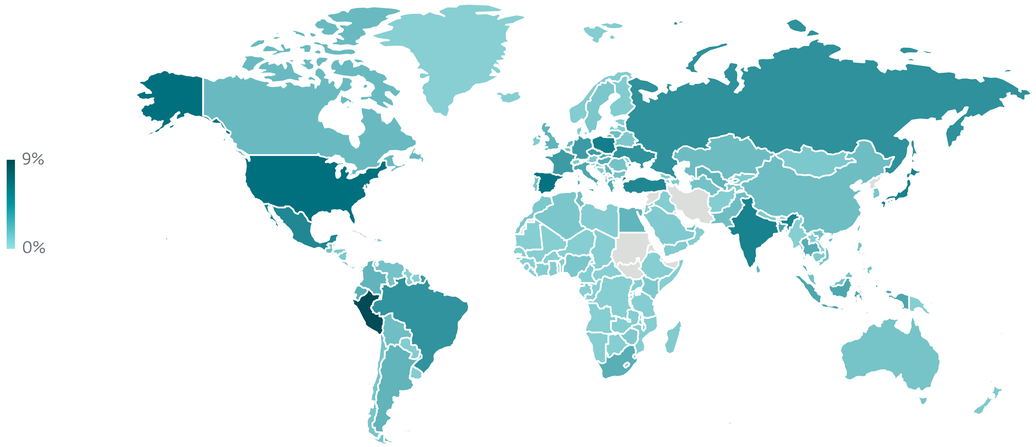


2024 年下半期の **Android の脅威の検出トップ 10**（Android の脅威の検出数に占める割合）

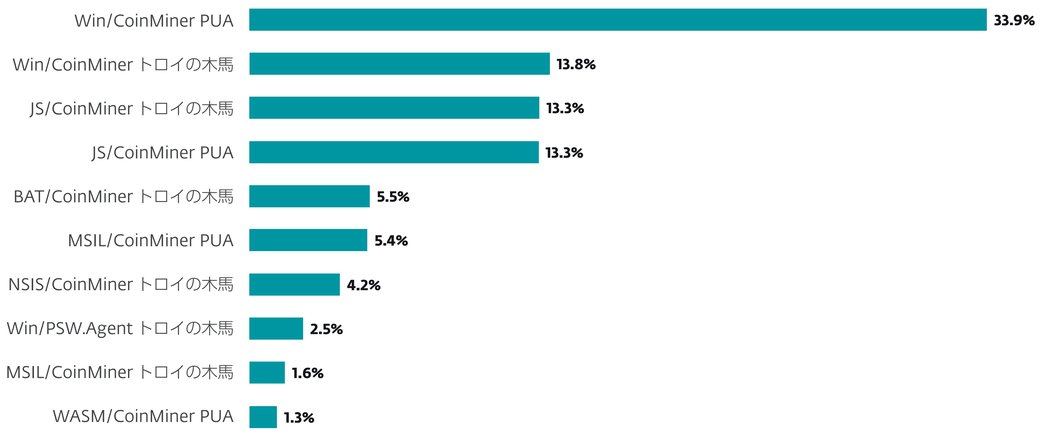
暗号通貨の脅威



2024 年上半期～ 2024 年下半期の**暗号通貨の脅威の検出傾向**、7 日移動平均線

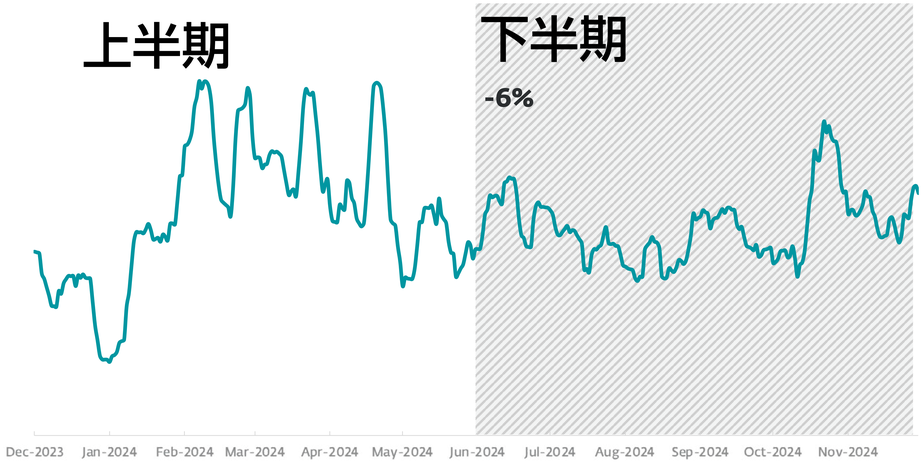


2024 年下半期における**暗号通貨の脅威検出の地理的な分布**

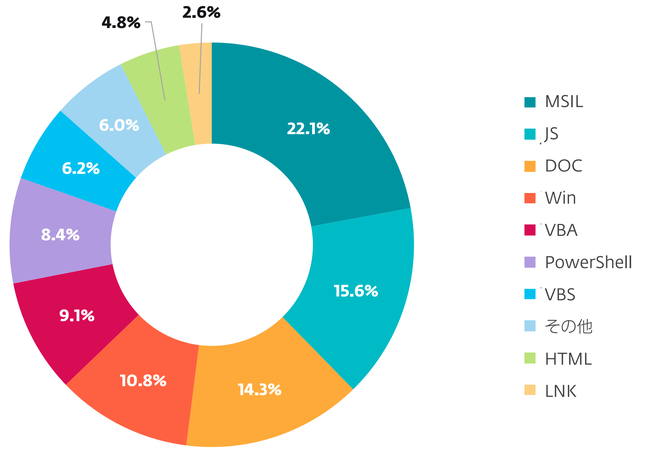


2024 年下半期の**暗号通貨の脅威の検出率トップ 10**（暗号通貨の脅威の検出数に占める割合）

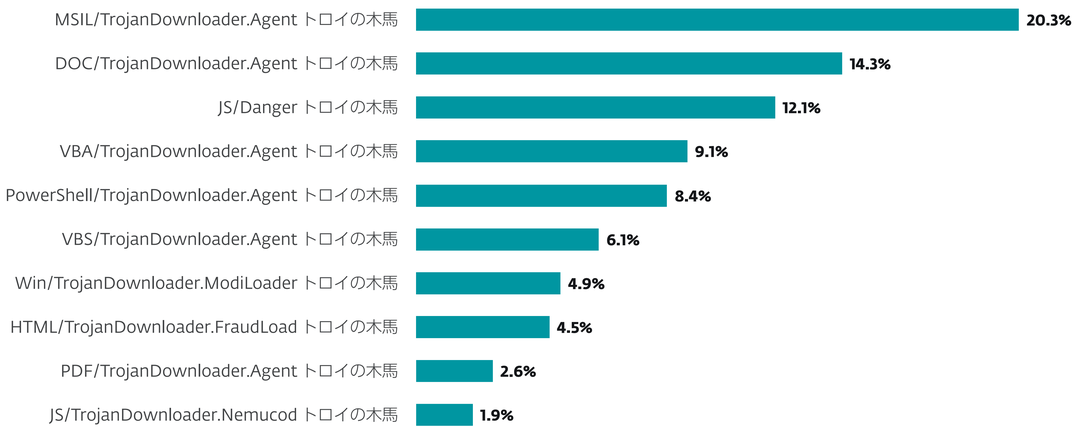
ダウンローダー



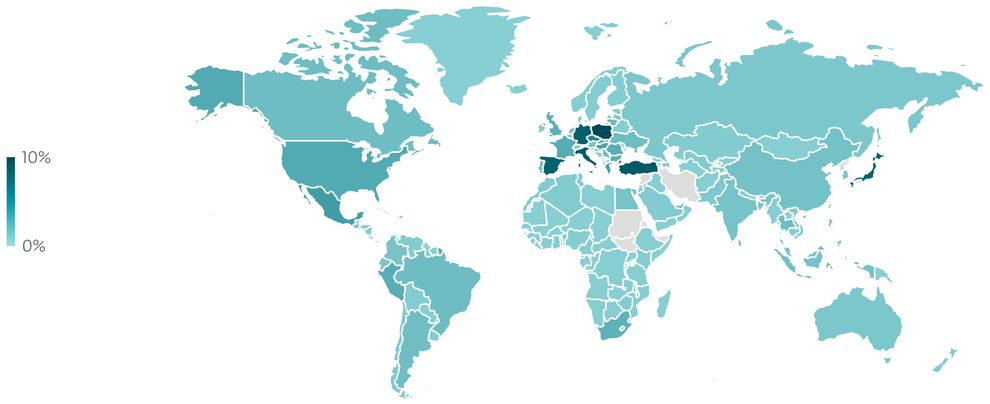
2024 年上半期～ 2024 年下半期の**ダウンローダーの検出傾向**、7 日移動平均線



2024 年下半期の**ダウンローダータイプ別の検出率**

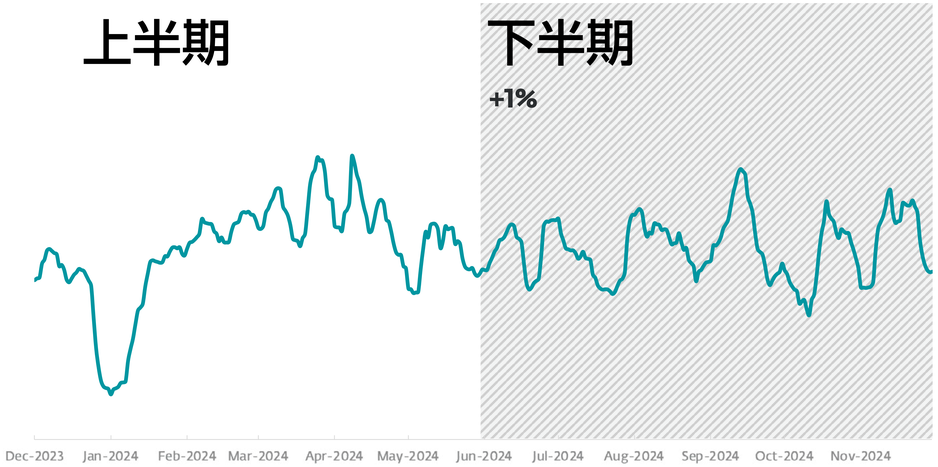


2024 年下半期の**ダウンローダーの検出トップ 10**（ダウンローダー検出数に占める割合）

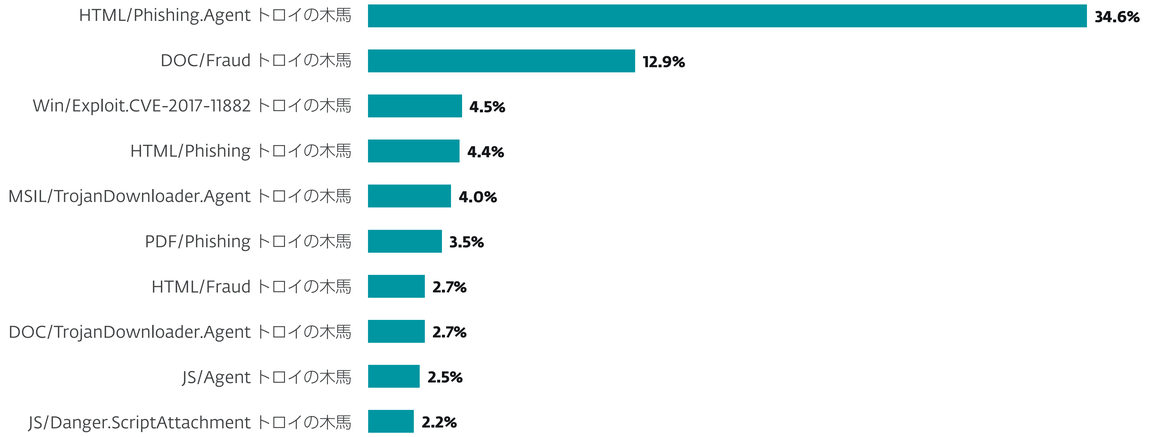


2024 年下半期における**ダウンローダー検出の地理的な分布**

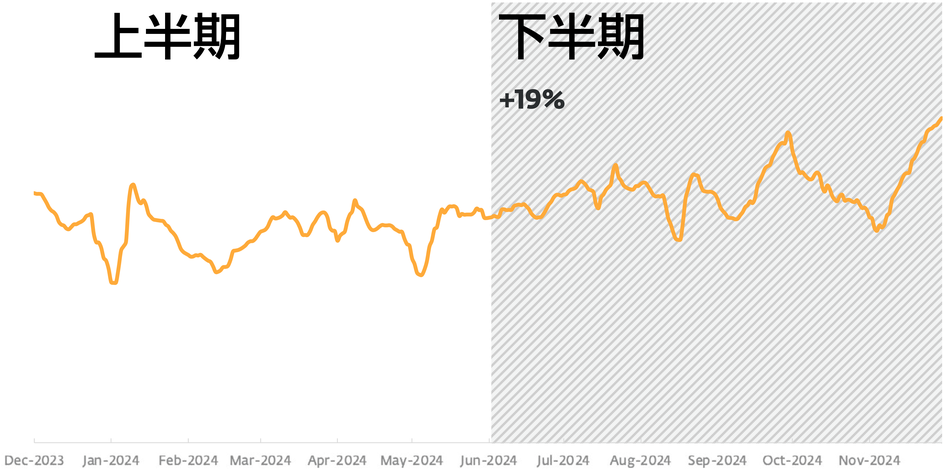
メールに関する脅威



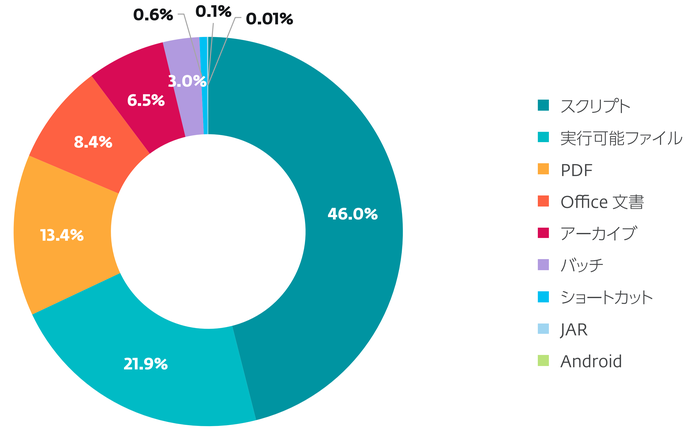
2024 年上半期～ 2024 年下半期の**悪意のあるメールの検出傾向**、7 日移動平均線



2024 年下半期に検出された**メールの脅威トップ 10**

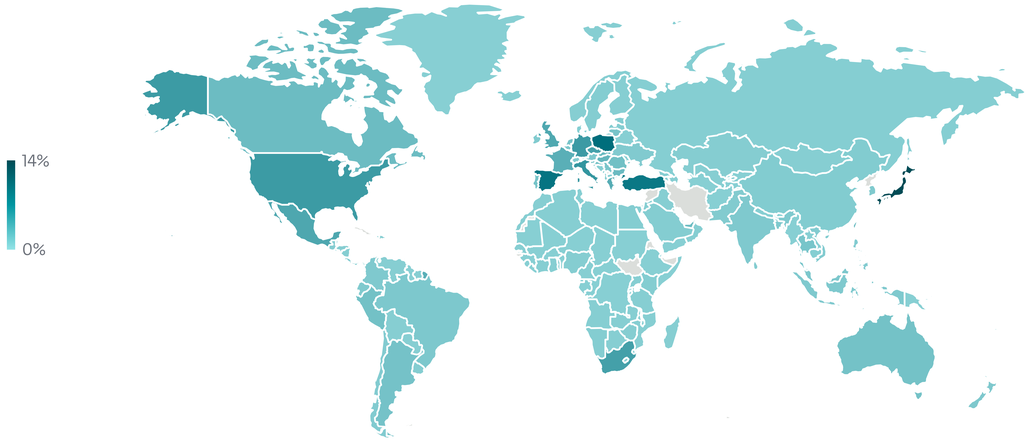


2024 年上半期～ 2024 年下半期の**スパムの検出傾向**、7 日移動平均線



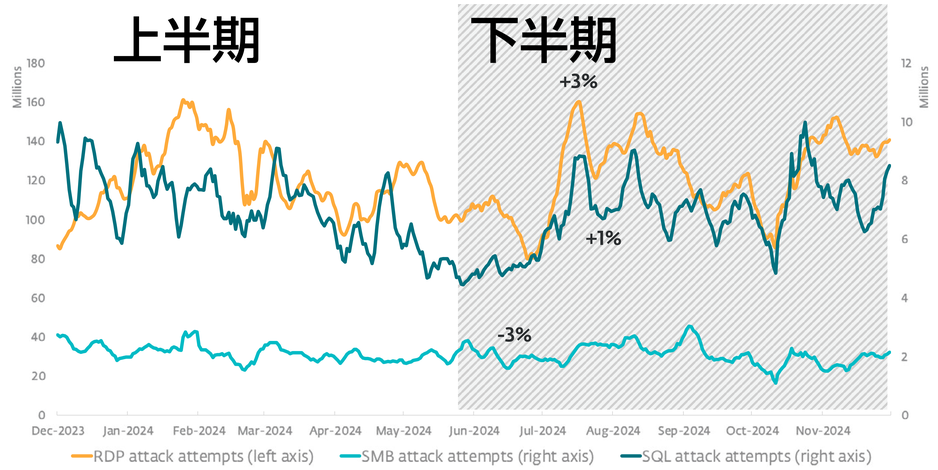
2023 年下半期の**主な悪意のあるメールの添付ファイルのタイプ**

メールに関する脅威

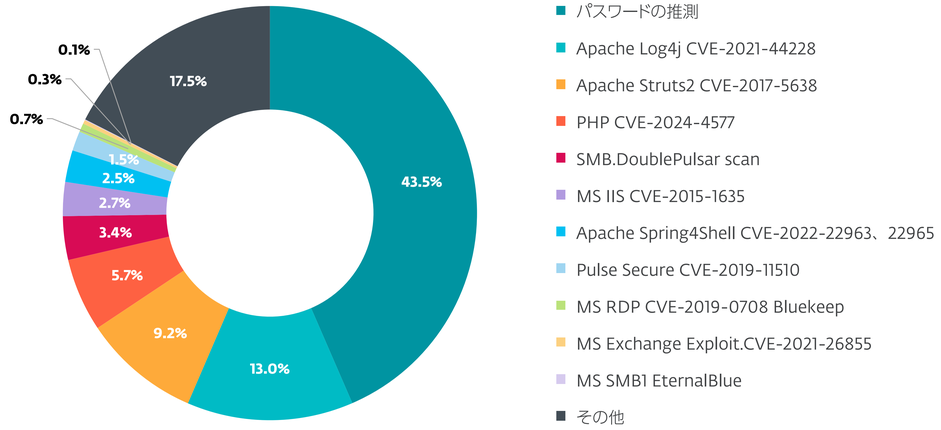


2024 年上半期における**メール脅威の検出の地理的な分布**

エクスプロイト

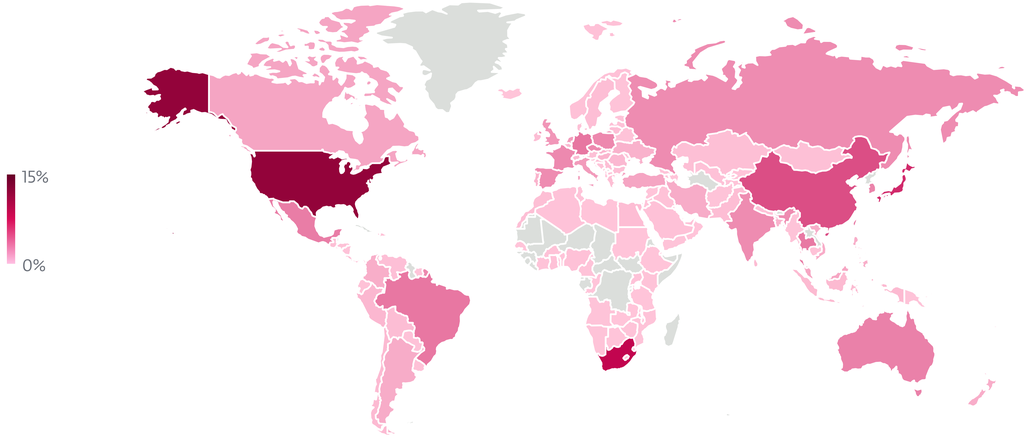


2024 年上半期および 2024 年下半期における **RDP、SMB、SQL 攻撃試行の傾向**、7 日間移動平均線

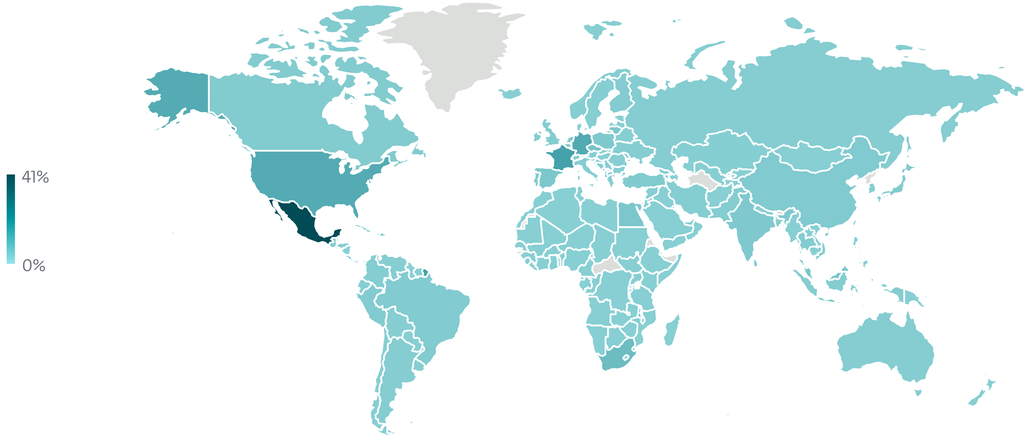


2024 年下半期にユニーククライアントから報告された**外部からのネットワークへの侵入方法**

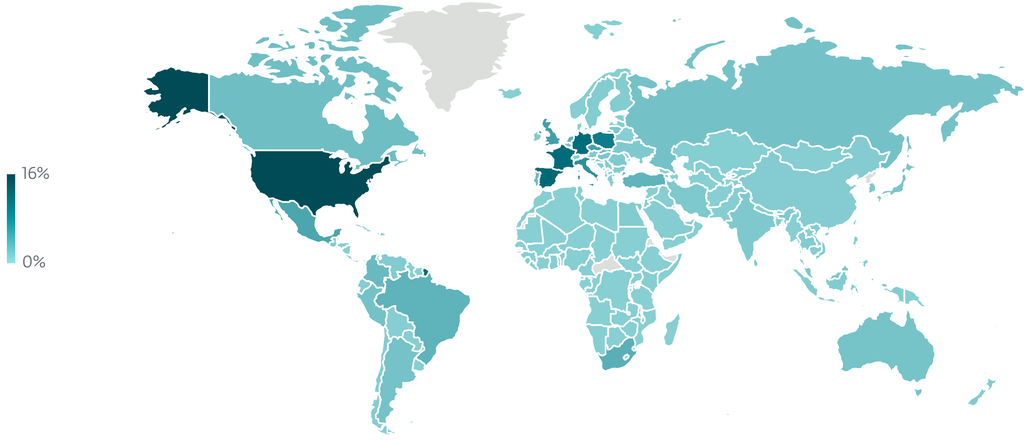
エクスプロイト



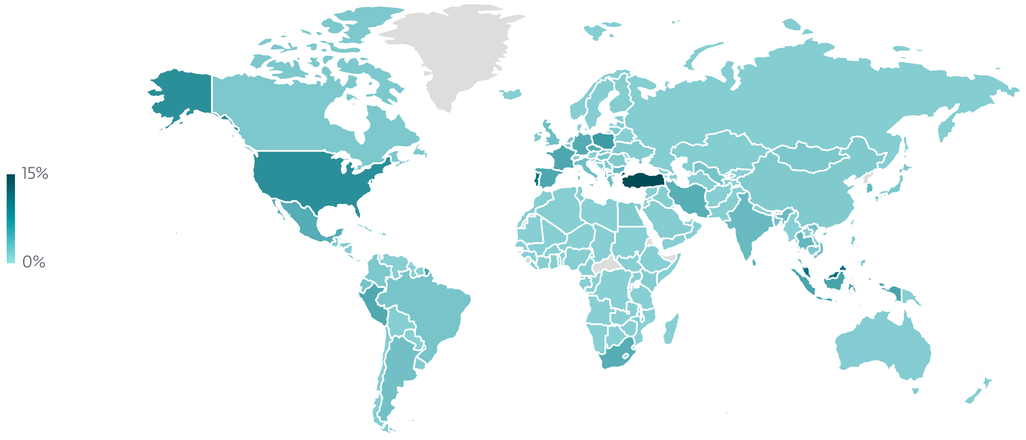
2024 年下半期に **RDP パスワード推測攻撃を実行したソースの地理的な分布**



2024 年下半期に **SMB パスワード推測攻撃が実行された標的の地理的な分布**

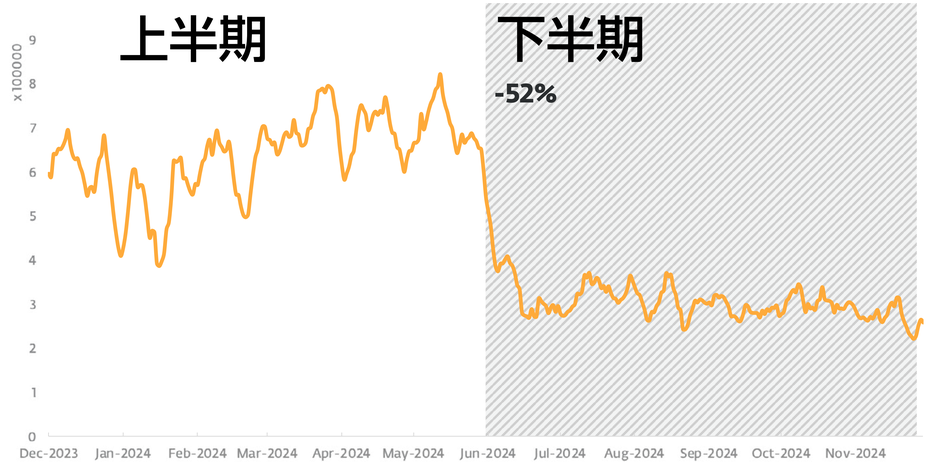


2024 年下半期に **RDP パスワード推測攻撃が実行された標的の地理的な分布**

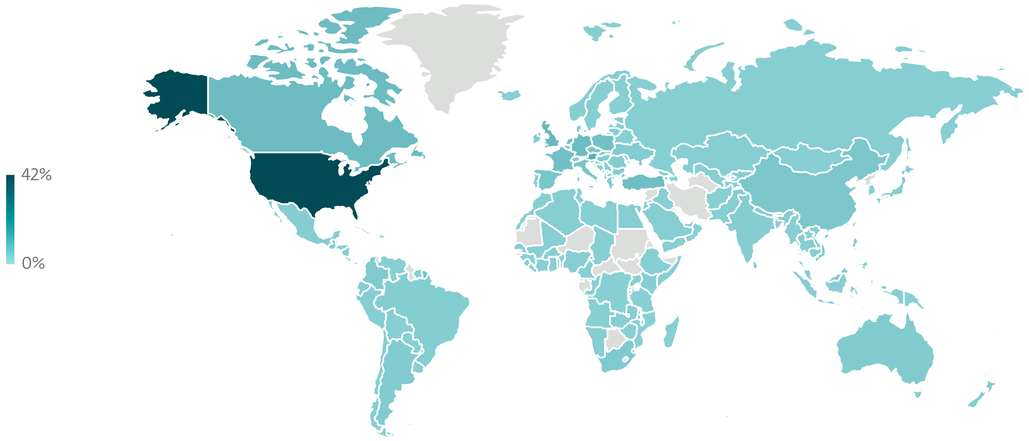


2024 年下半期に **SQL パスワード推測攻撃が実行された標的の地理的な分布**

エクスプロイト

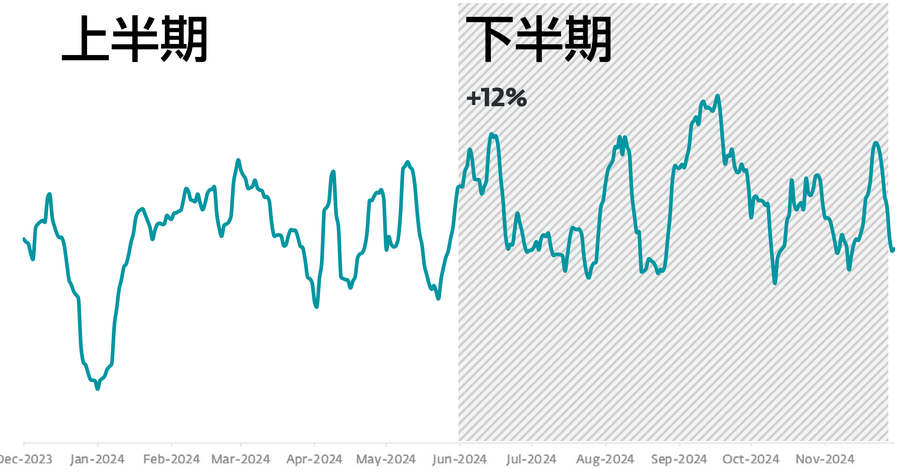


2024 年上半期～ 2024 年下半期における **Log4Shell 攻撃試行の検出傾向**、7 日間移動平均線

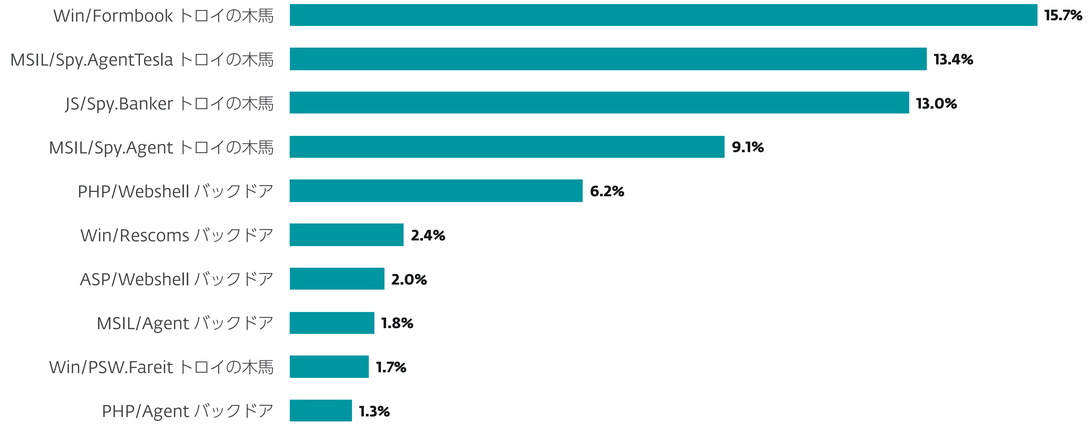


2024 年下半期における **Log4Shell 攻撃試行の地理的分布**

情報窃取型マルウェア

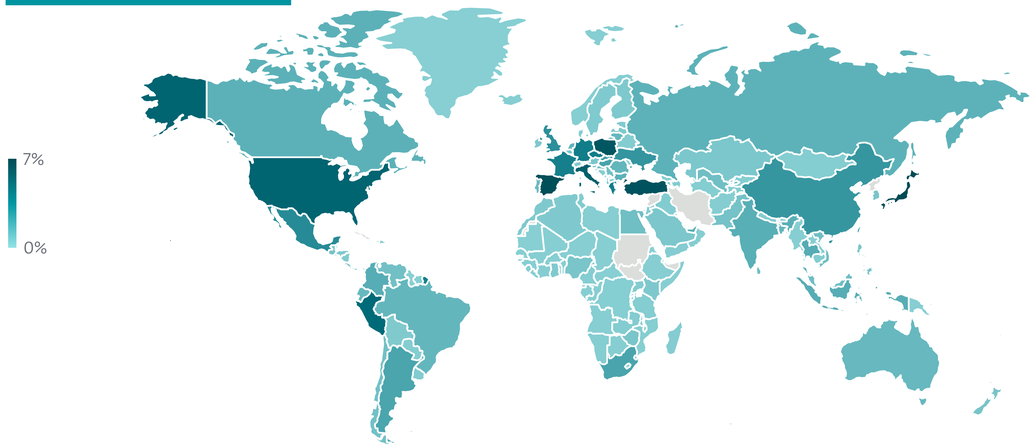


2024 年上半期～ 2024 年下半期の**情報窃取型マルウェアの検出傾向**、7 日間移動平均線



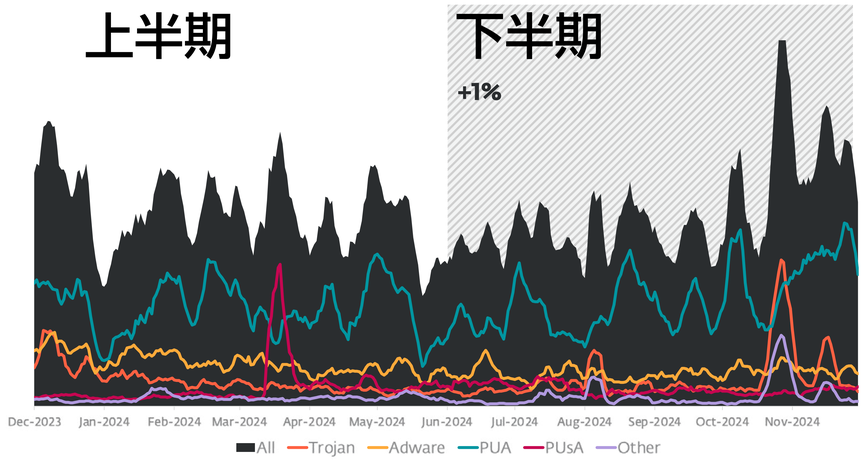
2024 年下半期における**情報窃取型マルウェアのトップ 10**（情報窃取型マルウェアの検出に占める割合）

情報窃取型マルウェア

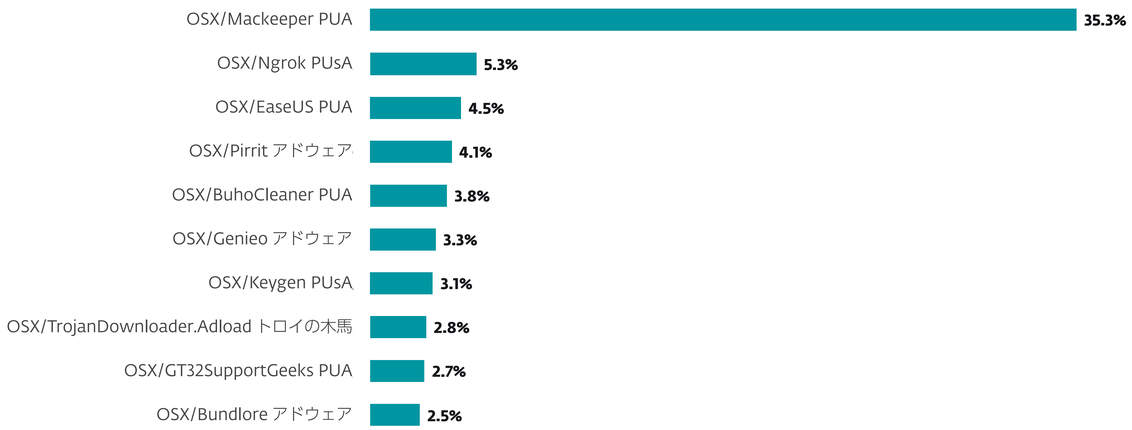


2024 年下半期における**情報窃取型マルウェアの検出の地理的な分布**

macOS

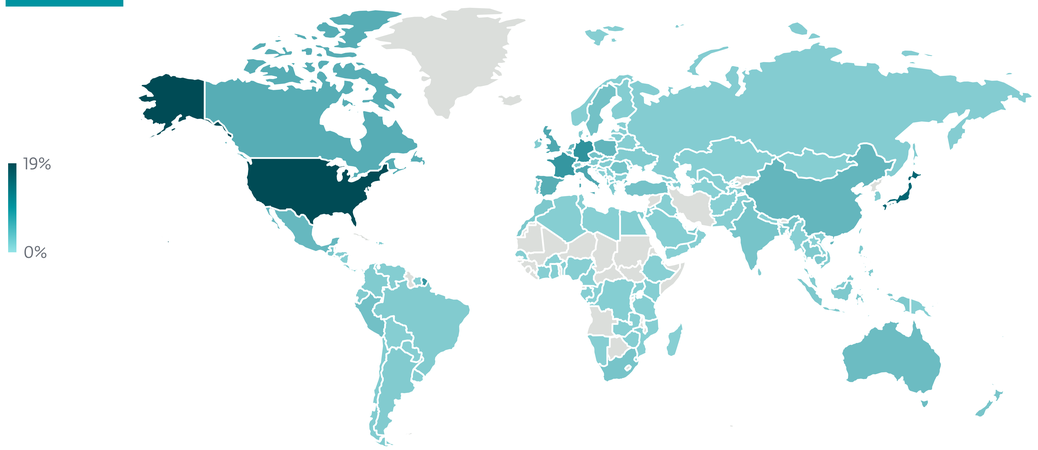


2024 年上半期～ 2024 年下半期の **macOS の脅威の検出傾向図**、7 日移動平均線



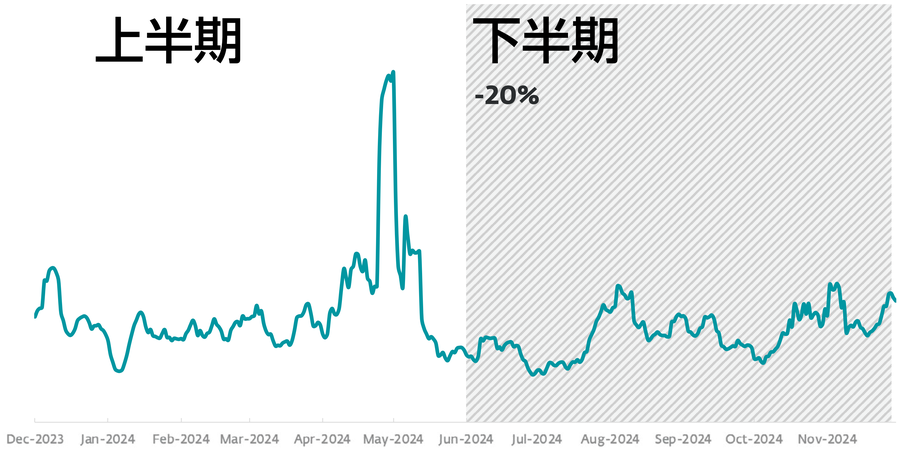
2024 年下半期の **macOS の脅威の検出トップ 10**（マルウェア検出数に占める割合）

macOS

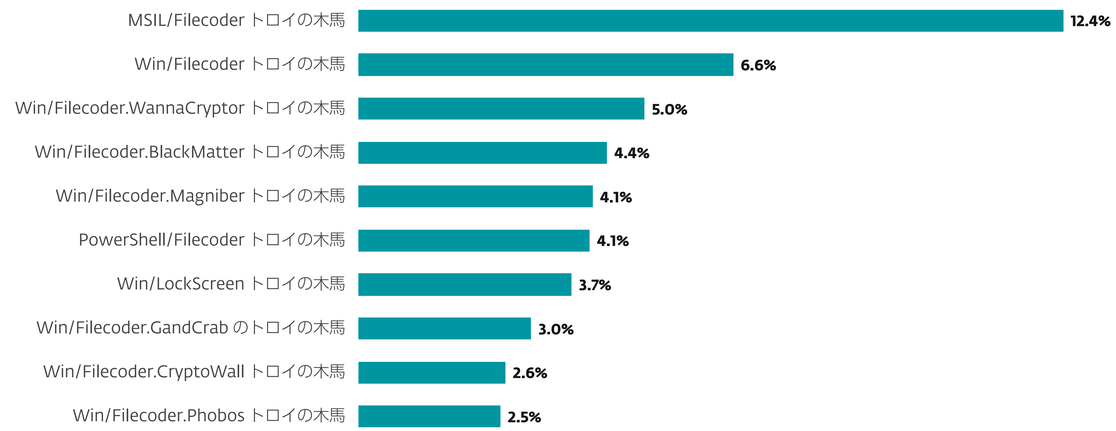


2024 年下半期における **macOS の脅威の検出の地理的な分布**

ランサムウェア

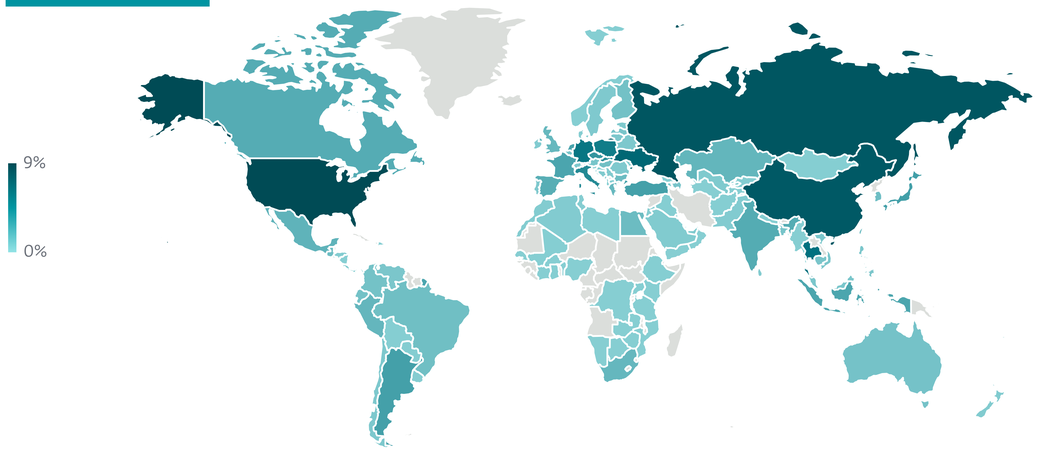


2024 年上半期～ 2024 年下半期の**ランサムウェアの検出傾向**、7 日移動平均線



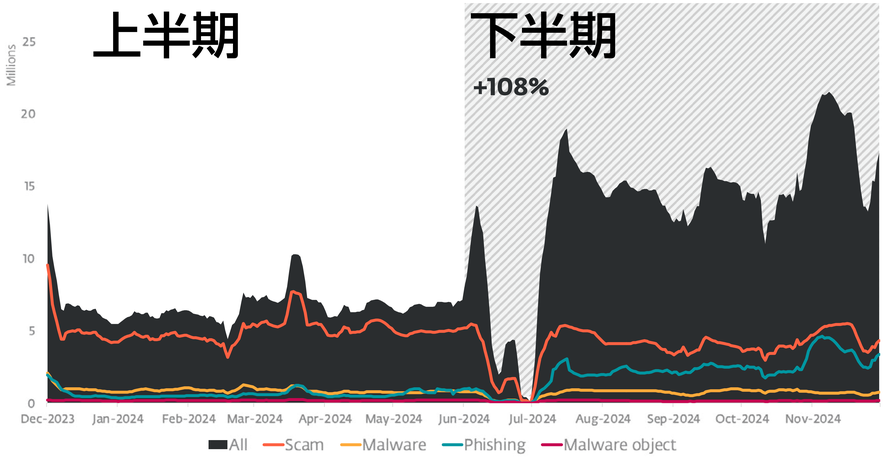
2024 年下半期における**ランサムウェア検出のトップ 10**（ランサムウェア検出数に占める割合）

ランサムウェア

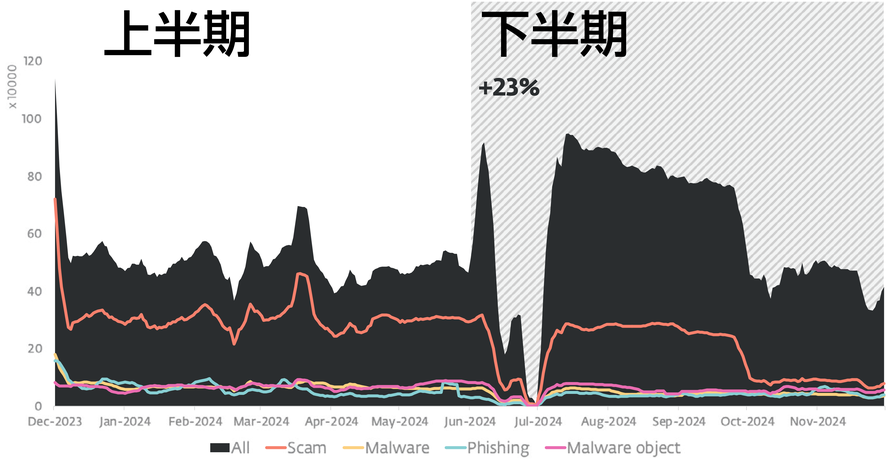


2024 年下半期における**ランサムウェアの検出の地理的な分布**

Web に関する脅威



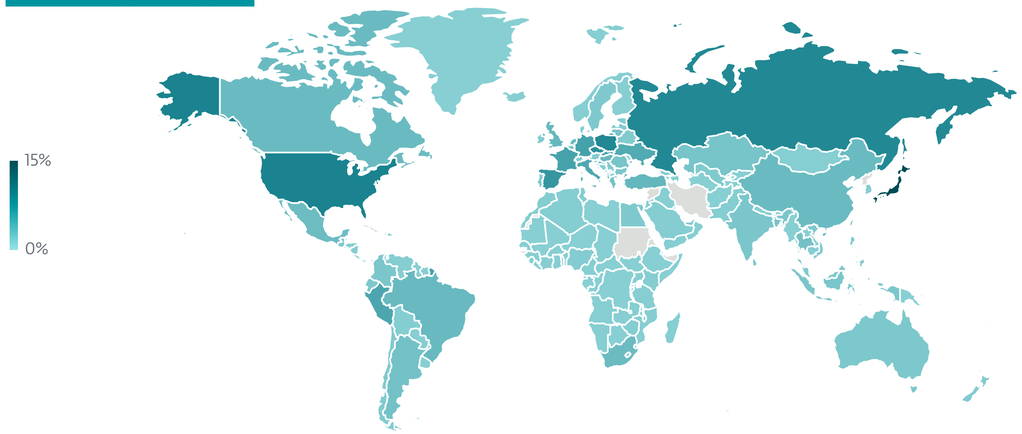
2024 年上半期～ 2024 年下半期に**ブロックされた Web 脅威の傾向**、7 日移動平均線



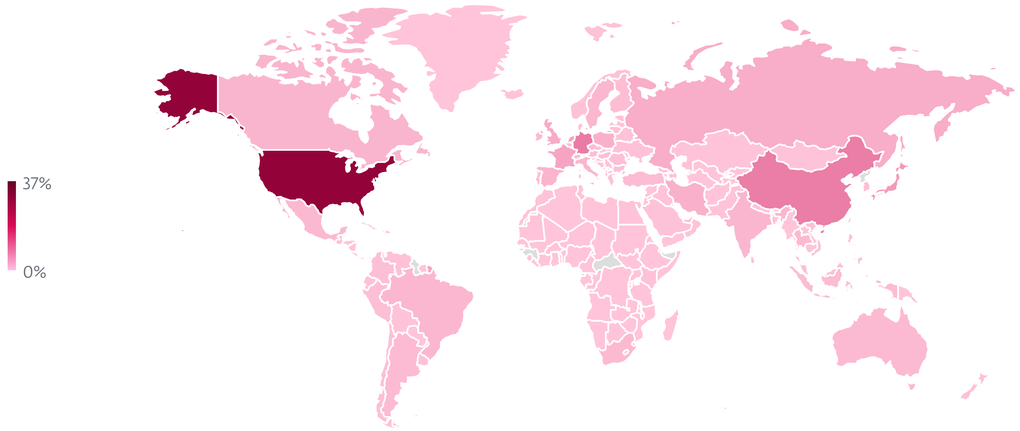
2024 年上半期～ 2024 年下半期に**ブロックされたユニーク URL の傾向**、7 日移動平均線 [3]

[3] 2024 年 6 月後半から 7 月初旬にかけて検出数が急減したのは、ESET の統計データベースへの接続に関する問題が短期間発生したことが原因です。この問題は脅威の保護機能には影響を与えていません。

Web に関する脅威



2024 年下半期における**ブロックされた Web 脅威の検出数の世界的な分布**



2024 年下半期における**ブロックされたドメインホストの検出数の世界的な分布**

調査レポート

Android アプリに AridSpy を仕込む Arid Viper

ESET の研究者は、Arid Viper のスパイ活動キャンペーンでエジプトとパレスチナの Android ユーザーにトロイの木馬化されたアプリが拡散されていることを発見しました。

Hamster Kombat ゲームのプレイヤーを狙う脅威

ESET の研究者は、Hamster Kombat という人気のクリックゲームを悪用する脅威を発見しました。

WPS Office に影響する任意コード実行の 2 つの脆弱性の解析

本ブログでは、CVE-2024-7262 と CVE-2024-7263 を解析した結果についてお伝えします。

ESET Research のポッドキャスト：:2023 年 第 4 四半期～ 2024 年第 1 四半期の APT 活動レポート

中国の IT サービス企業の I-SOON（Anxun）から流出したデータから、この企業が中国政府のためにサイバースパイ活動に関与していることが確認されました。また、イランとつながりのあるグループは 2023 年のハマス主導によるイスラエルへの攻撃を受けて、攻撃的な戦術を強化しています。

ポーランドの中小企業を狙った ModiLoader による フィッシング攻撃が継続

ESET の研究者は、2024 年 5 月にポーランドの中小企業をターゲットにした複数の広範なフィッシングキャンペーンを検出し、さまざまなマルウェア系統を配信していることを確認しました。

ESET Research のポッドキャスト：HotPage

ESET の研究者は、最近発見されたアドウェア「HotPage」について解説しています。このアドウェアは、最も高い権限が付与されているにも関わらず脆弱な Microsoft が署名したドライバを搭載しています。

HotPage：脆弱性を導入し、広告を挿入する署名付きのドライバ

多くの攻撃用のドアを開く、巧妙な中国製のブラウザインジェクターに関する調査。

思いがけないリスクが潜む - PWA アプリケーションのフィッシング

ESETのアナリストがAndroidとiOSユーザーに対する新しいフィッシングの手法を詳細に伝えています。

CosmicBeetle の活動の進化：RansomHub のアフィリエイトとして活動か？

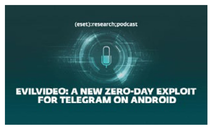
CosmicBeetle、独自のランサムウェアを改良し、RansomHub のアフィリエイトとして活動を活発化

呪われたテープ：Android 版の Telegram の EvilVideo 脆弱性の攻撃

ESET の研究者は、Android 版 Telegram にゼロデイ脆弱性を発見しました。この脆弱性を攻撃することにより、動画に見せかけた悪意のあるファイルを送信することが可能になります。

NFC トラフィックをリレーして現金を窃取する NGate Android マルウェア

ESET Research が発見した Android マルウェアは、被害者の携帯電話を経由して、被害者の支払いカードの NFC データを ATM で待機している犯人のデバイスに中継します。



ESET Research のポッドキャスト：EvilVideo

ESET の研究者は、Android 版 Telegram にゼロデイ脆弱性を発見しました。この脆弱性を攻撃することにより、動画に見せかけた悪意のあるファイルを送信することが可能になります。

Gamaredon によるサイバースパイ：2022 年と 2023 年にウクライナを監視するために使用されたツールセットの分析

ESET Research は、ウクライナを中心としたサイバースパイ活動に使用されている Gamaredon のツールセットについて技術的な分析を包括的に行いました。

ESET Research のポッドキャスト：CosmicBeetle

バグの多い悪意のあるツールを使用している技術力の低いサイバー犯罪グループが、世界各国の中小企業をどのように侵害しているのかをご確認ください。

Embargo ランサムウェア：Rust ベースの新しいツールキット

新たなランサムウェアグループである Embargo、Rust ベースの新しいツールキットをテストしながら展開

サイバー攻撃グループ CeranaKeeper、タイを標的に活動を活発化

ESET Research は、中国とつながりのある新たなサイバー攻撃グループ CeranaKeeper のツールと活動の詳細について説明しています。特に、東南アジアでの大規模なデータ収集活動に焦点を当てて説明します。

CloudScout：Evasive Panda によるクラウドサービスの情報収集

ESET の研究者は、Evasive Panda がクラウドサービスにアクセスしてデータを取得するために使用している、これまで検出・文書化されていなかったツールセットを発見した。

WolfsBane の正体：Gelsemium の Linux 版、Gelsevirine

このブログでは、ESET の研究者がこれまで知られていなかった Linux バックドアを分析した結果をお伝えします。このバックドアは、中国とつながりのある Gelsemium グループが使用する既知の Windows マルウェアと Project Wood バックドアにも関連しています。

エアギャップで隔離されているシステムへの攻撃：政府の保護機能を突破する GoldenJackal

ESET Research は、GoldenJackal として知られるサイバースパイグループがエアギャップで隔離されたシステムを侵害するために使用される 2 つの異なるツールセットを分析しました。

RedLine の悪意ある活動の実態：悪名高い情報窃取型マルウェアのバックエンドの分析

国際捜査機関による RedLine Stealer の摘発を受け、ESET の研究者はこの情報窃取型マルウェアのバックエンドモジュールに関する調査結果を公表しました。

RomCom、実環境で Firefox と Windows のゼロデイ脆弱性を攻撃

ESET Research は、これまで知られていなかった Mozilla 製品と Microsoft Windows の脆弱性を組み合わせたゼロクリックエクスプロイトを悪用している実環境の攻撃について分析した結果を公開しました。

Telekopye の方向転換：ホテル予約詐欺を通じて観光客を標的に

ESET Research は、オンラインマーケットプレイスのユーザーを欺くために使用されている詐欺ツールキット「Telekopye」についての新たな発見について説明しています。Telekopye は、最近宿泊施設予約プラットフォームを標的にしていることも明らかになりました。

ESET Research のポッドキャスト：Gamaredon

ESET の研究者は、APT グループ Gamaredon について説明し、典型的な作戦の手順、独自の標的プロファイル、広範なツールコレクションとソーシャルエンジニアリングの戦術、さらに、推測される活動地域について詳述しています。

Bootkitty：Linux 環境向けの初の UEFI ブートキットの分析

ESET の研究者は、Linux システム向け設計された最初の UEFI ブートキットを分析しました。

2024 年上半期 ESET サイバーセキュリティ脅威レポート

ESET のテレメトリ（監視データ）と ESET 脅威検出と調査の専門家から見た 2024 年上半期の脅威環境

2024 年第 2 四半期～ 2024 年第 3 四半期の ESET APT 活動レポート

ESET APT 活動レポートは、2024 年第 2 四半期および 2024 第 3 四半期に ESET Research が調査および分析した APT グループの活動の概要をまとめています。

クレジット

チーム

Peter Stančík、チームリーダー
Klára Kobáková、マネージングエディター

Aryeh Goretsky
Branislav Ondrášik
Bruce P. Burrell
Hana Matušková
Nick FitzGerald
Ondrej Kubovič
Rene Holt
Zuzana Pardubská

貢献者

Alexandre Côté-Cyr
Dušan Lacika
Igor Kabina
Jakub Kaloč
Jakub Osmani
Jakub Souček
Jan Holman
Juraj Horňák
Lukáš Štefanko
Martin Jirkal
Michal Malík
Ondřej Novotný
Radek Jizba

本レポートにおけるデータについて

本レポートに示されている脅威の統計と傾向は、ESET のグローバルテレメトリ（監視チーム）データに基づいています。特に明記されていない限り、検出に含まれるデータは標的となったプラットフォーム別にはなっていません。

さらに、詳細なプラットフォーム固有のセクションと「暗号通貨の脅威」のセクションで記載されている場合を除いて、これらのデータでは望ましくないアプリケーション（PUA）、潜在的に危険なアプリケーション、およびアドウェアの検出数が除外されています。

これらのデータは、情報の価値を最大化するため、偏った見方を緩和するために適正に処理されています。

本レポートのほとんどのグラフは、絶対数ではなく、検出傾向を示しています。このような表示を行っている主な理由は、ほかのテレメトリデータと直接比較する場合にデータについてさまざまな誤解を招きやすいためです。ただし、有益であると思われる場合は、絶対値または桁数を表示しています。

ESET について

攻撃を未然に防止するための最先端のデジタルセキュリティを提供しています。ESET は、AI と人間の専門知識の両方を取り入れて、既知のサイバー脅威や新たなサイバー脅威を防止し、企業、重要インフラ、そしてユーザーを保護します。AI を活用したクラウドファーストの ESET のソリューションとサービスは、エンドポイント、クラウド、モバイル保護のいずれの分野においても、優れた利便性と効果を発揮します。ESET のテクノロジーには、堅牢な検知・応答、極めて安全な暗号化、そして多要素認証が含まれます。24 時間 365 日体制でリアルタイムに攻撃を防ぎ、お客様一人ひとりに合わせた強力なサポートを提供し、ユーザーを保護し、サイバー攻撃による業務の中断を防止します。デジタル環境が常に進化し続ける中で、セキュリティにも先進的なアプローチが求められています。ESET は、研究開発センターと強力なグローバルなパートナーネットワークを活用し、世界最高クラスの調査研究と強力な脅威インテリジェンスを提供しています。詳細については、**www.eset.com/jp** をご覧ください。また、**LinkedIn**、**Facebook**、および **X** で最新の情報をご確認ください。

WeLiveSecurity.com

@ESETresearch

ESET GitHub

ESET 脅威レポートと APT アクティビティレポート

Digital Security
Progress. Protected.

(eset):research