Digital Security
Progress. Protected.

ESET 脅威レポート

2024 年上半期

2023 年 12 月～ 2024 年 5 月

(eset):research

目次

エグゼクティブサマリー

Android iOS 金融関連の脅威

アジアから新天地へと被害を拡大させている GoldDigger

Android および iOS の両方を攻撃できる新たなトロイの木馬が、アジア地域のユーザーから顔認識データを窃取し、金融取引の認証で使用するためのディープフェイク動画を作成しています。Android バージョンの古い亜種もラテンアメリカと南アフリカへと活動範囲を拡大しています 。

Linux ボットネット 情報窃取型マルウェア

Linux サーバーを侵害しながら生き続ける Ebury

Ebury のオペレータが、金銭的な利益を最大化するためのツールを導入し、何十万台ものサーバーを侵害しています。

AI Web に関する脅威 情報窃取型マルウェア

生成 AI アシスタントを装うマルウェア

情報窃取型マルウェアをインストールするために、偽の生成 AI アシスタントが利用されています。その背景には何があるのでしょうか？

Web に関する脅威

WordPress プラグインの脆弱性が増加し、悪意のあるスクリプトも増加

2024 年上半期には 2 万以上の Web サイトに悪意のある JavaScript コードが挿入され侵害されました。

情報窃取型マルウェア Web に関する脅威 ゲーム

攻撃者の台本に沿って進むストーリー：ゲーマーを捕食するサイバー犯罪者

ゲームファンの個人情報を狙う情報窃取型マルウェア。

ダウンローダー

配信方法を変更しカムバックしたダウンローダー

2022 年の激動期を経て、ダウンローダーの脅威が徐々に復活しつつあります。

ランサムウェア

世界的な解体作戦後の LockBit にみえる状況変化

クロノス作戦が実施された後、リークした LockBit の作成ツールを悪用するサイバー攻撃者が増加し、LockBit ランサムウェアグループを取り巻く状況は厳しくなっています。

序文

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

この 6 か月間、Android を標的とする金融関連の脅威（モバイルバンキングの資金を狙うマルウェア）に大きな変化が見られています。従来型のバンキングマルウェアも使用されていますが、最近では暗号通貨を盗み出すマルウェアも登場しています。

GoldPickaxe は、顔認識のデータを窃取し、マルウェアのオペレータが不正に認証するために使用するディープフェイクビデオを作成して金融取引を行う新しいモバイルマルウェアです。この脅威には、Android と iOS を攻撃するバージョンがあり、ローカライズされた悪意のあるアプリを通じて東南アジアのユーザーを標的にしています。ESET の研究者がこのマルウェアファミリーを調査したところ、GoldDiggerPlus と呼ばれる GoldPickaxe の古い Android バージョンの亜種が、ラテンアメリカや南アフリカのユーザーを積極的に標的にしており、これらの地域にも活動範囲を広げていることが判明しました。

情報窃取型マルウェアも、時代に合わせて生成 AI ツールになりすますようになりました。 2024 年上半期に Rilide Stealer は、OpenAI の Sora や Google の Gemini などの生成 AI アシスタントの名前を悪用し、ユーザーを誘いだそうとしていることが確認されています。別の悪意あるキャンペーンでは、情報窃取型マルウェアの Vidar は、AI 画像生成ツールである Midjourney の Windows デスクトップアプリケーションを装っていましたが、Midjourney の AI モデルは Discord からしか入手できません。2023 年以降、サイバー犯罪者が AI を悪用するケースが増加していますが、この傾向は今後も継続すると考えられます。

いわゆる「ガチ勢」と呼ばれる熱心なゲーマーは、ゲーム開発元が提供するゲーム環境から飛び出してさまざまなゲーム情報を収集するものですが、情報窃取型マルウェアによってこよなく愛する趣味が台無しにされる場合もあります。いくつかのオンラインマルチプレイヤーゲームはクラックされており、不正なツールが使用されています。また最近、Lumma Stealer や RedLine Stealer などの情報窃取型マルウェアが含まれていることも明らかになっています。

2024 年上半期にスペイン、日本、ドイツを対象した一度限りのキャンペーンが実行され、RedLine Stealer の検出率が急上昇したケースがありました。この情報窃取型マルウェアはサービスとして提供されていましたが、2023 年に解体作戦が実行されたことで積極的な開発は行われていないと思われていました。しかし、最近の攻撃は非常に大規模であり、2024 年上半期の RedLine Stealer の検出数は 2023 年下半期よりも約 33% 上回っています。

WordPress プラグインの脆弱性を悪用していることが広く知られているサイバー攻撃グループ「Balada Injector」は、2024 年上半期も猛威を振るっており、20,000 以上の Web サイトを侵害しています。このサイバー攻撃グループが最近実行したキャンペーンで使用したマルウェアの亜種は、ESET のテレメトリ（監視データ）で 400,000 回を超える検出数が記録されています。

ランサムウェアの分野では、2024 年 2 月に法執行機関によって実施された世界的な解体作戦「クロノス作戦」によって、これまで君臨してきた LockBit がトップの座から叩き落とされました。ESET のテレメトリでは、2024 年上半期に注目すべき LockBit キャンペーンが 2 件記録されていますが、これらは LockBit 以外のサイバー攻撃グループが、リークした LockBit 作成ツールを使用した攻撃であることが判明しています。

Ebury ボットネットは、ESET が 2014 年に公開したホワイトペーパー「ウィンディゴ作戦」でも検証されていますが、10 年が経過した今でも危険な存在のままです。ESET の研究者による最近の調査から、この脅威は 2009 年から約 40 万台のサーバーを侵害していることが判明しました。Ebury のツールキットは当初の調査時点ですでに高度な技術が組み込まれていましたが、今回の最新の調査結果では、ボットネットの拡張機能が明らかになり、暗号通貨やクレジットカードの窃取など収益化のための機能が主に強化されていました。

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

Android iOS 金融関連の脅威

アジアから新天地へと被害を拡大させている GoldDigger

Android および iOS の両方を攻撃できる新たなトロイの木馬が、アジア地域のユーザーから顔認識データを窃取し、金融取引の認証で使用するためのディープフェイク動画を作成しています。Android の古い亜種もラテンアメリカと南アフリカへと活動範囲を拡大しています。

2024 年上半期の ESET のテレメトリでは、ESET が追跡しているほぼすべての Android の脅威の検出が大幅に減少しました。これらの多くカテゴリは、クリスマスや祝祭日などの季節的なイベントの影響を受けて、検出数は変動しますが（詳細は、**ESET 脅威レポート 2022 年第 3 三半期**を参照）、Android の金融関連の脅威は一貫して広がり続けています。

このカテゴリは 2024 年上半期に 2023 年下半期と比べて比較的小幅に減少（3.8%）しましたが、過去 2 年間の検出率に大きな変化は見られません。ただ、このカテゴリのマルウェアの動作や標的を攻撃する手法は、継続的に変化しています。

ESET 脅威レポートでは、**Android の金融関連の脅威**に Android バンキングマルウェアとクリプトスティーラー（暗号通貨を窃取するマルウェア）の両方が含まれています。銀行を標的とする多くのトロイの木馬が、暗号通貨ウォレットの認証情報を盗み出し、これらの資金を盗み出す機能を取り入れ始めていることから、これらの脅威は 1 つのカテゴリに統合されました。

2022 年下半期～ 2024 年上半期の **Android の金融関連の脅威の検出傾向**、7 日移動平均線

この脅威の攻撃手法は大きく変化しています。例えば、セキュリティ企業の Group-IB は、顔認識データを窃取するマルウェアファミリーを発見しています。これらのデータはディープフェイク動画を作成するために使用されています。このような動画の作成では、顔入れ替えの人工知能サービスが利用されており、金融取引の認証に悪用されています。このマルウェアは GoldPickaxe と命名され、Android と iOS に対応する両方のバージョンが存在します。GoldPickaxe は、暗号通貨ウォレットの所有者や東南アジアで提供されている金融関連サービスの顧客を主に攻撃しています。ESET は、GoldDiggerPlus と呼ばれる GoldPickaxe の古い Android バージョンの亜種も、アジア地域からラテンアメリカと南アフリカへと活動範囲を広げていることを発見しました。

顔認識データはデジタル認証プロセスの重要な一部となっているため、サイバー犯罪者からも注目を集めています。特定の金融アプリまたは特定の地域で使用されているアプリでは、ユーザーはモバイルデバイスのフロントカメラを使用して、さまざまな角度から自分の顔を撮影したショート動画を録画する必要があります。この動画に加えて、本人確認書類の両面の画像をアップロードしなければなりません。このような動画は本人確認に使用されています。このようなプロセスは生体認証や顔認証とも呼ばれ、口座を作成したり取引したりする人物が、提供されている本人確認書類の人物と同一であることを確認するために金融アプリで使用されています。このような動画はアイデンティティ情報の窃取や詐欺を防ぐためのセキュリティレイヤーを追加するために使用されていることは、皮肉なことです。

Android と iOS の両方に対応する GoldPickaxe

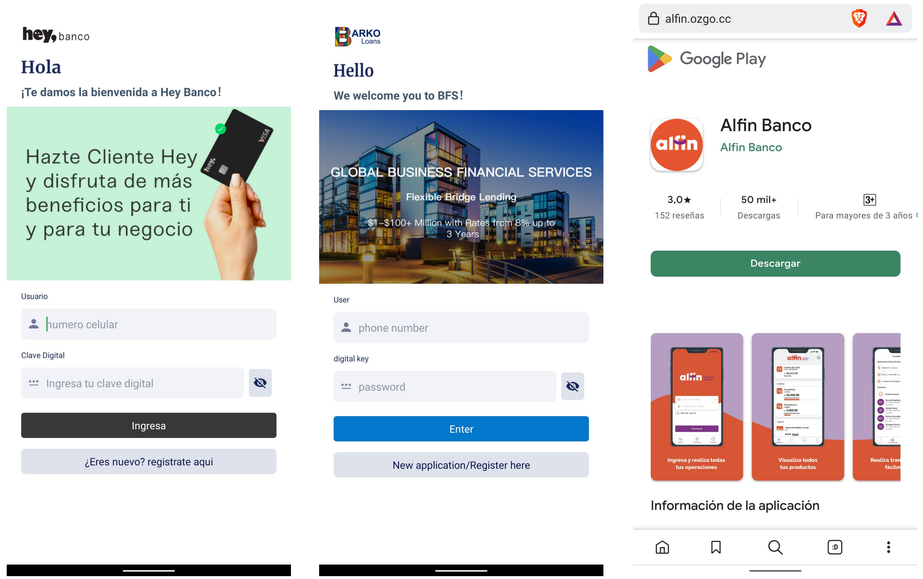
GoldPickaxe の Android バージョンは、ESET のセキュリティソリューションによって Android/Spy.Banker.CNA として検出されます。GoldPickaxe は公式の Google Play ストアを偽装した Web サイトから配信されています。ESET のセキュリティソリューションが iOS/Riskware.Frp.A として検出している iOS バージョンは、当初は、Apple のモバイルアプリケーションのテストプラットフォームである TestFlight から配信されていましたが、同プラットフォームから削除されました。その後、このサイバー攻撃者はさらに巧妙な手法を取り入れています。このサイバー攻撃者は現在、多段階型のソーシャルエンジニアリングによって被害者を騙して、モバイルデバイス管理プロファイルをインストールさせ、iOS デバイスを完全に乗っ取っています。

GoldPickaxe を操っているサイバー攻撃者は、中国語を使用し高度に組織化されているサイバー犯罪グループ「GoldFactory」であると、Group IB は考えています。このグループは、GoldPickaxe の亜種である GoldDigger と GoldDiggerPlus も攻撃に利用しています。実際、GoldPickaxe は GoldDigger をベースにして作成されています。GoldFactory については未だに不明な点もありますが、ESET はいくつかの GoldDiggerPlus の亜種の配信方法の変化を特定しており、ESET のセキュリティ製品はこれらを Android/Spy.Banker.CAY および Android/Spy.Banker.CMQ として検出しています。

GoldDigger には Android バージョンしかありませんが、Android のアクセシビリティサービスを悪用し、個人情報の窃取、バンキングアプリの認証情報の詐取、SMS メッセージの傍受、またその他のさまざまな攻撃を実行します。最新のバージョンである GoldDiggerPlus には独自の機能が追加されており、サイバー攻撃者は被害者とリアルタイムで通話できます。被害者が悪意のあるアプリでカスタマーサービスボタンをタップすると、マルウェアはこのアプリを管理しているサイバー攻撃グループのメンバーにつないで通話に対応し、正規のカスタマーサービスセンターを実際に稼働しているように錯覚させます。

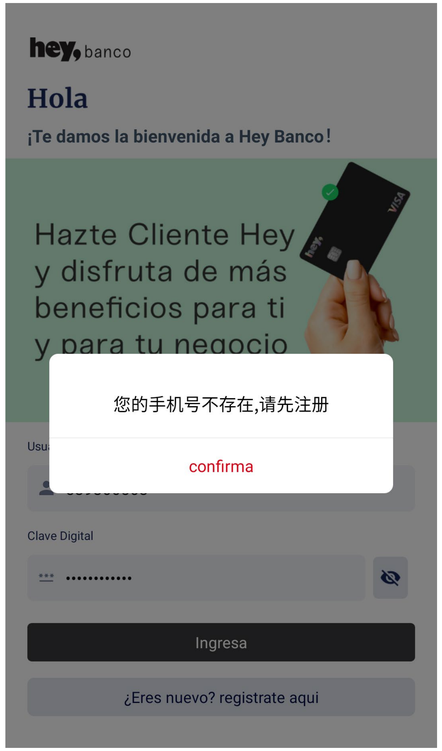
中南米と南アフリカで新たな標的を積極的に求めている

GoldDiggerPlus は主に東南アジアのユーザーを標的にしていますが、ESET のテレメトリデータでは、このトロイの木馬はラテンアメリカと南アフリカでも検出されています。さらに、GoldDiggerPlus を操っているサイバー攻撃者がこれらの地域を標的として積極的に活動していること、さらに、デバイスの所有者である東南アジアのユーザーがこれらの他国に偶然いたわけではないことも確認されています。

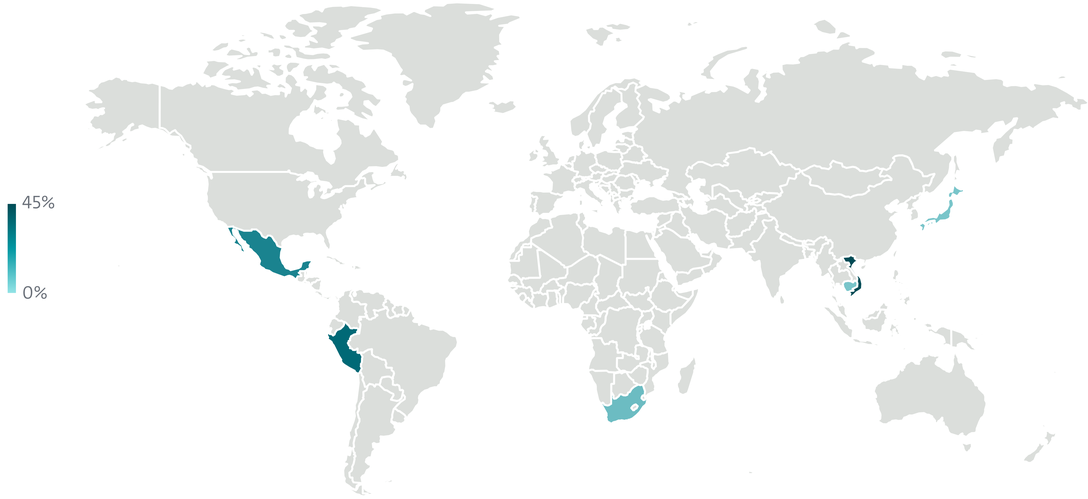


メキシコの銀行が提供している Hey Banco アプリ、南アフリカの銀行の Barko Financial Services、ペルーの銀行の Alfin Banco の悪意あるバージョンが、Google Play を偽装した Web サイトを通じて提供されている。

ESET が分析した GoldDiggerPlus マルウェアは、ペルーの銀行である Alfin Banco、メキシコの銀行の Hey Banco、南アフリカの銀行の Barko Financial Services の公式アプリを装っていました。配信方法は、東南アジアで使用されている方法と同じであり、Google Play の公式ストアを偽装した



ユーザーに登録を求めるメキシコの銀行「Hey Banco」のアプリの悪意あるバージョン。ただし、中国語でメッセージが書かれている。



2024 年上半期における **GoldDiggerPlus の検出の地理的な分布**

Web サイトから悪意のあるアプリが配信されています。これらの悪意のあるすべてのアプリは、標的としている地域の言語にローカライズして提供されています。これらのアプリでは中国語の痕跡が何度か検出されています。例えば、ユーザーが悪意のあるバージョンの「Hey Banco」アプリに間違ったデータを入力すると、中国語で「あなたの携帯電話番号は存在しません、最初に登録してください」というメッセージが表示されます。ただし、このメッセージ画面の「確認」ボタンは正しくローカライズされています。

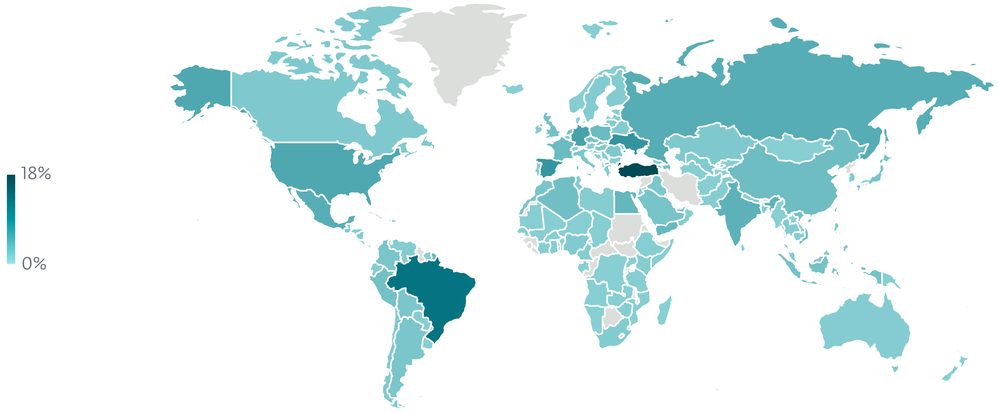
金融関連の脅威の攻撃手法の変化

近年、セキュリティ対策の強化やデジタル環境の変化に対応して、Android の金融関連の脅威も大きく進化しています。前に説明した GoldDigger マルウェアの手法は、サイバー攻撃者が新しく取り入れている手法の一部に過ぎません。このような変化が生じているのは、攻撃者がより巧妙で検出されにくい侵入方法を追求しているためです。

例えば、攻撃者は、Android のアクセシビリティサービスを悪用して、デバイスでイベントをトリガーおよび記録して、完全に乗っ取っています。また、仮想ネットワークコンピューティングのテクノロジーを使用して、被害者の画面をリアルタイムでストリーミングすることも可能になっています。攻撃者はまた、被害者の口座から不正に送金および預託できる自動送金システムを開発しており、取引をできる限り不審に見せないようにし、Google Authenticator のようなソフトウェアベースの二要素認証システムを回避する方法を見つけています。また、Android 13 で導入されたセキュリティ対策である**制限付き設定**も回避しています。

モバイルデバイスを標的とする金融関連の新たな脅威は、ラテンアメリカや東南アジアで見つかることが多くあります。これらの地域は、特にこれらのモバイルの金融関連の脅威に関するサイバー犯罪の震源地となりつつあります。しかし、ESET のテレメトリによると、過去 2 年間で Android に対する金融関連の脅威の影響を最も受けた国はトルコでした。

トルコが最も大きな影響を受けている理由、そしてラテンアメリカ、東南アジア、一部のアフリカ諸国でこれらの脅威が蔓延している理由は、デジタルトランスフォーメーションが急速に進んでいることです。これらの地域の人口の大部分が、デスクトップ PC やノートパソコンを所有する段階から、スマートフォンで直接オンラインサービスを使用する段階へと移行しています。これまでオンラインバンキングサービスを利用できなかった多くのユーザーが、現在ではスマートフォンで取引しています。デジタルバンキングへの急速な移行は、



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

残念ながらサイバー犯罪の呼び水にもなっています。サイバー犯罪者は、このような地域を標的にし、これらの脆弱な環境に付け込んで詐欺を働くことが多くあります。

Android の金融関連の脅威の検出数は横ばい傾向にありますが、隠しアプリ（-67%）、スパイウェア（-43%）、SMS トロイの木馬（-25%）、アドウェア（-23%）、ストーカーウェア（-22%）、ランサムウェア（18%）、クリッカー（-15%）など ESET が監視しているほぼすてのカテゴリで Android の脅威の検出数は減少しています。このため、Android の脅威全体の検出数は 41% 減少しています。減少していないカテゴリは詐欺アプリであり、このカテゴリの検出数は 18% 増加しています。

しかし、ドロッパーを経由してデバイスに侵入している脅威もあります。検出数が減少している Android の脅威の中には追跡が困難になっているものもあります。これらのプログラムは、正規のアプリを偽装していることも多く、デバイスに一度インストールされると、通常、ユーザーが気づかないうちに、さまざまな悪意のあるソフトウェアを展開します。ドロッパーの主な目的は、最初にインストールした悪意のあるアプリが検出され削除された場合でも、デバイスに別のマルウェアをインストールして確実に常駐させることです。ESET は 2024 年上半期に、隠しアプリをインストールする汎用的ないくつかのドロッパーを確認しています。これらのドロッパーは異なるタイプの脅威をインストールしたり、将来的にはインストールするマルウェアを変えたりすることもあるため、ESET のテレメトリでは隠しアプリとして追跡することはできません。しかし、今年の前半はドロッパー自体も減少しています。

iOS デバイスを侵害する新たな手法

iOS に対する脅威は、他のオペレーティングシステムに比べて非常に少ないものの、iOS を攻撃する GoldPickaxe のバージョンがあるように、これらの脅威は存在しています。iOS のリスクが低くなっている理由は、主に Apple が厳格なアプリの承認プロセスを採用していること、そして iOS が閉鎖的なエコシステムであることです。iOS は、**サンドボックスの原理**を取り入れており、各アプリが隔離され、相互に干渉することや互いのデータに簡単にアクセスすることを防止しているため、潜在的に悪意のある活動が軽減されています。一方、この原則によって、iOS デバイスのセキュリティアプリは、デバイス全体や他のアプリをスキャンすることができず、スキャンできる対象が限られているため、脅威を検出することが困難になっています。通常、潜在的な iOS の脅威は、Apple に組み込まれているセキュリティプロトコルによって特定され軽減されます。

iOS は Android と異なり、これまではサードパーティからのアプリのダウンロードを許可していなかったため、脅威が発生する可能性がさらに低くなっていました。しかし、このポリシーが変更されることになり、少なくとも欧州連合（EU）域内の iOS デバイスユーザーに大きな転換期が訪れるようとしています。

欧州委員会の**デジタル市場法**によって、EU 域内の iOS ユーザーは、従来のアプリマーケットプレイスに加え、Web サイトや App Store とは別のアプリマーケットプレイスからもアプリをダウンロードできるようになります。この変更は、**いくつかの訴訟や規制当局の監視**の影響を受けたものであり、Apple がこれまで守ってきた閉鎖的なエコシステムを、規模の小さな競合他社に開放し、消費者に幅広い選択肢を提供することを目的としていています。

しかし、この変化にもいくつかの課題が伴います。ユーザーを保護するために、Apple は配信チャネルに関係なく、すべてのアプリがプラットフォームの整合性に関する基準を満たすことができるように、**公証プロセス**を導入しました。新しい Web ダウンロードプログラムでは、EU でアプリが 100 万回以上ダウンロードしているなどの特定の基準を開発者に要求しています。また、1 社のアプリのみを扱っている企業は EU 域内の iPhone 向けにアプリストアを提供できます。

このような要件が課せられていますが、攻撃者は、悪意のあるソフトウェアを正規のアプリケーションのように偽装したり、セキュリティ対策が脆弱なマーケットプレイスを侵害したりすることで、この新しい仕組みを攻撃する方法を今後見つけることになるでしょう。

ESET は、EU 域内のユーザーに対し、不明なソースから iOS アプリをダウンロードする場合には慎重に行動し、App Store 以外からダウンロードされるアプリに関する問題への Apple の対応には限界があることを理解するように助言しています。

Linux ボットネット 情報窃取型マルウェア

Linux サーバーを侵害しながら生き続ける Ebury

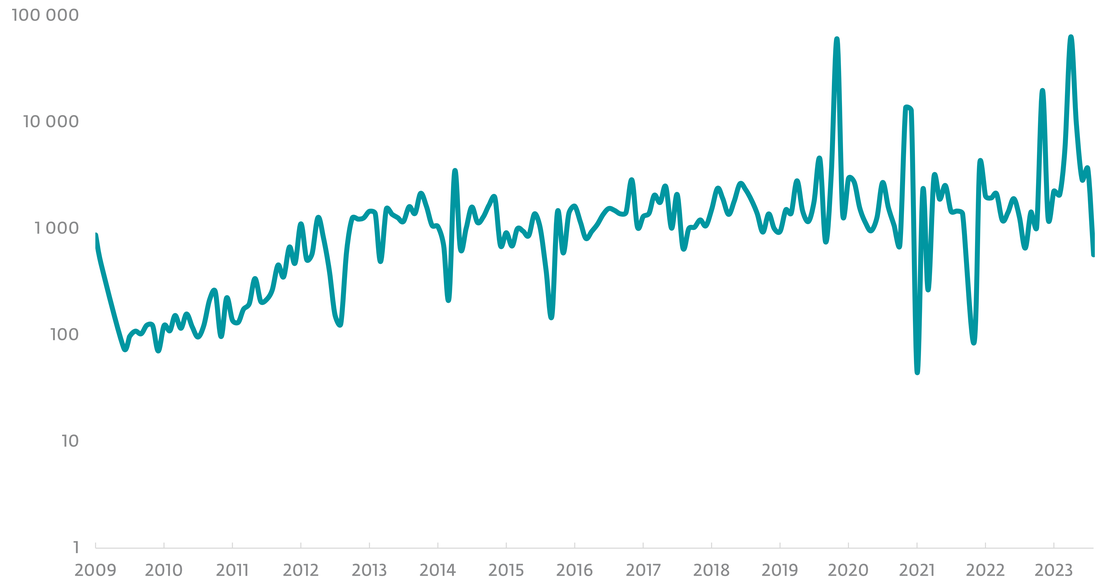
Ebury のオペレータは、金銭的な利益を最大化するためのツールを導入し、何十万台ものサーバーを侵害しています。

ESET は、10 年前に「ウィンディゴ作戦」と命名された大規模なキャンペーンについて**ホワイトペーパー** を公開し、詳細を解説しました。ウィンディゴ作戦では、サイバー攻撃者がボットネットを使用し、Ebury マルウェアによって数千台の Linux および Unix サーバーを侵害しました。2015 年に犯人の一人が逮捕され、身柄を引き渡されているにもかかわらず、このボットネットの活動は今日まで続いています。Ebury の検出数は 2009 年から、ほぼ継続して増加しています。Ebury は定期的に更新されており、年間数千台のサーバーが影響を受け、これまで全体で約 40 万台のサーバーが影響を受けています。

ESET は法執行機関と協力してこのボットネットを長期にわかって広範に調査し、新しく判明したこのボットネットの詳細を**新しいホワイトペーパー**にまとめて 2024 年 5 月に公開しました。

当初の調査時点で Ebury のツールキットはすでに高度で充実していましたが、法執行機関からの協力と、ESET がカスタマイズしたハニーポットによって、このボットネットの拡張機能が明らかになりました。これらのボットネットは、暗号通貨やクレジットカードの窃取などの手段でサーバーを侵害して金銭的な利益を得ることを主な目的としています。

Ebury は、OpenSSH を使用するバックドアであり認証情報を盗むマルウェアでもあります。Ebury は、サーバーサイドの脅威のクラスタの中核を形成しています。当初の Ebury ボットネットは、Web のリダイレクト、Windows マルウェアの配信、スパムの送信に使用されていました。最近の Ebury ボットネットは、サーバーへの HTTP POST リクエストを傍受し、金融取引の Web サイトから金融情報を窃取しています。



2009 年以降の 1 か月あたりの **Ebury の展開数**（対数 Y 軸）

Ebury は暗号通貨資金を標的として、世界各国のデータセンターで **AiTM 攻撃**（中間者攻撃）を行っています。Ebury のオペレータは価値の高いサーバーを特定すると、ネットワークトラフィックを自らが管理するシステムにリダイレクトして SSH 認証情報を取得し、スクリプトを実行してシステムから暗号通貨ウォレットのデータを流出させます。

このボットネットがクレジットカード情報を窃取するときには、ネットワークトラフィックを盗聴し、ユーザーが侵害されたオンラインストアにクレジットカード情報を送信する瞬間を待ちます。カード情報が送信されたときに傍受できるように、Ebury はさまざまなツールを展開しています。

クレジットカードデータと暗号通貨資金を盗むだけにとどまらず、Ebury を操っているサイバー攻撃者は、さらなる収益化を目指して他の手段も開発しています。新しく開発された機能には、HTTP リクエストを取得したりトラフィックをプロキシしたりする Apache モジュール、リダイレクトを実行する Linux カーネルモジュール、ファイアウォールルールを注入する Netfilter ツールの修正版などがあります。

また、攻撃者の活動が可視性され、Ebury がどのようにして認証情報を盗み、ホスティングプロバイダーのインフラを侵害し、顧客がレンタルしているすべてのサーバーにマルウェアを配信し、時には何千台ものサーバーを侵害し、何百万ものドメインをホスティングして拡散している方法が明らかになりました。

Ebury が数十年にわたって大規模な活動を展開しつづけていること、そして、`linux.org` を運用しているような豊富な知識がある Linux ユーザーも侵害しているその能力の高さは、現在の Linux セキュリティが抱えているいくつもの課題を浮き彫りにしています。

技術的な詳細については、ホワイトペーパーを参照してください。このホワイトペーパーには、利用しているシステムを確実に保護しなければならない方向けのアドバイスについても記載されています。Ebury マルウェアはルートキットの手法を取り入れているためこの攻撃を回避することは容易ではありませんが、さまざまな手法を用いてユーザーランドのルートキットの存在を検出する方法も説明しています。Ebury によって侵害されたシステムを、進行中の侵害から完全に保護するためには、影響を受けたサーバーの鍵や認証情報を再利用せず、完全に再インストールする必要があることに注意してください。

AI Web に関する脅威 情報窃取型マルウェア

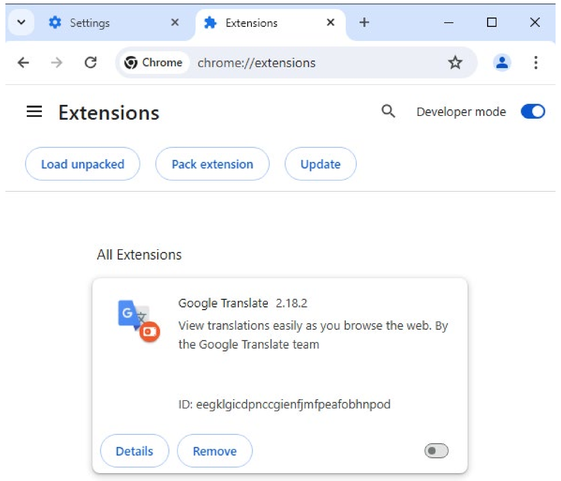
生成 AI アシスタントを装うマルウェア

情報窃取型マルウェアをインストールするために、偽の生成 AI アシスタントが利用されています。その背景には何があるのでしょうか？

ESET のテレメトリには、生成 AI アシスタントの名前を利用してマルウェアを拡散させようとするいくつもの試みが記録されています。2024 年上半期に確認され、最も注意が必要なケースは、「Rilide Stealer」として知られる悪意のある Chrome ブラウザ拡張機能と、AI ソフトウェアのデスクトップアプリを提供すると謳って、実際には情報窃取型マルウェア「Vidar」を配信する悪意のあるインストーラです。

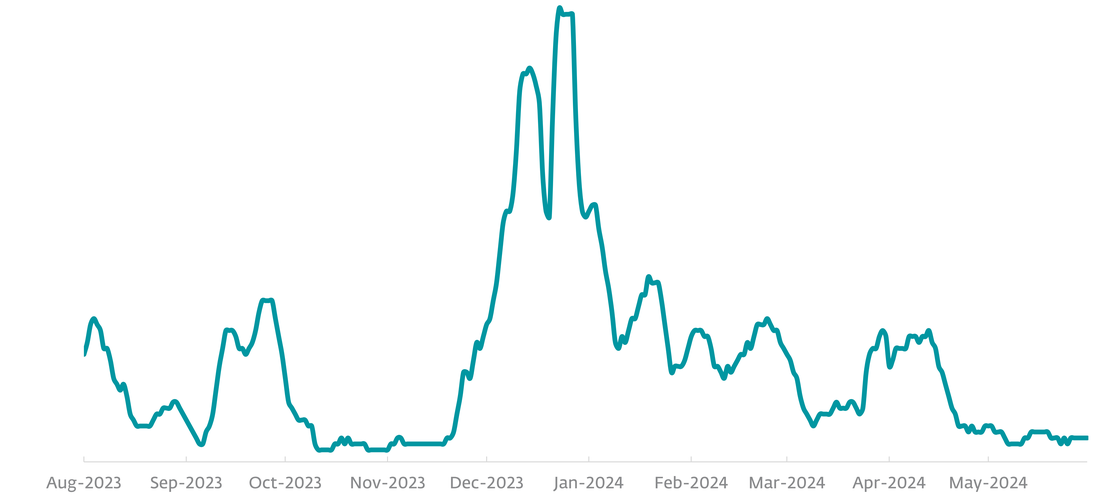
Rilide Stealer

生成 AI サービスを提供するという悪意のある広告（通常は Facebook に掲載）にユーザーが騙されてクリックした場合に、悪意のあるブラウザ拡張機能が配信されます。この拡張機能は Google 翻訳を装っていますが、ルアーとして使用している AI サービスの公式ウェブページを提供しています。これらのルアーには、OpenAI の Sora や Google の Gemini が含まれます。この拡張機能は、ESET セキュリティ製品によって JS/Extenbro.Agent.EK および JS/Extenbro.Agent.EP として検出されますが、実際には、Rilide Stealer V4 として知られる情報窃取型マルウェアであり、Facebook の認証情報を狙っています。



Google 翻訳を装った **Chrome ブラウザの拡張機能「Rilide Stealer V4」**

2023 年 8 月以降、ESET のテレメトリには、4,000 回以上の悪意のある拡張機能のインストール試行が記録されています。



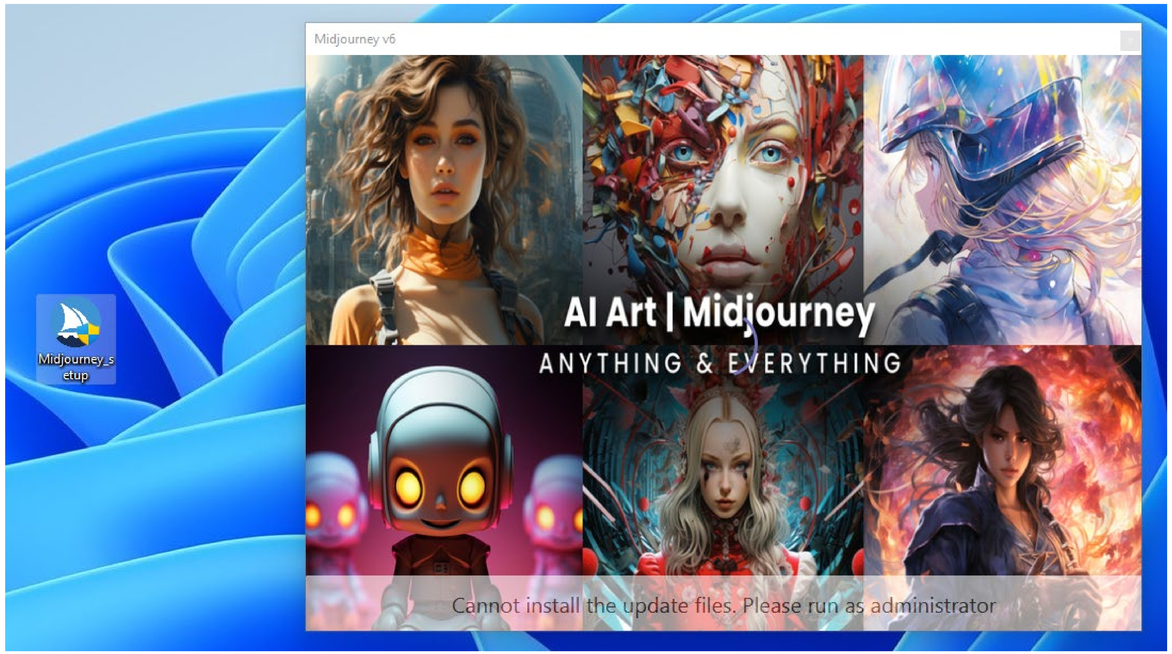
ブラウザ拡張機能の **Rilide Stealer V4 の検出傾向**、7 日移動平均線

情報窃取型マルウェア Vidar

この悪意のあるインストーラは、Facebook の広告、Telegram のグループ、ダークウェブフォーラムを通じて拡散しており、画像生成 AI である「Midjourney」を提供すると謳いながら実際には情報窃取型マルウェアである Vidar を配信しています。このインストーラは、実行時に Java 実行環境（JRE）がシステムにインストールされていないことを検出すると、不足しているランタイムに関するエラーメッセージを表示し、公式の Java ダウンロードページを開き、インストーラを実行するには Java が必要であると伝えてきます。JRE がインストールされている場合は、Midjourney を宣伝するスプラッシュ画面が表示されます。

このインストーラは、Java/TrojanDownloader.Agent.NWR として検出されます。このインストーラは、いくつかのマルウェアと AutoIt のバージョン 3 を配信し、この AutoIt が次に Vidar を配信します。この情報窃取型マルウェアは、キー入力を記録し、ブラウザに保存された認証情報や暗号通貨ウォレットのデータを盗み出すことができます。

Midjourney はデスクトップアプリを提供していません。Midjourney の AI モデルは、Midjourney の公式 Discord サーバーの Discord ボットとして利用できます。また、Discord でボットに直接メッセージを送るか、サードパーティの Discord サーバーに追加することで利用できます。このマルウェアが `Midjourney v6` という名前を使っていることから、現在利用可能な Midjourney モデルの最新バージョンを偽装しようとしていると考えられます。



Midjourney になりすました**情報窃取型マルウェア Vidar のインストーラが表示するスプラッシュ画面**

ESET のエキスパートの解説

生成 AI モデルの開発には、悪用を防止するための安全対策が講じられてきましたが、それでもサイバー犯罪者による生成 AI の悪用を防ぐことはできませんでした。2023 年以降、生成 AI に便乗した情報窃取型マルウェアが多数を占めるようになりましたが、この傾向は今後も続くはずです。生成 AI モデルを利用できると約束する不審なリンクをクリックするのではなく、必ずプロバイダーの公式 Web サイトに移動して生成 AI を利用してください。そして、情報窃取型マルウェアから身を守るために、デバイスに信頼できるセキュリティソリューションを導入してください。

ESET 脅威検出部門ディレクター
Jiří Kropáč

Web に関する脅威

WordPress プラグインの脆弱性が増加し、悪意のあるスクリプトも増加

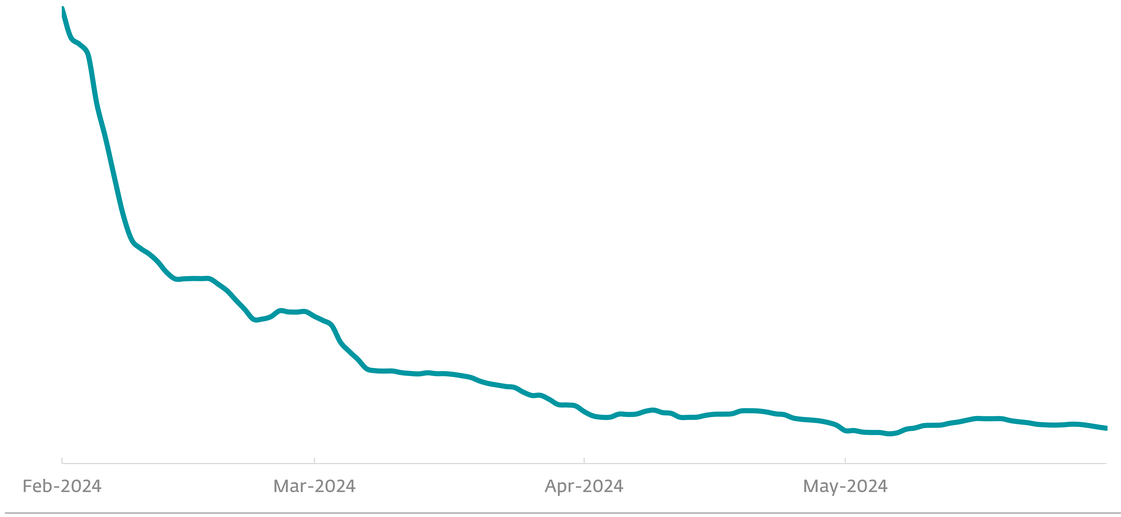
2024 年上半期には 2 万以上の Web サイトに悪意のある JavaScript コードが挿入され侵害されました。

2023 年下半期の ESET 脅威レポートでも説明しましたが、WordPress プラグインの脆弱性の悪用は、Balada Injector と呼ばれるサイバー攻撃グループが頻繁に使用している初期アクセスの手法です。2024 年 1 月に、このグループが攻撃を再開し、JS/Agent マルウェアの悪意のある多くの JavaScript が ESET のテレメトリに記録されるようになりました。

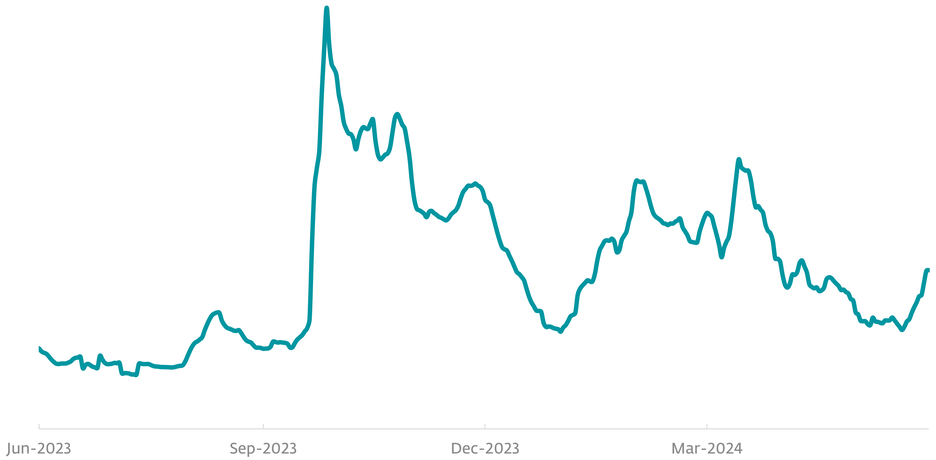
検出された亜種は、同月に公開された Sucuri のブログで説明されているマルウェアと同じか類似しています。WordPress プラグイン Popup Builder の脆弱なバージョンを実行している Web サイトに対して攻撃が現在も進行していることが懸念されます。悪意のあるスクリプトのすべての JavaScript は難読化されており、悪意のあるサーバーにリダイレクトし、さらにマルウェアを配信しようとします。このマルウェアの最終的な目的は、Web 管理者のアカウントや Web サーバーを侵害し、バックドアを配信し、侵害された Web サイトにアクセスしたユーザーを攻撃することです。

このマルウェアの検出の多くを占めているのは、2024 年に初めて確認された新しい亜種である JS/Agent.RJR です。ポーランド（9%）、フランス（7%）、米国（6%）でこれらの亜種の検出が最も多くなっていますが、.RJR の検出は、スペイン、イタリア、ドイツで 5%、チェコで 3% を占めており、広範に拡散していることがわかります。.RKY や .RJZ などの他の亜種には、.RKA という別の亜種が埋め込まれています。

このキャンペーンで使用された Balada Injector 亜種の ESET テレメトリにおける総ヒット数は 400,000 回を超えており、影響を受けた Web サイトの数は 20,000 を超えています。2024 年上半期、.RJR は JS/Agent のすべての亜種の中で 4 位となり、2023 年 9 月以降、このマルウェアファミリーが継続的に増加した原因の一因となっています。



2024 年上半期における Balada Injector の検出傾向。7 日移動平均線



2023 年 6 月から 2024 年 5 月までの **JS/Agent の検出傾向**、7 日間移動平均

ESET のエキスパートの解説

Balada Injector スクリプトによって、Web サーバーが完全に乗っ取られる恐れがあるため、このスクリプトを Web サイトから削除し、脆弱なプラグインを更新して、今後悪用されることがないようにしてください。Balada Injector を使用しているサイバー攻撃者は、いくつもの常駐化の仕組み確立することに長けています。Web サーバー上の不正な管理者アカウントや悪意のあるファイルをチェックし、認証情報を交換することで、これらの脅威を除去することを忘れないでください。

ESET シニア検出エンジニア
Ján Adámek

情報窃取型マルウェア Web の脅威 ゲーム

攻撃者の台本に沿って進むストーリー：ゲーマーを捕食するサイバー犯罪者

ゲームファンの個人情報を狙う情報窃取型マルウェア。

ビデオゲームは数十億ドル規模の産業に成長しており、この業界の成功は当然のことながらサイバー犯罪者も引き寄せています。すでに数社のゲーム会社がランサムウェアの標的になっていますが、最も話題になった最近の**ランサムウェア攻撃**は、2024 年上半期初めに発生しています。この攻撃では、大作ゲーム「スパイダーマン」の開発元として知られるインソムニアックゲームズが、悪名高いランサムウェアグループ「Rhysida」への身代金の支払いを拒否したために、膨大なデータがリークされる被害に遭いました。これにより、開発者の個人情報からインソムニアックゲームズの今後のゲームリリースのロードマップ情報などの機密**データ**がインターネットにアップロードされました。

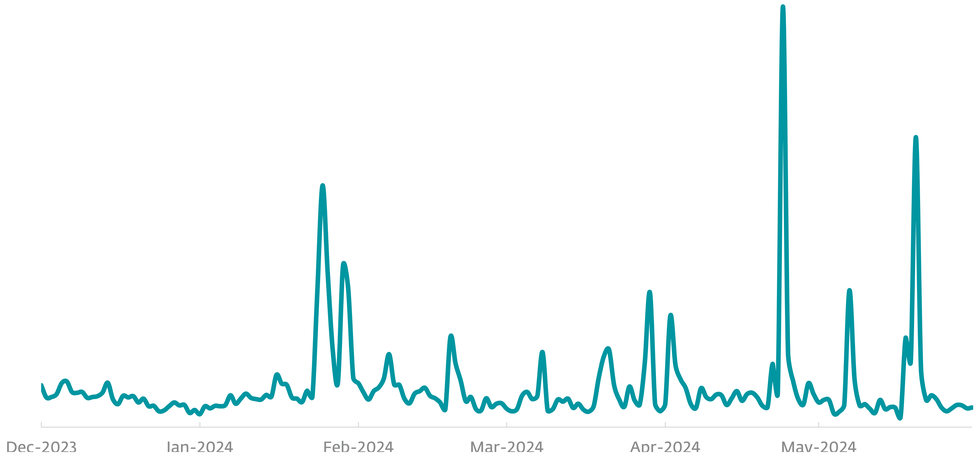
攻撃を受けるリスクがあるのは大企業だけではありません。ビデオゲームをプレイするユーザーの個人情報もまた、サイバー犯罪者にとって魅力的な標的であり、実際にサイバー攻撃者はゲーム関連のあらゆるタイプのファイルにマルウェアペイロードを隠蔽しています。

ビデオゲームの熱心なファンは、ストアフロントや公式ビデオゲームのコンテンツリポジトリなどの公式のサイトだけではなく、クラックされたゲームやチートツールを提供するトレントサイトや怪しげな Discord サーバーまで情報を求めてアクセスし、マルウェアに感染しています。このようなグレーゾーンは、犯罪者の巣窟でもあります。サイバー攻撃者は、無料でゲームを手に入れる方法や、多人数参加型のシューティングゲームで壁越しにヘッドショット（致命的な一撃）を完璧に決めるための情報などをちらつかせ、無防備なゲーマーをおびき寄せています。このような情報に引き寄せられたゲーマーを待ち受けているのは、パスワード、クレジットカードデータ、暗号通貨ウォレットを狙う情報窃盗型マルウェアです。

サービスとして提供される情報窃取型マルウェア

これらの多くの攻撃では、サービスとして配信されている情報窃取型マルウェアが使用されています。前回の ESET の脅威レポートで説明したように、**RedLine Stealer** と **Lumma Stealer** は、**ソフトウェアチート**や**クラックされたビデオゲーム**のいずれかを装ったファイルのペイロードとして見つかっています。ESET のテレメトリデータから、この 2 つの脅威は 2024 年上半期も活発であったことがわかります。

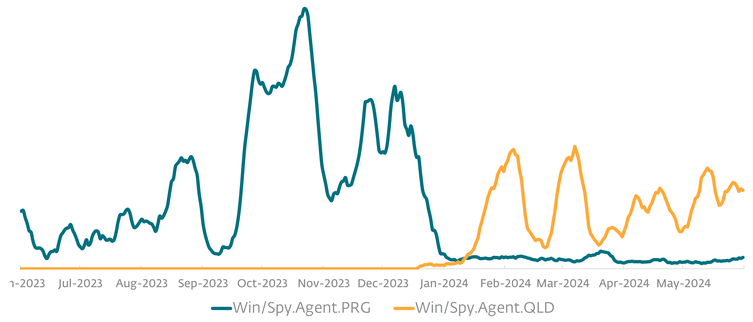
RedLine Stealer に関しては、2023 年にサービスとして展開されていたこの情報窃取型マルウェアの**解体作戦**が実施されましたが、依然として活動が続いています。ESET が収集したデータでは、RedLine Stealer はすでに更新されていませんが、未だに使用されています。2024 年には、これらの攻撃



RedLine Stealer の一日あたりの検出数の傾向（2024 年上半期）

のほとんどは 1 ～ 2 か国に限定された 1 回限りのキャンペーンで使用されています。2024 年には、1 月 25 日（50% の検出はドイツ）、4 月 24 日（87% の検出はスペイン）、5 月 20 日（91% の検出は日本が）の 3 回の攻撃ピークがありました。これらのピークとなった攻撃は非常に大規模であり、2024 年上半期の RedLine Stealer の検出数は 2023 年下半期を上回り、増加率は 31% に達しています。

2023 年下半期に Lumma Stealer が**急増**した後、暗号通貨ウォレットを主な標的とするこの脅威の検出数は、2024 年上半期には減少傾向にありました。しかし、このマルウェアファミリーで使用される特定の亜種に変化が起きています。2023 年下半期に ESET は Lumma Stealer を Win/Spy.Agent.PRG として検出して登録していましたが、これらの亜種は 2024 年にはほぼ完全に沈静化しています。一方で、2023 年末にこのマルウェアは、新しい亜種、特に Win/Spy.Agent.QLD に切り替えています。.PRG の亜種とは対照的に、.QLD の検出数は 2024 年上半期に増加しました。



2023 年下半期～ 2024 年上半期の **Win/Spy.Agent.PRG および Win/Spy.Agent.QLD の検出傾向**、7 日移動平均線

MOD の侵害

海賊版ゲームを使用しない、また、チートプレイをしないゲーマーでも、ビデオゲームの一般的な資産をダウンロードするときに、思いがけずに有害なファイルに出くわすことがあります。例えば、ゲームファンによって作られたビデオゲームのデータを改造したプログラムやファイル改造（MOD）も、サイバー犯罪者によって侵害されている場合があります。広く知られている MOD リポジトリのみを利用するか、Steam のような正規のプラットフォームから MOD を入手することが推奨されますが、それでも攻撃を受けるリスクはあります。

2023 年 6 月、ハッカーが Minecraft の MOD プラットフォーム上の複数のアカウントを**侵害**し、既存のプロジェクトに情報を窃取するコードを挿入しました。最近では、2023 年 12 月に、ゲーム「Slay the Spire」の人気の MOD が**侵害**され、Steam のアップデートシステムから Epsilon Stealer がプッシュされました（ESET は、Epsilon Stealer を JS/PSW.Agent トロイの木馬、それらの亜種を .CH および .CI として検出します）。このような場合、最新のセキュリティソフトウェアを使用して、悪意のある可能性があるファイルを検出することが最善の防御策となります。

ビデオゲーム MOD

既存のビデオゲームの改造版（MOD）は、通常、ゲームファンによって作成され、無料で提供されます。このような MOD は、新たな機能を追加したり、ゲーム内の登場人物のスキンを変えたり、あるいは新しいゲームプレイやストーリーコンテンツを追加したりする場合もあります。大規模な MOD が火付け役となり人気を博したビデオゲームもあります。最も有名な例の一つが、一人称視点のシューティングゲーム「カウンターストライク」です。このゲームは、「Half-Life」の MOD から始まっています。ゲーム開発元の多くの企業はユーザーコミュニティが作った MOD を認めていますが、ゲームの MOD は著作権法に抵触する恐れもあり、法的にはグレーゾーンです。

ビデオゲームのクラック版

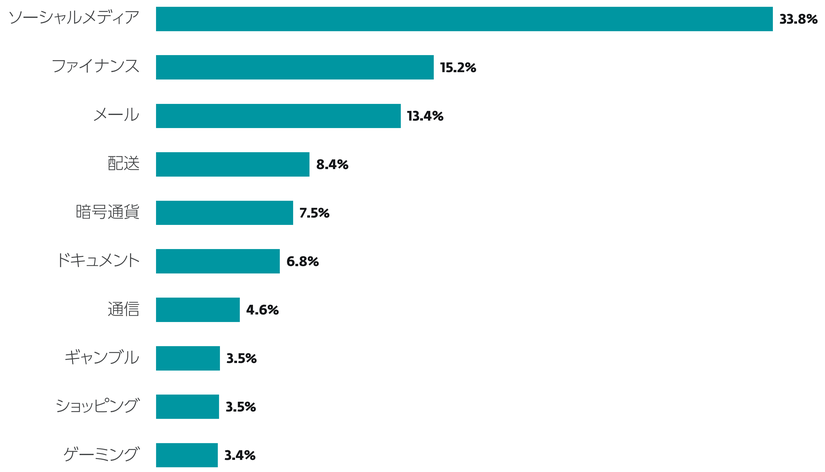
クラック版とは、コピープロテクトが解除されたゲームのバージョンです。クラックは通常、海賊版対策を回避するために行われます。

チートツール

チートツールは主にオンラインマルチプレイヤーゲームで使用され、プレイヤーが他のプレイヤーより不正な手段で有利にゲームに参加できるようにするサードパーティのソフトウェアです。例えば、FPS（一人称視点のシューティング）ゲームにおけるエイムアシスト（エイムボットとも呼ばれる）を利用すると、物体を透視できるようになります（ウォールハック）。

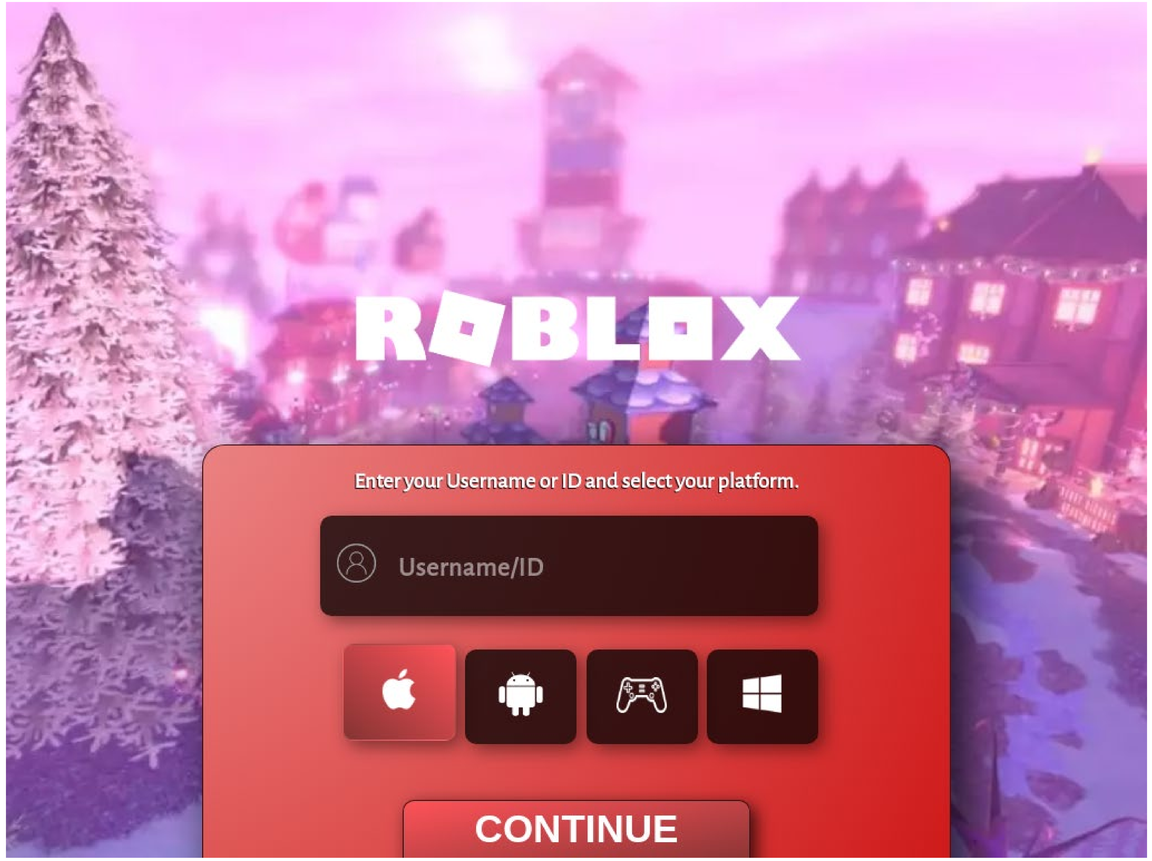
フィッシング詐欺

ゲーマーは、騙されて悪意のあるペイロードをダウンロードさせられるだけでなく、フィッシング詐欺の被害に遭う恐れもあります。ESET のフィッシングフィードによると、2024 年上半期のフィッシングサイトカテゴリのランキングで、ゲームは 10 位にランクインしました。



2024 年上半期の**上位 10 のフィッシングサイトカテゴリ**

フィッシングが特に危険になるのは、未成年者を主な対象としているゲームが標的となる場合です。昨年、脅威インテリジェンス組織の Cisco Talos は、昨年、他のユーザーが作成したさまざまなゲームをプレイしたり、ユーザー自身もゲームを作成したりできる子供に大人気のゲームプラットフォーム「Roblox」がサイバー犯罪者に悪用されている多くの方法について[レポート]を発表しました。Cisco Talos が作成した攻撃方法の一覧には、フィッシング詐欺が最初に記載されています。Roblox では Robux という仮想通貨が利用されており、実際に購入することもできるため、サイバー犯罪者にとって非常に魅力的な標的となっています。ESET のフィッシングフィードでは、Roblox の偽ログイン画面や、サインインすると Robux がもらえると謳った Web サイトがいくつも確認されています。



`robuq[.]com` で Roblox になりすましたフィッシングサイト

ダウンローダー

配信方法を変更しカムバックしたダウンローダー

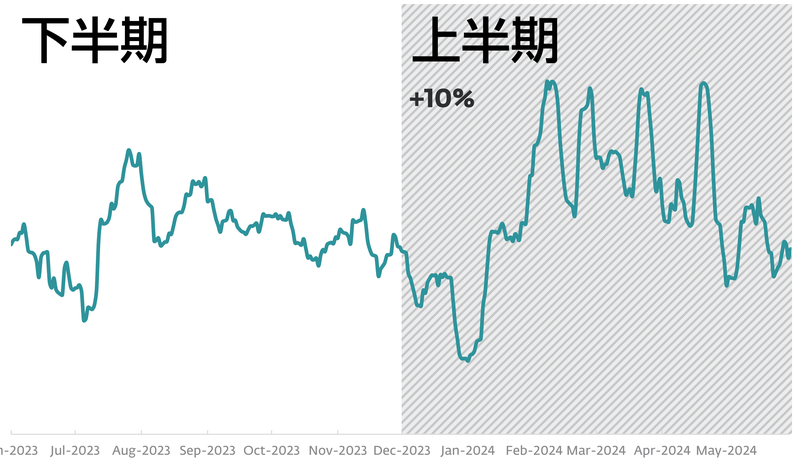
2022 年の激動期を経て、ダウンローダーの脅威が徐々に復活しつつあります。

Microsoft が、2022 年にインターネットを経由して入手したファイルのマクロを無効にしたことで、悪意のあるダウンローダーは大きな打撃を受けました。特にマクロを悪用していたダウンローダーにとってこの対策は致命的となりました。このマクロに大きく依存していた Emotet の拡散も終息し、ダウンローダーの全盛期は終焉を迎えることになりました。この現象は ESET のテレメトリでも明確に確認されており、2022 年から 2023 年にかけて、ダウンローダーの数は 65% 減少しました。しかし、2023 年の後半から、ダウンローダーの脅威は徐々に増加し始めています。2023年下半期には、同年の上半期と比較してすでに 10% 増加しており、この上昇傾向は 2024 年上半期にも継続しており、さらに 10% 増加しています。

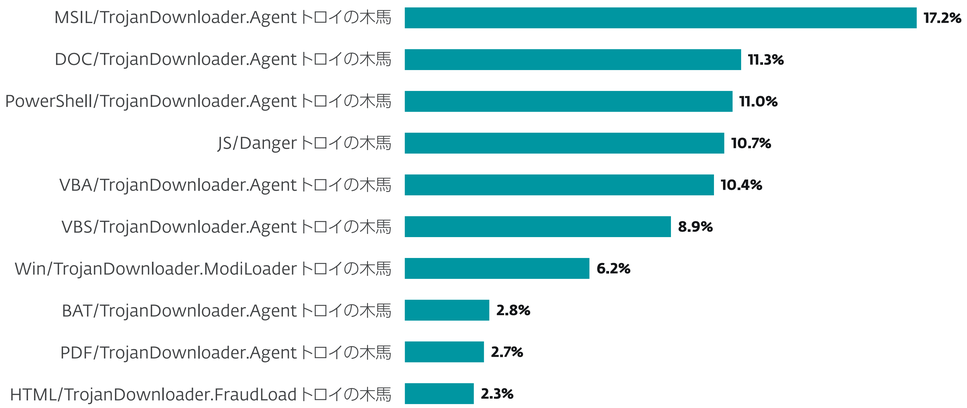
2024 年上半期の増加は、ESET が追跡している多くのダウンローダーと関係があります。この期間に検出されたダウンローダーのトップ 10 をみると、大幅に増加していないのは 2 つのダウンローダーのみでした。ESET のテレメトリデータによると、この増加傾向は 1 月末から続いており、サイバー攻撃者がダウンローダーを積極的に悪用していることがわかります。

マクロが自動的に無効に設定されるようになった後でも、攻撃を成功させるために、多くのサイバー犯罪者は配信方法を変えています。そのため、現在最も拡散しているダウンローダーは、マクロではなく悪意のあるスクリプトを仕込んだファイルを添付したスパムメールとして配信されています。ユーザーがこれらの添付ファイルをクリックすると、ダウンローダーが実行されます。

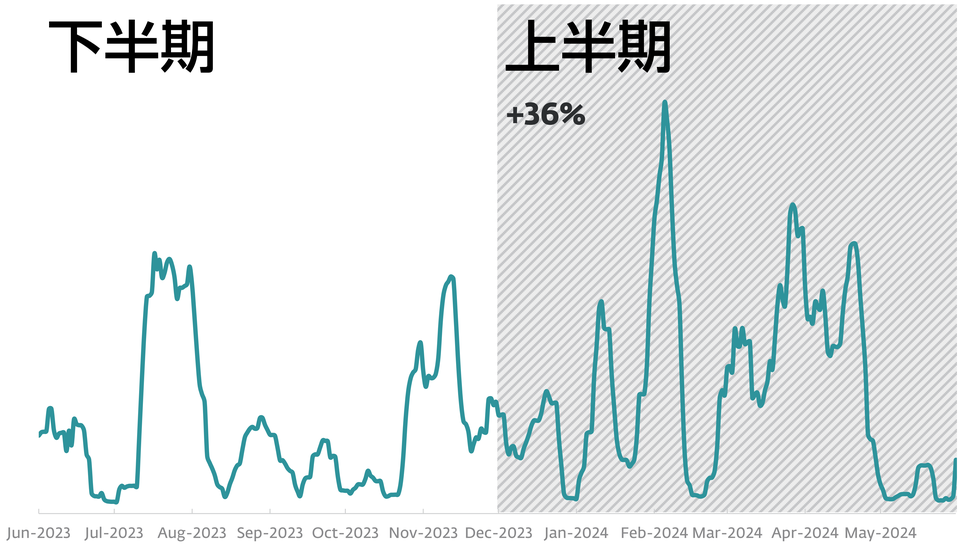
このような変化は、悪意のある JavaScript を添付したメールが増加していることでも確認されています。これらのメールは、ESET テレメトリでは、JS/Danger トロイの木馬という名前で記録されています。このマルウェアファミリーは、



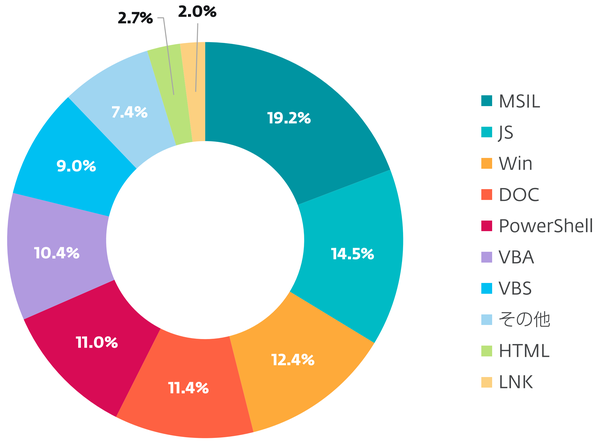
2023 年下半期～ 2024 年上半期のダウンローダーの検出傾向、7 日移動平均線



2024 年上半期のダウンローダーの検出率トップ 10（ダウンローダー検出数に占める割合）



2023 年下半期～ 2024 年上半期の**JS/Danger トロイの木馬の脅威の検出傾向**、7 日移動平均線



2024 年上半期の**ダウンローダーの検出率（検出タイプ別）**

2021年の始めに急激に減少した後に大きな変化を遂げており、直近の2024年上半期には36%増加しています。同時期に、JSダウンローダーのカテゴリも ESET のテレメトリで検出数が 2 位になっています。

ダウンローダーが全体的に増加している傾向は、ダウンローダーが送り込むマルウェアファミリーの検出数の増加と密接に関係しています。例えば、米国では 2 月 9 日と 3 月 8 日に VBS/TrojanDownloader.Agent が最も多く検出されましたが、これは Agent Tesla をダウンロードする亜種によって引き起こされています。この悪名高い情報窃取型マルウェアは、2024 年上半期に 40% 増加しています。

マクロに依存する脅威も 2024 年上半期に増加していることに注意が必要です。VBA/TrojanDownloader.Agent トロイの木馬は 24% 増加しています。2 月 22 日には、VBA/TrojanDownloader.Agent.EGF の脅威の検出が急増しました。この亜種は Word 文書のマクロとして配信されており、PowerShell の簡易なダウンローダースクリプトを実行し、別のマルウェアをダウンロードします。

ESET のエキスパートの解説

マクロに依存するダウンローダーが増加しているのは、偶然かもしれません。サイバー攻撃者は、少なくとも一部のユーザーが Microsoft 文書のマクロを手動で有効にすることを期待して、マクロベースの脅威を継続して配信しています。このような犯罪の手口は、有り得ない報酬や商品を提供すると謳って、手数料などをだまし取る前払い金詐欺に似ています。一部のユーザーを騙すことさえできれば、犯罪者にとってその手法は十分に価値があるのです。

シニア検出エンジニア
Dušan Lacika

ランサムウェア

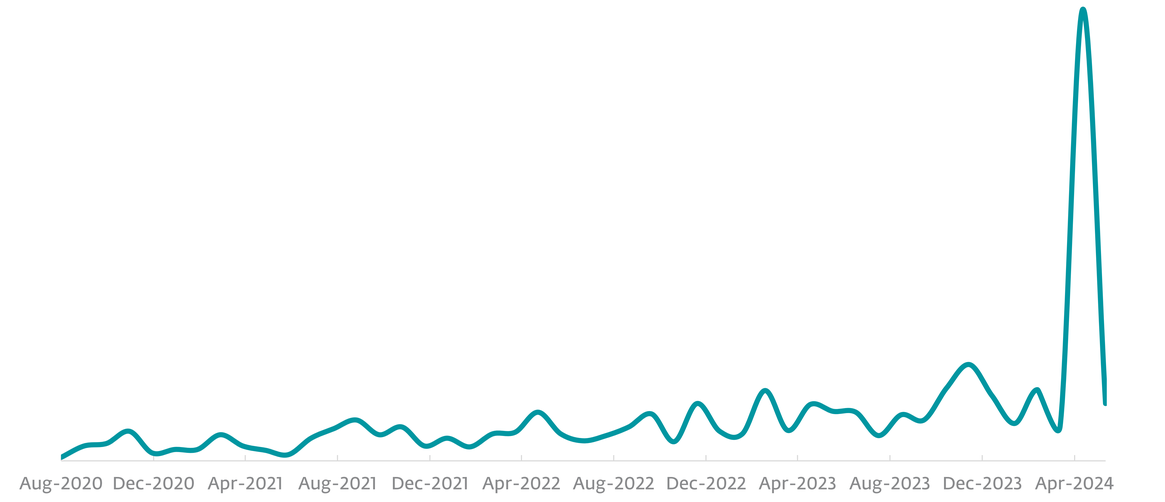
世界的な解体作戦後の LockBit にみえる状況変化

世界的な解体作戦「クロノス作戦」が実施された後、リークした LockBit の作成ツールを悪用するサイバー攻撃者が増加し、LockBit ランサムウェアグループを取り巻く状況は厳しくなっています。

LockBit が初めて確認されたのは 2019 年であり、その時には「ABCD」という名前が付けられていました。2023 年 9 月から 2024 年 4 月にかけて、世界のランサムウェア攻撃で最大のシェアを得たことが報告されるなど、ランサムウェア業界では有力な存在となりました。その後、LockBit のリーダーである LockBitSupp が XSS や Exploit などのハッキングフォーラムから追放され、さらに 2024 年 2 月に英国の国家犯罪対策庁、欧州警察機構（ユーロポール）、欧州司法当局（ユーロジャスト）が連携した世界的な解体作戦「クロノス作戦」が実施された結果、LockBit は主役の座を失いました。

この解体作戦により、ポーランドとウクライナで LockBit のアフィリエイトの 2 人が逮捕され、フランスと米国の司法当局は、複数の LockBit の共犯者に対して起訴状と国際逮捕状を発付しました。さらに、法執行機関は 200 以上の暗号通貨ウォレットを押収し、約 200 人のアフィリエイトのリストを発見し、LockBitSupp の正体を暴き、復号化ツールを開発して公開しました。

ESET のテレメトリも、解体作戦の後に、LockBit グループの活動が停滞していることを裏付けています。ESET は、解体作戦の後で実行された 2 回の LockBit キャンペーンを観測しています。これらの両方のキャンペーンでは、2022 年 9 月にリークした LockBit 作成ツールで構築されたサンプルが使用されていました。このコードを LockBit 以外のグループが使用している明確な証拠は、身代金のメモにあります。



2020 年 8 月以降の **LockBit ランサムウェアの一日あたりの検出数の傾向**

ランサムウェアは通常、フィッシング、エクスプロイト、ブルートフォース攻撃、認証情報の侵害、ダウンローダー、または独自のマルウェアなど、攻撃チェーンの最終段階で実行されるペイロードです。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るため、気付かれないケースが多くあります。攻撃者が脆弱性を攻撃したり、組織の防御策の隙間を突いたりしてランサムウェアを展開できた場合も、評判の良いセキュリティ製品を導入していれば、攻撃チェーンの最終段階で実行されるこの攻撃を検出できるはずです。

LockBit グループが使用している身代金メモでは、被害者に LockBit のリークサイトを伝えますが、これらのキャンペーンで使用された身代金には、メールアドレスまたは **Tox** の連絡先だけが提供されていました。

上記のキャンペーンの一つは、2 月の解体作戦の直後に発生しています。複数のサイバー攻撃者が、**新たに公表**された ScreenConnect の脆弱性 **CVE-2024-1708** および **CVE-2024-1709** を悪用して LockBit を配信していました。主にヨーロッパとアメリカのさまざまな業界が標的となりました。

もう一つのキャンペーンは、2024 年 4 月中旬に悪意のあるメールによって実行され、メールの添付ファイルから LockBit ランサムウェアが配信されました。添付ファイルの形式と名前、そしてメールの文面から、特定の業界を標的としておらず、広範な業界を狙っていることがうかがえます。ある**レポート**は、Phorpiex ボットネットがこれらの悪意あるメールの送信に利用されていたことを報告しています。

LockBit は通常、標的を極めて限定していますが、このキャンペーンは広範な標的に攻撃を実行していたため、ESET のテレメトリにおける LockBit の検出数に大きな影響を与えており、2024 年 4 月 17 日には急激な増加が確認されました。

ESET のエキスパートの解説

「クロノス作戦」については当初は懐疑的な見方もありましたが、LockBit がランサムウェア攻撃のシェア 1 位の座を奪われ、リークサイトに過去の被害者を掲載することで必死にそのブランドを守ろうとしていることから、この作戦が効果をあげていることは明らかです。

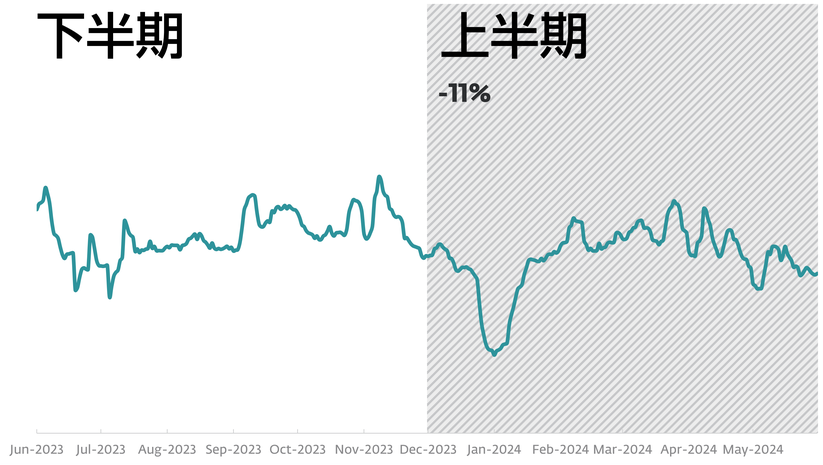
ヘルスケアテクノロジー企業の Change Healthcare でインシデントが発生した後に BlackCat が行った**出口詐欺**によって、ランサムウェアの状況はさらに大きく変化しています。2 月中旬に初めて登場した「RansomHub」グループと、2022 年半ばから活動している古いグループである「Play」の両方が、この機に乗じて新しいアフィリエイトを誘い込み、「サービスとしてのランサムウェア」のビジネスでのし上がろうとしています。

リークサイトに掲載されたデータによると、2024 年第 1 四半期のランサムウェア攻撃の件数は前四半期と比較して 20% 以上増加しましたが、主に前述のサイバー攻撃グループが弱体化し、ランサムウェアを取り巻く環境が混沌としていることから、2024 年第 2 四半期はランサムウェア攻撃の件数は減少すると予想されます。しかし、サービスとしてのランサムウェアが消滅するわけではありません。2024 年の後半には、活動を停滞させているアフィリエイトがどのグループに移るかが明らかになり、検出されるランサムウェアの順位も、このようなアフィリエイトとの協力の変化を反映した結果になると考えられます。

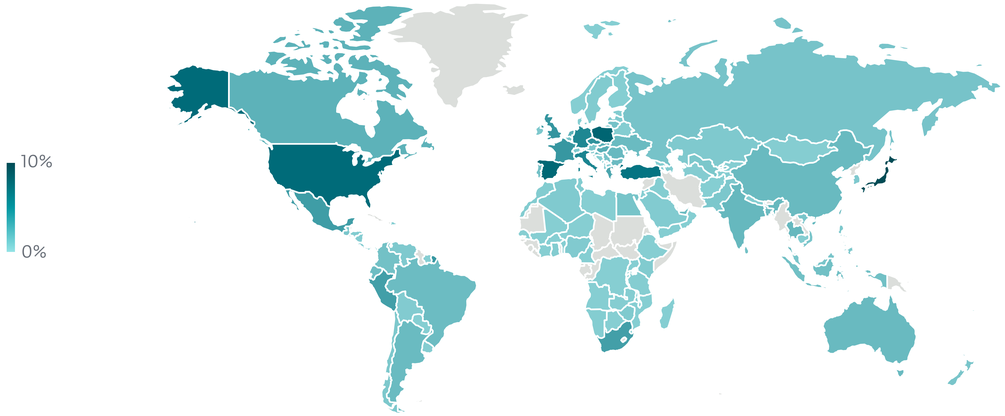
ESET シニアマルウェア研究者
Jakub Souček

脅威テレメトリ

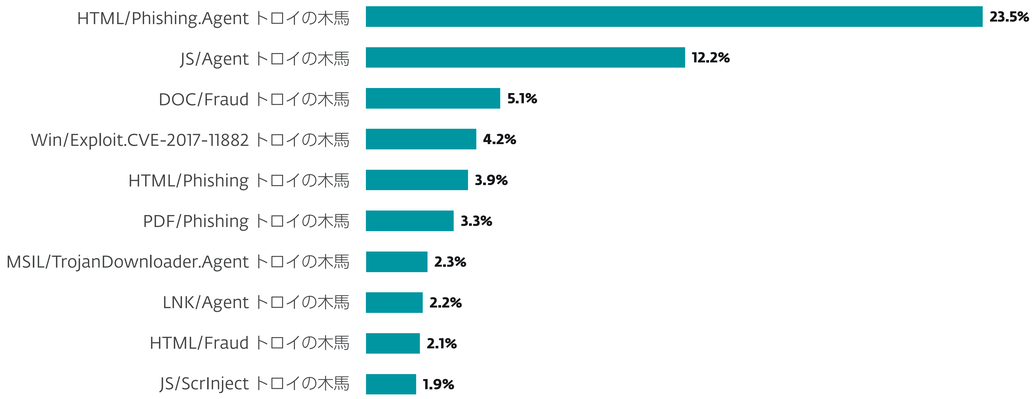
すべての脅威



2023 年下半期～ 2024 年上半期の**脅威全体の検出傾向**、7 日移動平均線

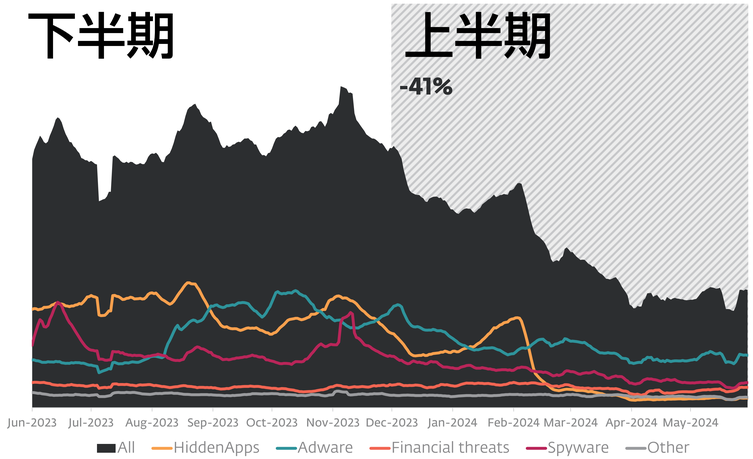


2024 年上半期における**マルウェア検出の地理的な分布**

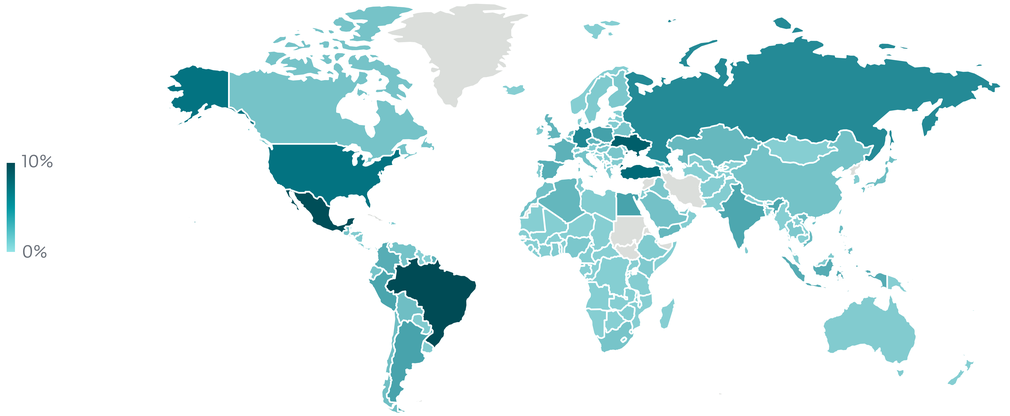


2024 年上半期ににおける**マルウェア検出数トップ 10**（マルウェア検出数に占める割合）

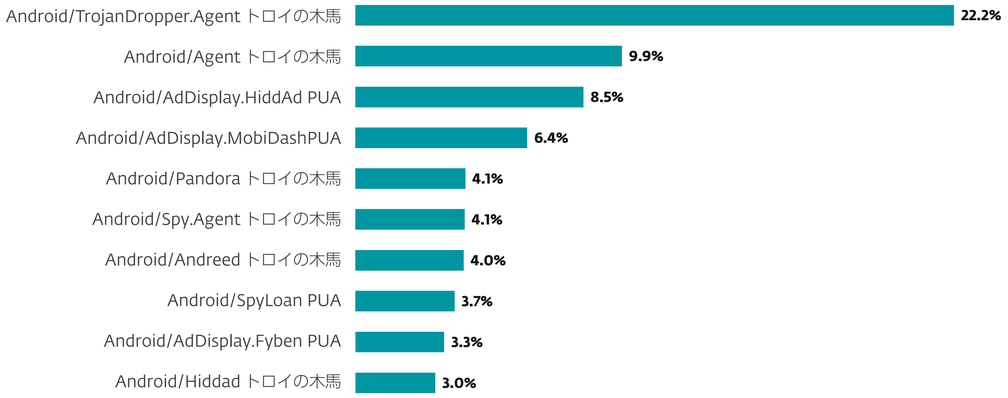
Android



2023 年下半期～ 2024 年上半期の **Android に関する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）

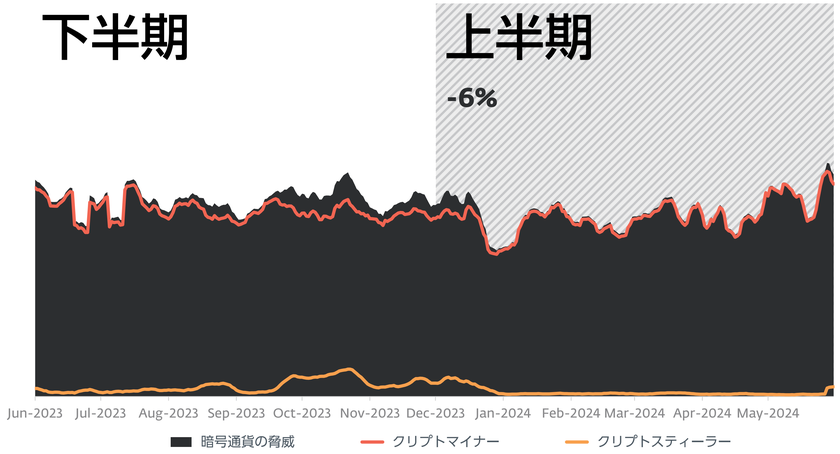


2024 年上半期における **Android に関連する脅威検出の地理的な分布**

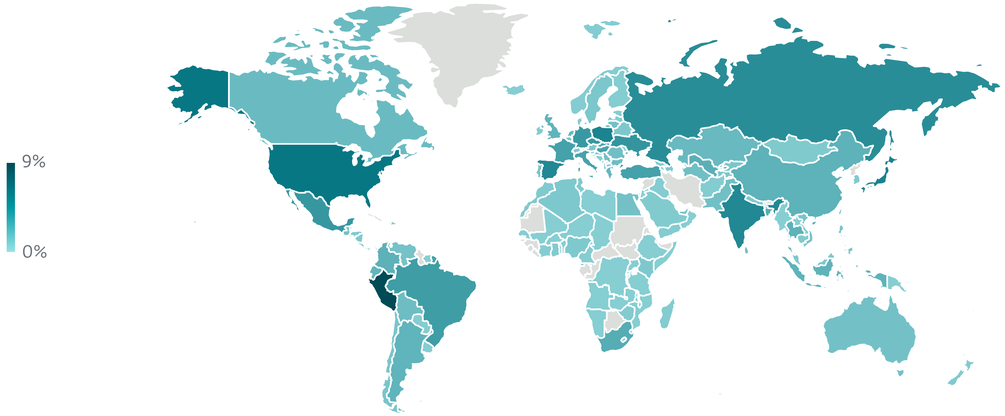


2024 年上半期に検出された Android に関する脅威**検出数トップ 10**（Android の脅威の検出数に占める割合）

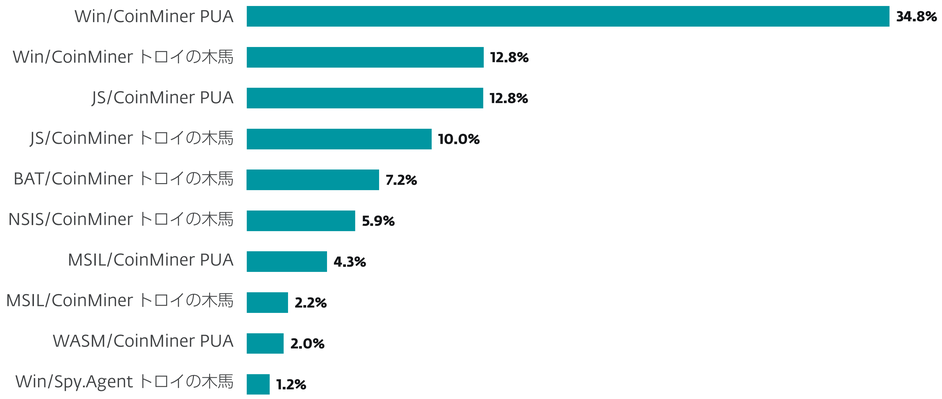
暗号通貨の脅威



2023 年下半期～ 2024 年上半期の**暗号通貨に関する脅威の検出傾向**、7 日移動平均線

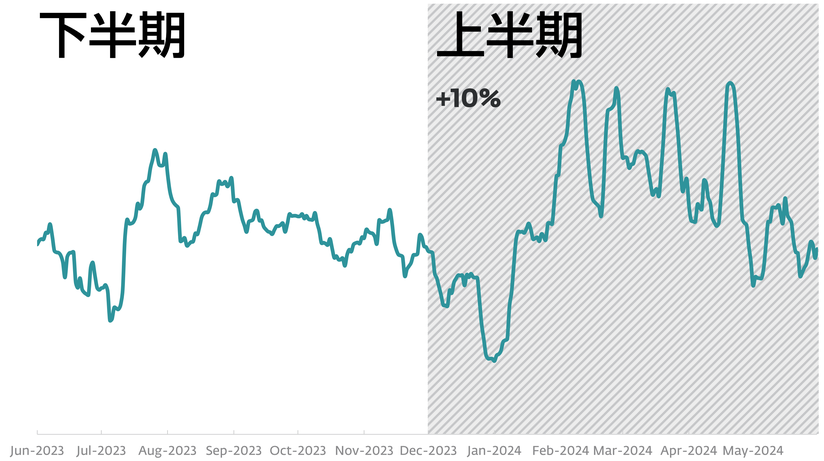


2024 年上半期における**暗号通貨の脅威の検出数の地理的な分布**

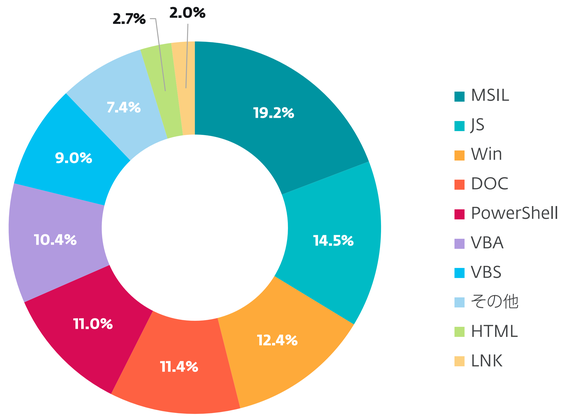


2024 年上半期における**暗号通貨の脅威検出数トップ 10**（暗号通貨の脅威の検出数に占める割合）

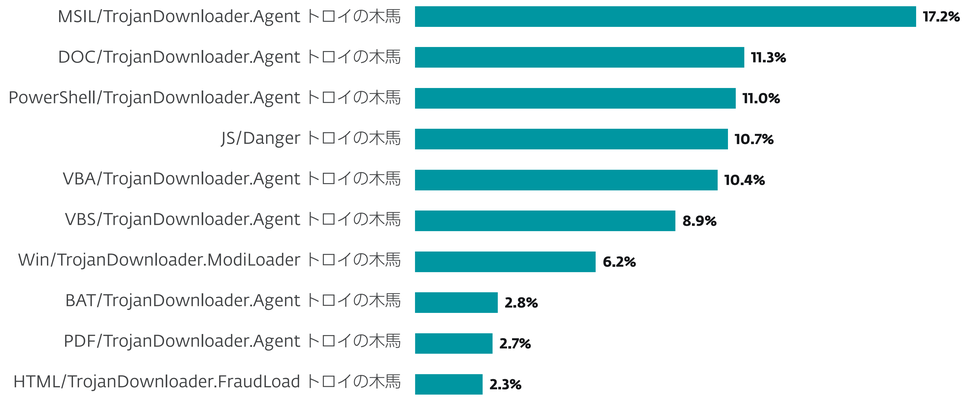
ダウンローダー



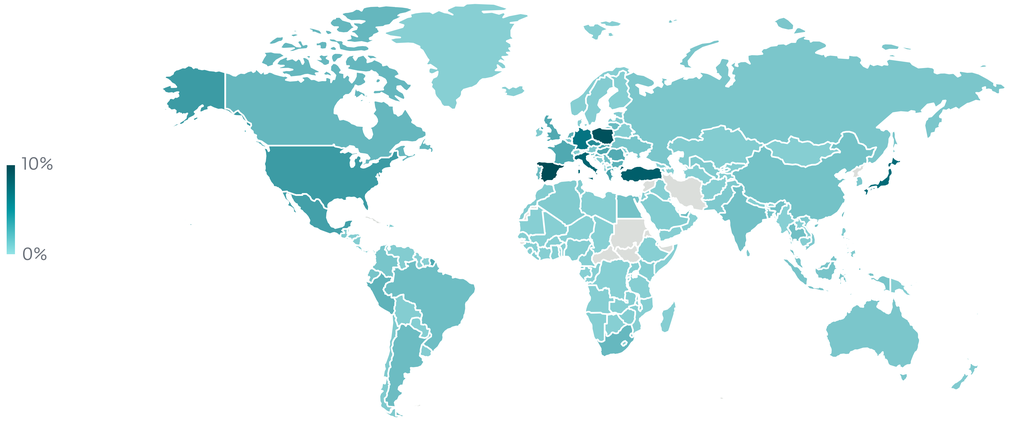
2023 年下半期～ 2024 年上半期の**ダウンローダーの検出傾向**、7 日移動平均線



2024 年上半期における**ダウンローダータイプ別の検出率**

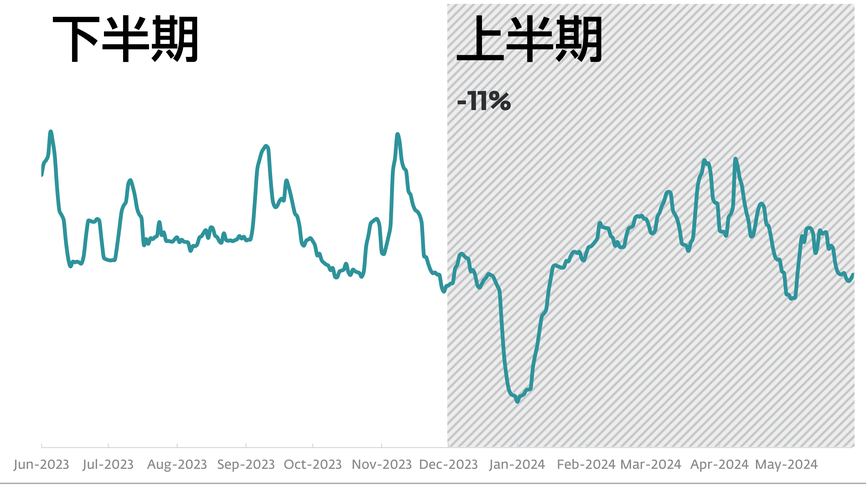


2024 年上半期における**ダウンローダーの検出数トップ 10**（ダウンローダーの検出数に対する割合）

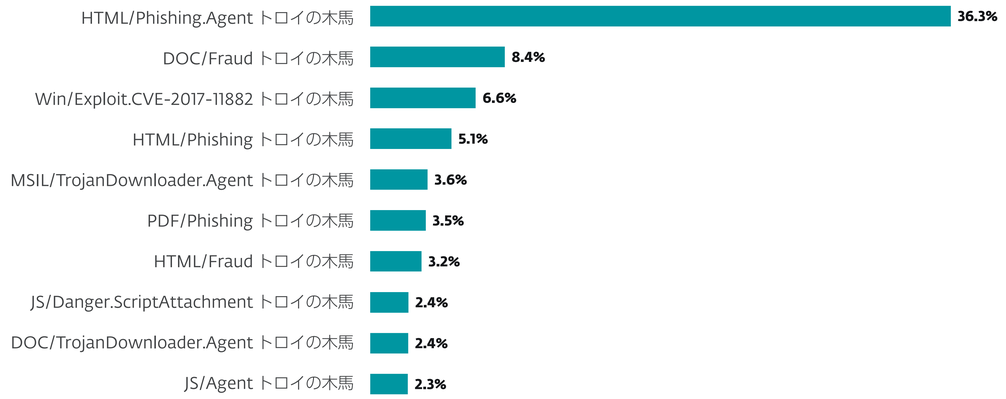


2024 年上半期における**ダウンローダー検出数の地理的な分布**

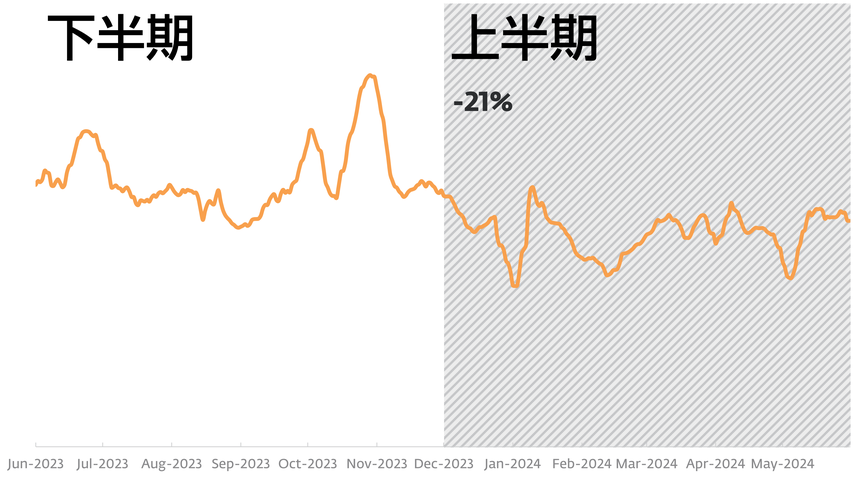
電子メールに関する脅威



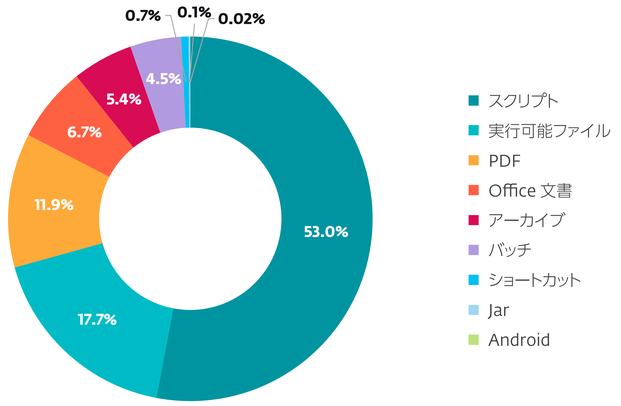
2023 年下半期～ 2024 年上半期の**悪意のあるメールの検出傾向**、7 日移動平均線



2024 年上半期に検出された**メールの脅威トップ 10**

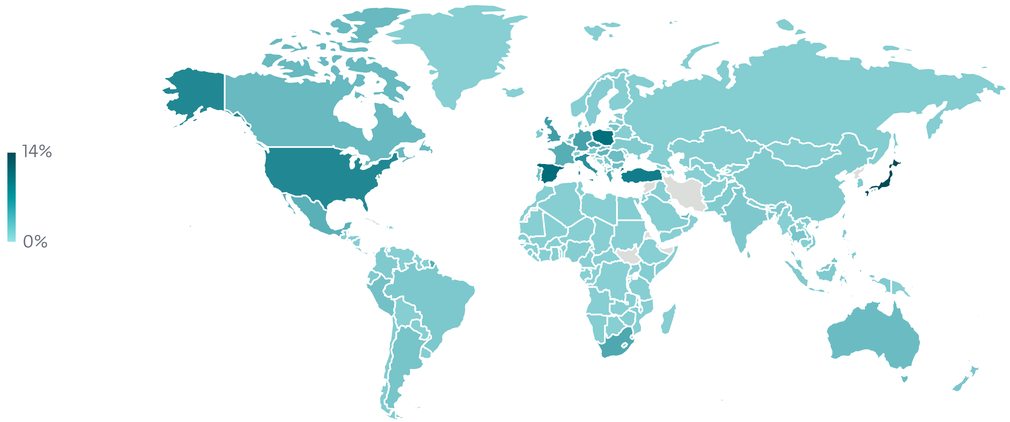


2023 年下半期～ 2024 年上半期の**スパムの検出傾向**、7 日移動平均線



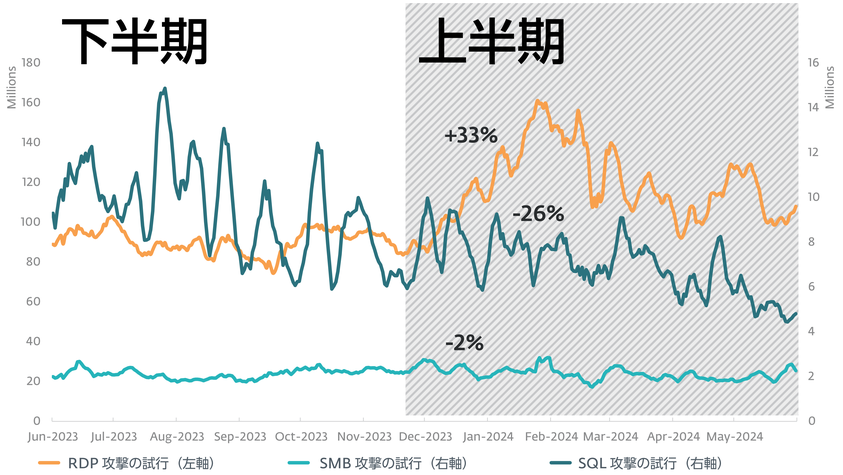
2024 年上半期に検出された**メール添付ファイルのタイプ**

電子メールに関する脅威

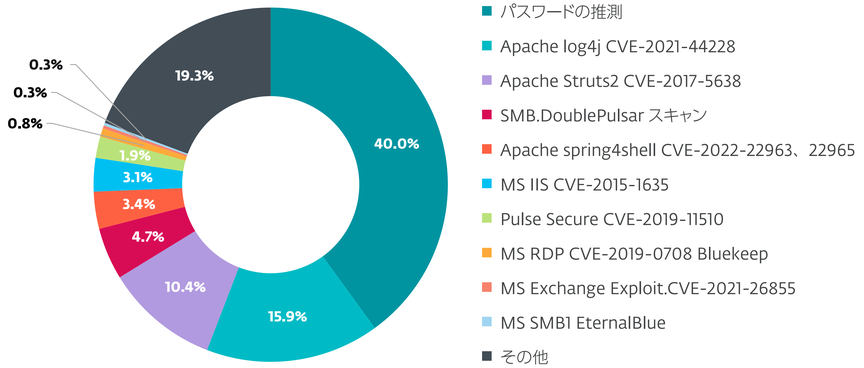


2024 年上半期における**メール脅威検出数の地理的な分布**

エクスプロイト

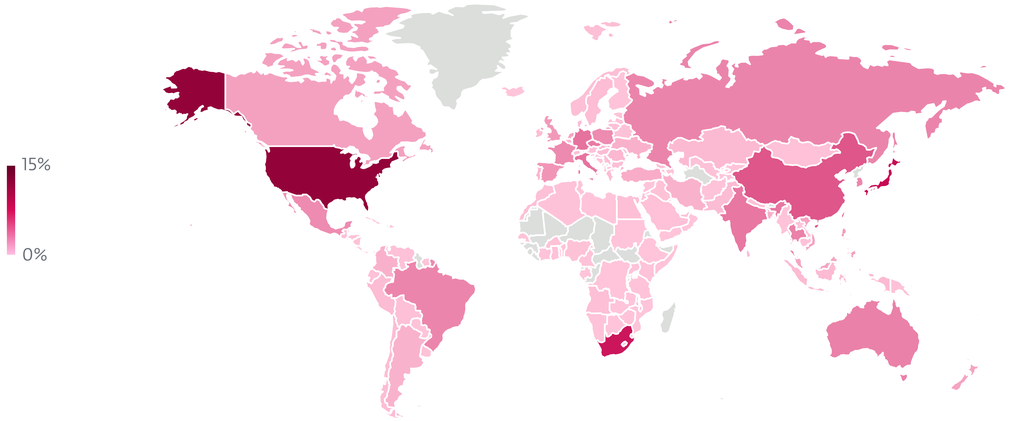


2023 年下半期および 2024 年上半期における **RDP、SMB、SQL 攻撃試行の傾向**、7 日間移動平均線

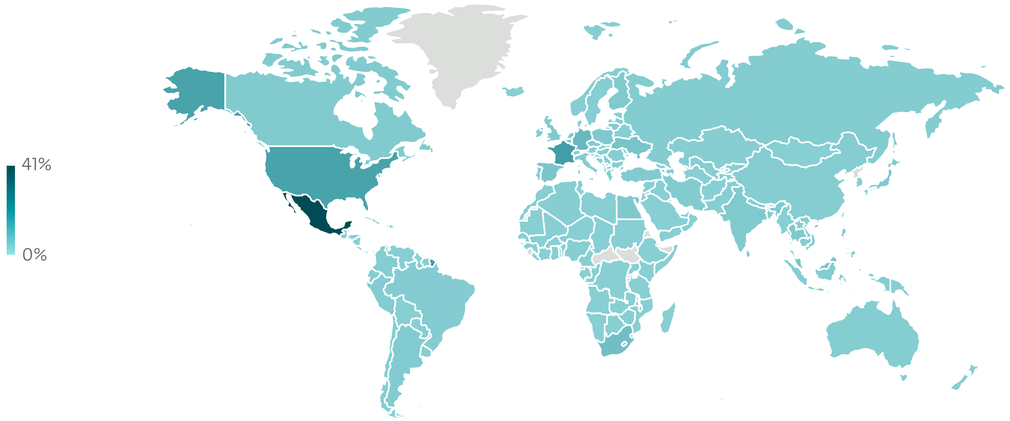


2024 年上半期にユニーククライアントから報告された**外部からのネットワークへの侵入方法**

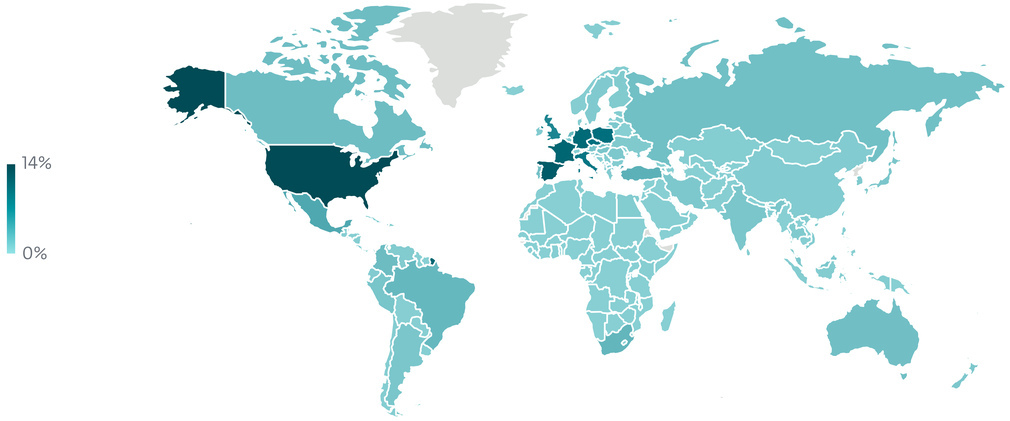
エクスプロイト



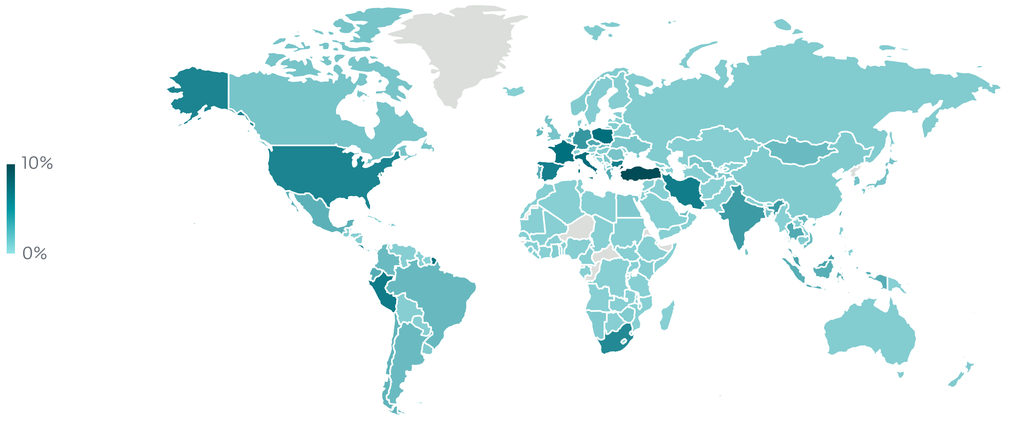
2024 年上半期に **RDP パスワード推測攻撃を実行したソースの地理的な分布**



2024 年上半期に **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**

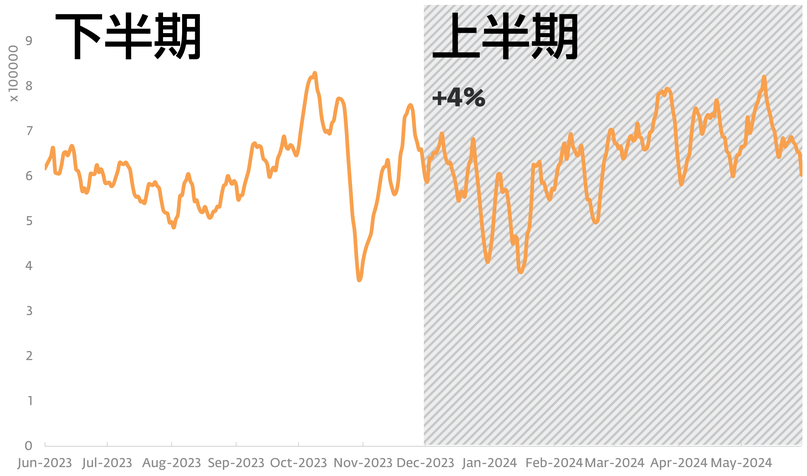


2024 年上半期に **RDP パスワード推測攻撃が実行された標的の地理的な分布**

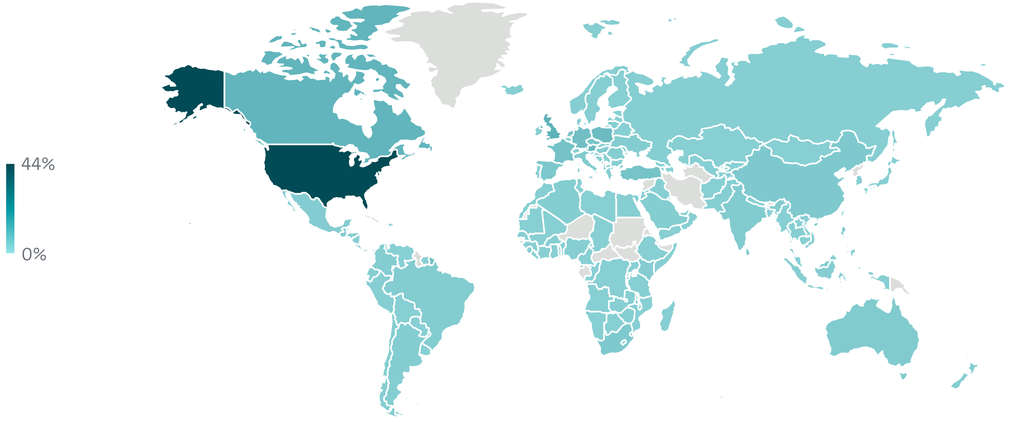


2024 年上半期に **SQL パスワード推測攻撃が実行された標的の地理的な分布**

エクスプロイト

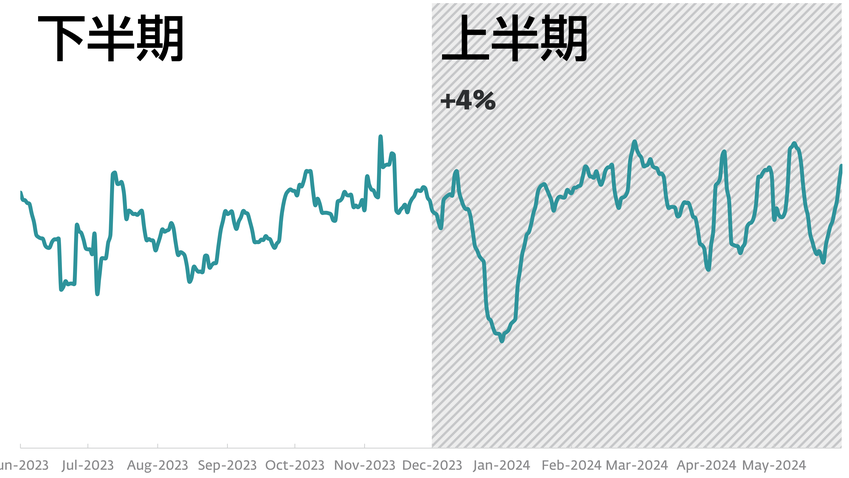


2023 年下半期から 2024 年上半期における **Log4Shell 攻撃試行の検出傾向**、7 日間移動平均線

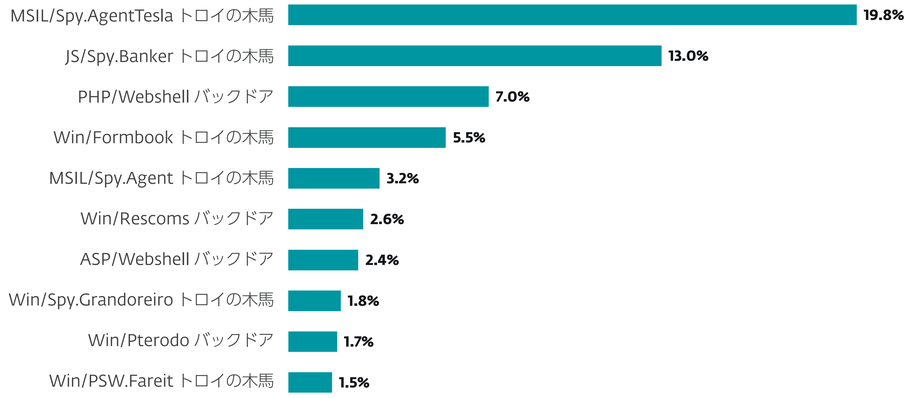


2024 年上半期における **Log4Shell 攻撃試行の地理的分布**

情報窃取型マルウェア

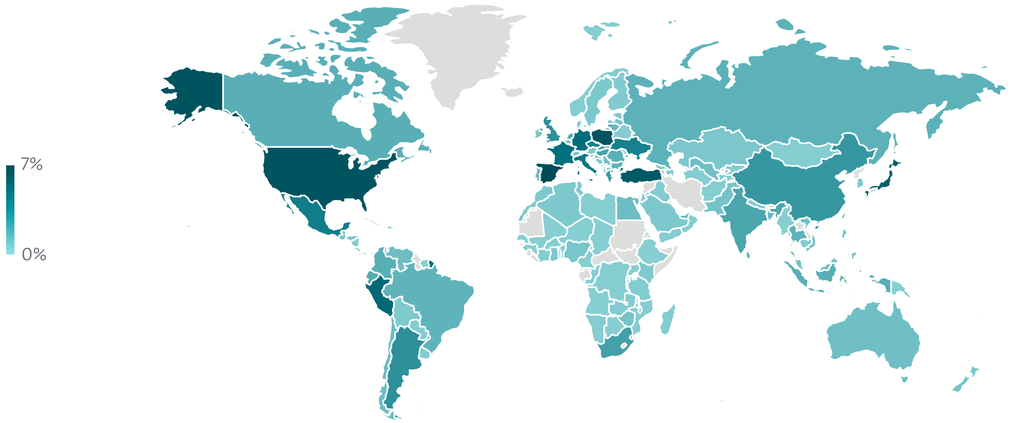


2023 年下半期から 2024 年上半期の**情報窃取型マルウェアの検出傾向**、7 日間移動平均線



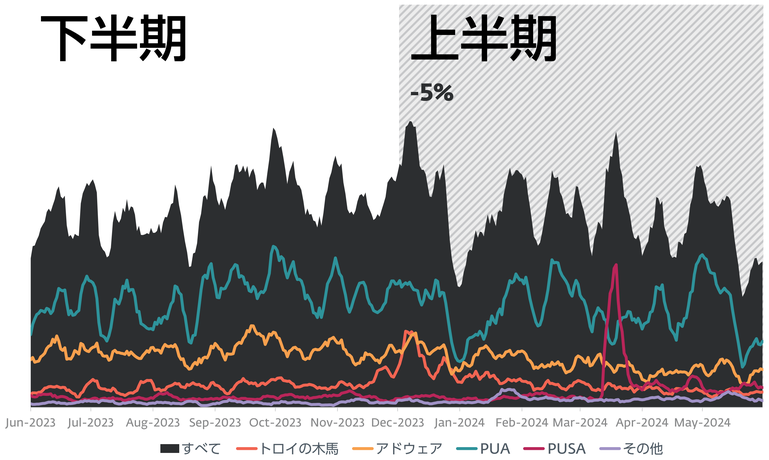
2024 年上半期における**情報窃取型マルウェアのトップ 10**（情報窃取型マルウェアの検出に占める割合）

情報窃取型マルウェア

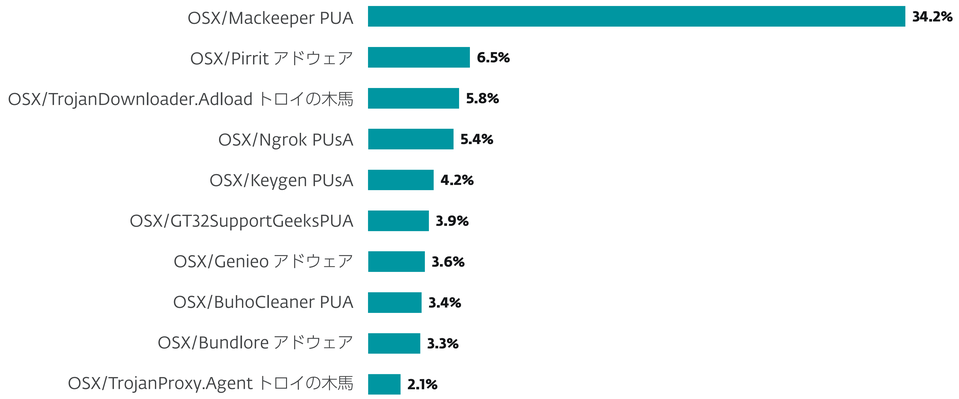


2023 年上半期における**情報窃取型マルウェアの検出の地理的な分布**

macOS

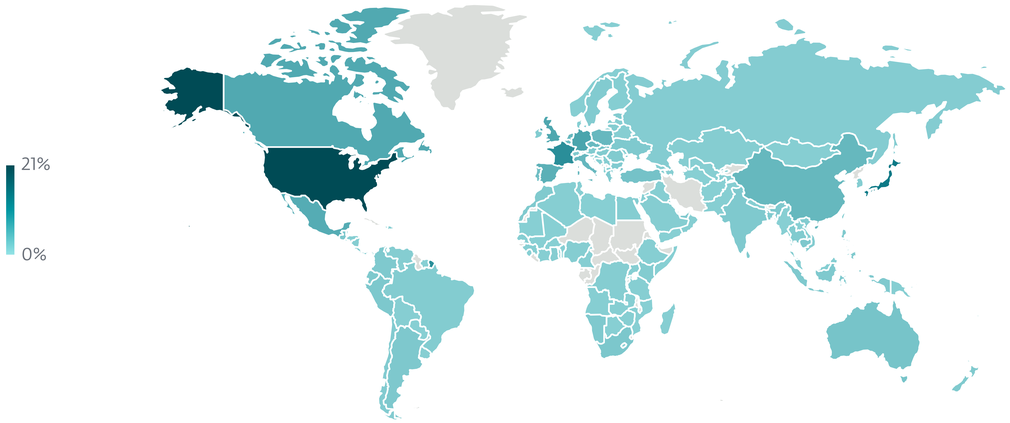


2023 年下半期～ 2024 年上半期の **macOS の脅威の検出傾向**、7 日移動平均線



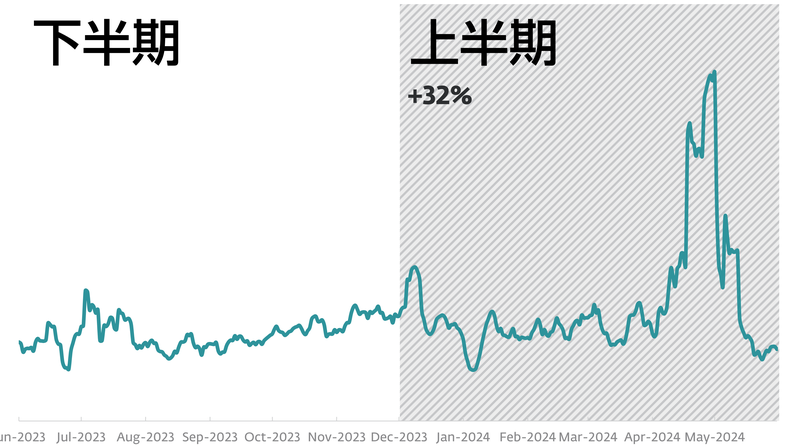
2024 年上半期における **macOS の脅威検出率トップ 10**（macOS の脅威の検出に占める割合）

macOS

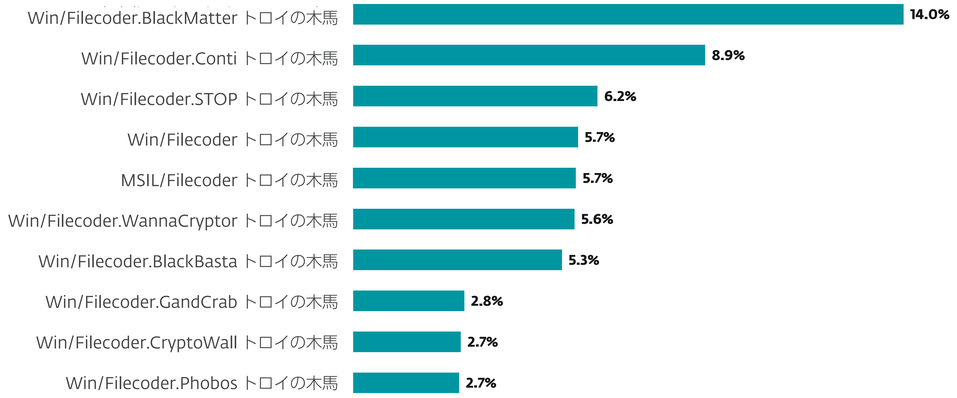


2024 年上半期における **macOS の脅威検出の地理的な分布**

ランサムウェア

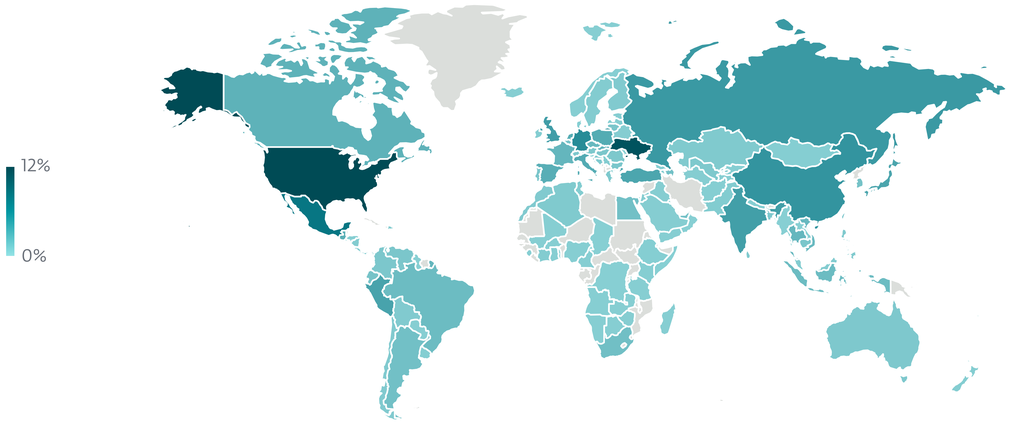


2023 年下半期～ 2024 年上半期の**ランサムウェアの検出傾向**、7 日移動平均線



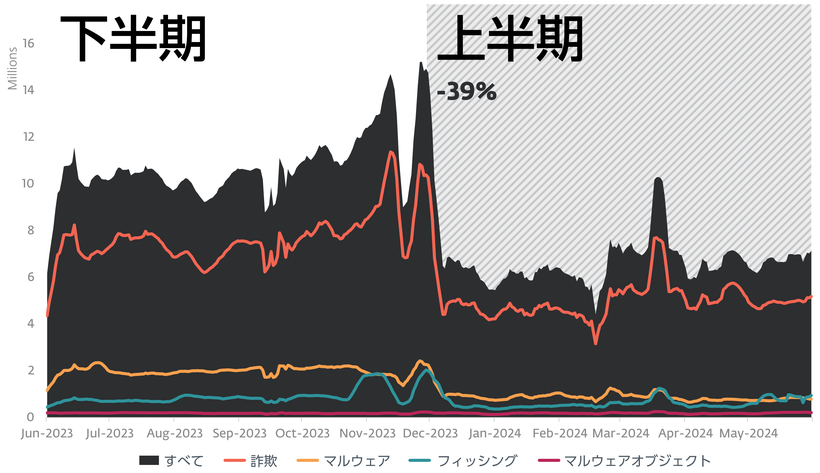
2024 年上半期における**ランサムウェア検出率のトップ 10**（ランサムウェアの検出に占める割合）

ランサムウェア

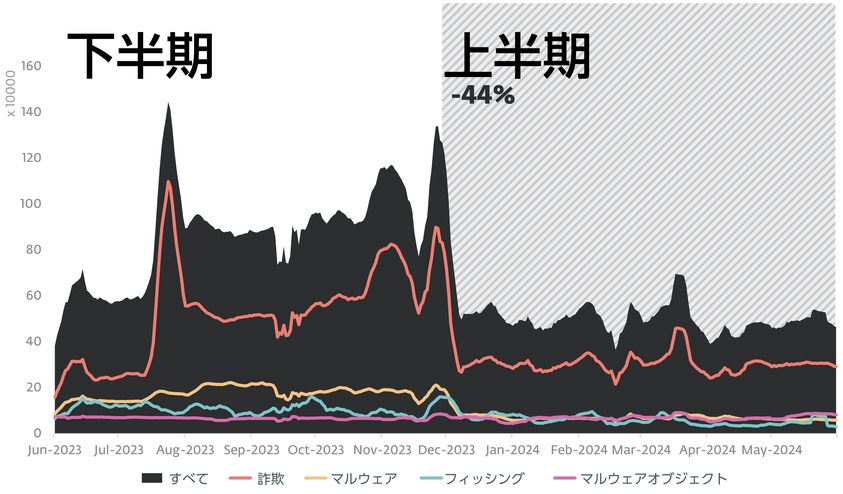


2024 年上半期における**ランサムウェア検出の地理的な分布**

Web に関する脅威

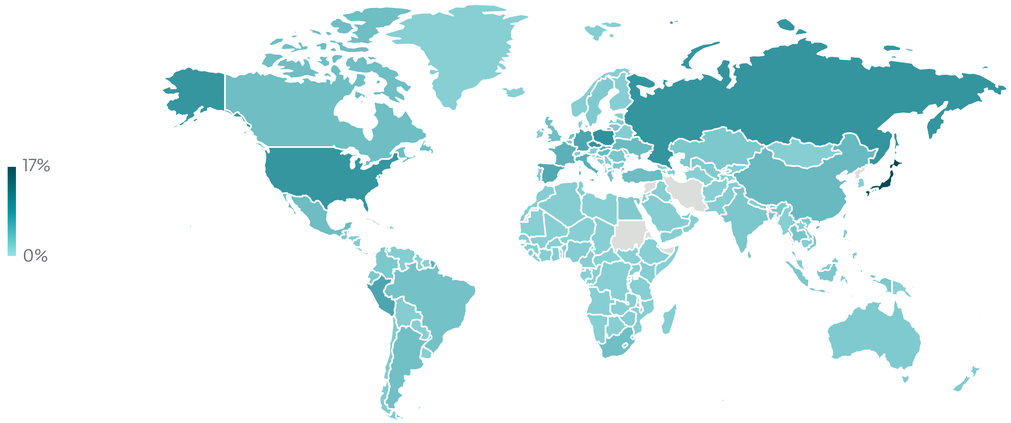


2023 年下半期～ 2024 年上半期に**ブロックされた Web 脅威の傾向**、7 日移動平均線

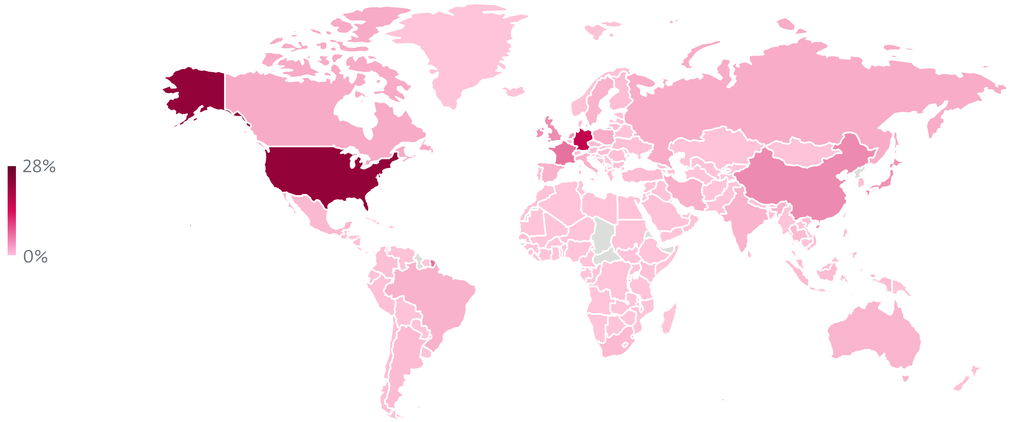


2023 年下半期～ 2024 年上半期に**ブロックされたユニーク URL の傾向**、7 日移動平均線

Web に関する脅威

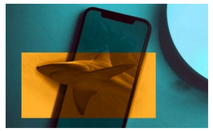


2024 年上半期に**ブロックされた Web 脅威の地理的な分布**



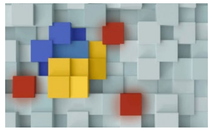
2024 年上半期に**ブロックされたドメインホストの検出数の地理的な分布**

調査レポート



ユーザーを食いものにするフィンテック：Android 向け不正な高金利の融資アプリ

ESET の研究者は、Android 向けの不正な高金利の融資アプリが増加していること、そして Google Play を回避するために使用されている手法について説明しています。



Python パッケージリポジトリ「PyPI」に混入したマルウェア

この 1 年間で、Python の公式パッケージリポジトリでホストされている悪意のあるパッケージが 1 万件以上ダウンロードされています。

クラウドサービスを利用したダウンローダーを使用する OilRig の執拗な攻撃

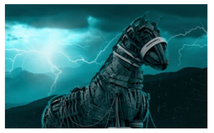
ESET の研究者は、C&C との通信に正規のクラウドサービスプロバイダを利用する一連の新しい OilRig ダウンローダーについての調査結果を公開しました。

ESET Research のポッドキャスト：ネアンデルタール人と マンモスと Telekopye

ESET の研究者は、Telekopye と呼ばれる Telegram ボットを使用してオンラインマーケットプレイスで詐欺を行っているさまざまな詐欺グループとこれらのグループ間の力関係について解説しています。

中国が関与する新しい APT グループによる、高度な AiTM（中間者）攻撃によって配信されるインプラント NSPX30

ESET の研究者は、中国とつながりがあると考えられる新たな APT グループ Blackwood が使用する高度なインプラント NSPX30 を発見しました。



銀行を標的とするトロイの木馬「Grandoreiro」を解体するためのグローバル作戦に参加

ESET は、技術分析、統計情報、既知のコマンド＆コントロールサーバーのドメイン名と IP アドレス情報を提供し、このプロジェクトに貢献しました。

ESET Research のポッドキャスト：ChatGPT、MOVEit のハッキング、Pandora マルウェア

このポッドキャストでは、AI チャットボットがサイバー犯罪を誘発している状況、ランサムウェアグループがランサムウェアを展開せずに組織から金銭を得ている手法、Android TV ボックスを標的とする新たなボットネットについて解説しています。

VajraSpy：APT グループ「Patchwork」が展開するスパイアプリ

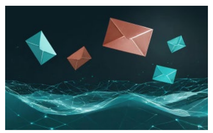
ESET の研究者は、APT グループ「Patchwork」が使用しているリモートアクセス型トロイの木馬「VajraSpy」を配信する Android アプリを複数発見しました。

Texonto 作戦：ウクライナ語を使用するユーザーを標的にした、戦時下における情報操作

心理戦、スパイ活動、カナダ薬局になりすますスパムメールなどについて解説しています。

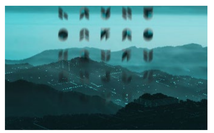
Evasive Panda、モンラム祭に便乗しチベット人を標的にした攻撃キャンペーンを実行

ESET の研究者は、チベット人を標的とするサイバースパイキャンペーンを発見しました。



AceCryptor スパムを利用するキャンペーン「Rescoms」

2023 年下半期における AceCryptor に関する ESET テレメトリの統計を、欧州諸国を対象とした Rescoms キャンペーンを中心に考察します。



eXotic Visit キャンペーン：Virtual Invader の足跡を追う

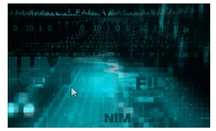
ESET の研究者は、一見無害なアプリを使用して主にインドとパキスタンのユーザーを標的とするスパイキャンペーン「eXotic Visit」を発見しました。

40 万台の Linux サーバーを侵害：暗号通貨を窃盗し、金銭的利益を目的とした Ebury の現状と隠蔽機能の進化

非常に高度なサーバーサイドのマルウェアキャンペーンが現在も展開されています。数十万台のサーバーが侵害されており、クレジットカード情報や暗号通貨を窃取する能力が追加され、Ebury の機能は多様化しています。

外交関連機関を狙う Lunar の 2 つのバックドア

欧州の外務省に侵入している APT グループ「Turla」が使用していると考えられる Lunar ツールセットについて ESET の研究者が技術的に分析した結果をお伝えします。



Nimfilt：Nim でコンパイルされたバイナリのリバースエンジニアリングツール

Nimfilt は、IDA プラグインと Python スクリプトの両方で利用でき、パッケージ名と関数名を分離し、文字列に構造体を適用することで、Nim プログラミング言語コンパイラでコンパイルされたバイナリのリバースエンジニアリングを支援します。

2023 年第 4 四半期～ 2024 年第 1 四半期の ESET APT 活動レポート

ESET APT 活動レポートは、2023 年第 4 四半期および 2024 第 1 四半期に ESET 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
Hana Matušková、マネージングディレクター

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

貢献者

Alexandre Côté-Cyr
Dušan Lacika
Igor Kabina
Jakub Souček
Jan Holman
Ján Adámek
Ján Šugarek
Jiří Kropáč
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Mathieu Tartare
Vladimír Šimčák
Yevhenii Fomiachenko

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

ESET® は、最先端のデジタルセキュリティで攻撃を未然に防ぎます。ESET は、AI と人間の専門知識の両方を取り入れて、既知や新たなサイバー脅威を防ぎ、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。詳細は、**www.eset.com/jp** をご覧ください。また、**LinkedIn**、**Facebook**、**Twitter（X）**でフォローしてください。

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