Digital Security
Progress. Protected.

ESET 脅威レポート

2023 年上半期

2022 年 12 月～ 2023 年 5 月

(eset):research

目次

序文 4

脅威環境の傾向 5

- 不正ローンアプリ、Android に新境地を見出す 6
- さまざまな顔を持つ暗号通貨の脅威 9
- 新しい攻撃方法を模索する Emotet のオペレーター。キャンペーンは縮小傾向。 12
- 悪意のある OneNote ファイル：マクロに代わる新たな侵入方法 14
- メールの脅威としてセクストーション（性的詐欺）が復活 16
- Microsoft SQL Server：ブルートフォース攻撃の魅力的なターゲットへ 19
- RedLine Stealer：マルウェアを配信するビジネス 22
- macOS が相互に関連する 2 つのサプライチェーン攻撃を受けた初めてのケース 25
- 同じコードを利用する異なるランサムウェアソースコードの漏えいにより、無数の亜種が登場 28

脅威テレメトリ 31

調査レポート 44

本レポートのデータについて 45

ESET について 46

エグゼクティブサマリー

Android

不正ローンアプリ、Android に新境地を見出す。

悪意のあるローンアプリの被害者の元には、迅速な資金援助ではなく、殺害予告や高利で貸付する案内が送り付けられています。

暗号通貨の脅威

多様な顔を持つ暗号通貨の脅威。

2023 年上半期、ビットコイン価格が復活したにもかかわらず暗号通貨の脅威の検出数は減少しましたが、決して油断できる状況ではありません。

Emotet ダウンローダー 攻撃手法

新しい攻撃方法を模索する Emotet のオペレーター。キャンペーンは縮小傾向。

悪名高いボットネット「Emotet」は、2023 年上半期には小規模な 3 つのキャンペーンを実施して存続を図っていますが、影響力は低下しています。

攻撃手法

悪意のある OneNote ファイル：マクロに代わる新たな侵入方法。

有名ないくつかのマルウェア系統は、拡散のメカニズムとして OneNote を利用する手法をテストしています。

メールの脅威 Web の脅威 詐欺 フィッシング

メールの脅威としてセクストーション（性的詐欺）が復活。

この半年で、セクストーションに関する詐欺やフィッシングが増加しました。

エクスプロイト 攻撃手法 SQL 攻撃

Microsoft SQL Server：ブルートフォース攻撃の魅力的なターゲットへ。

MSSQL のパスワード推測攻撃は急増し、Log4Shell の攻撃は特定の地域で増加し続けています。

情報窃取ツール サービスとしてのマルウェア

RedLine Stealer：マルウェアを配信するビジネス。

最近、ESET Research は、悪名高い情報窃取ツール「RedLine」の活動を妨害することに成功しました。

macOS サプライチェーン攻撃

macOS が相互に関連する 2 つのサプライチェーン攻撃を受けた初めてのケース。

相互に関連する 2 つのサプライチェーン攻撃が初めて実行され、macOS で検出された脅威が急増しました。この攻撃によって、多くの macOS デバイスが侵害されました。

ランサムウェア

同じコードを利用する異なるランサムウェア。ソースコードの漏えいにより、無数の亜種が登場。

ソースコードが漏えいしたことで、多くの犯罪者がランサムウェアを簡単に利用できるようになった一方で、既存の検知手法が新しいマルウェアに対しても高い効果を発揮するようになりました。

序文

2023 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。

ESET 脅威レポートの最新号をお届けします。この最新号では、内容が洗練されわかりやすくなっています。重要な変更点の 1 つは、データの表示方法です。検出カテゴリごとにすべてのデータの変化を詳述するのではなく、注意が必要な動向にフォーカスして、より詳細な分析を提供しています。各カテゴリに関連するテレメトリ（監視データ）を包括的に把握できるように、脅威テレメトリのセクションでは多くの図表を掲載しました。

もう1つの変更点は発行頻度であり、年3回から年2回に変更されました。本号では、2023 年上半期（2022 年 12 月から 2023 年 5 月まで）のハイライトを取り上げます。この期間と比較する場合の 2022 年下半期とは、2022 年 6 月から 2022 年 11 月までの期間を指します。

2023 年上半期には、サイバー犯罪者の驚くべき適応能力と、悪意のある目標（脆弱性の悪用、不正なアクセス、機密情報の窃取、ユーザーからの金銭詐取など）を達成するためであれば、新たな手法を探求し、どんな手段も厭わない姿勢が明確となっています。攻撃パターンが変化している理由の 1 つは、Microsoft が行った、マクロが埋め込まれたファイルを開くときのポリシーの変更です。2023 年上半期、攻撃者はこうした対策を回避する新たな試みとして、OneNote に別のファイルを直接埋め込む機能を利用し、武器化した OneNote ファイルをマクロの代わりにしました。これを受けて Microsoft が再調整を行ったことで、サイバー犯罪者は別の侵入方法を模索し続けることになりました。Microsoft SQL Server に対するブルートフォース攻撃が激化したのは、攻撃者がさまざまなアプローチをテストしていたことが原因と考えられます。

ESET のテレメトリデータから、かつて悪名を轟かせていた Emotet ボットネットのオペレーターが、マイクロソフトがインターネット経由で入手したファイルのマクロをデフォルトで無効にするなどの対策に格闘していることを読み取ることができます。攻撃手法が変化していることなどから、別のグループが Emotet ボットネットを買収した可能性があります。ランサムウェアの領域では、攻撃者が新しいランサムウェアの亜種を作成する目的で、流出したソースコードを再利用するケースが増えています。これにより、スキルの低い攻撃者であってもランサムウェアを簡単に悪用できるようになった一方で、防御側は汎用的なルールと検出結果を使用して、最新のランサムウェアなど幅広い亜種に対応できるようになりました。

ESET のテレメトリでは、暗号通貨の脅威は引き続き減少しています。最近、ビットコインの価値は上昇していますが、これらの脅威は増加していません。しかし、暗号通貨関連のサイバー犯罪活動は依然続いており、暗号通貨を不正にマイニングする機能や窃取する機能が汎用性の高いマルウェアに組み込まれるケースが増えています。この進化は、キーロガーなどのマルウェアが最初は別の脅威として特定されていたものの、最終的には多くのマルウェアが実装する共通の機能として認識されるというこれまでと同じパターンをたどっています。

金銭を目的とする他の脅威を調査したところ、インターネットの利用に関するユーザーの恐怖心につけ込む、いわゆるセクストーション（性的詐欺）メールの復活や、正規の個人向けローンサービスを装い、緊急の融資を必要としている個人を狙った偽の Android ローンアプリの増加が確認されました。

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。

リサーチ部門　最高責任者
Roman Kováč

脅威環境の傾向

Android

不正ローンアプリ、Android に新境地を見出す

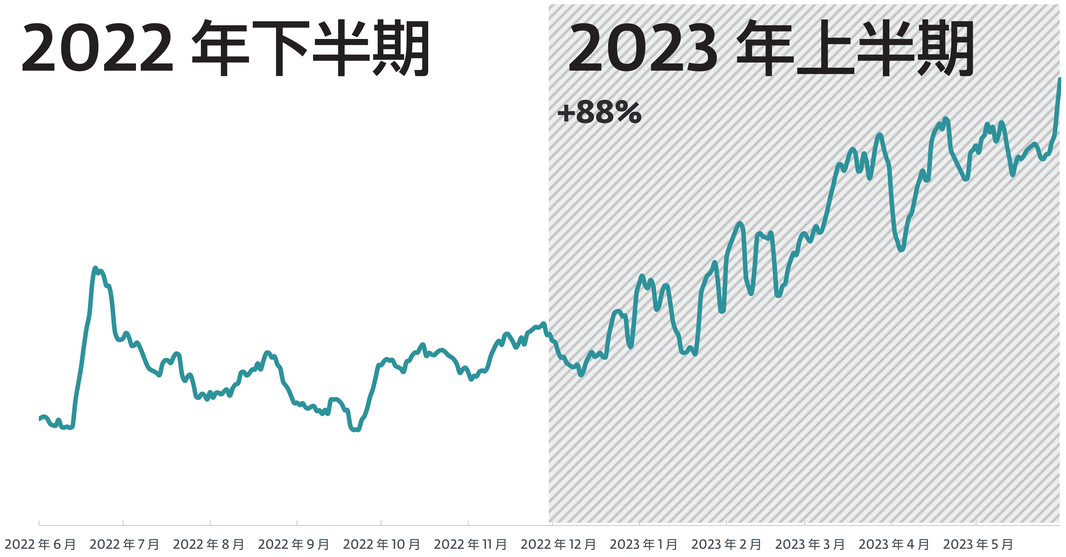
悪意のあるローンアプリの被害者の元には、迅速な資金援助ではなく、殺害予告やデジタル高利貸しの案内が送り付けられています。

I2023 年上半期、合法的な個人向けローンサービスを装い、手軽な貸付を約束する Android ローンアプリが急増していることが、ESET のテレメトリにより確認されました。これらのサービスは、実際にはユーザーを騙して個人情報や資産情報を入手することを目的としています。ESET 製品は、これらのアプリを、スパイウェア機能の「スパイ」と融資の「ローン」を組み合わせた「SpyLoan」という検出名で識別しています。

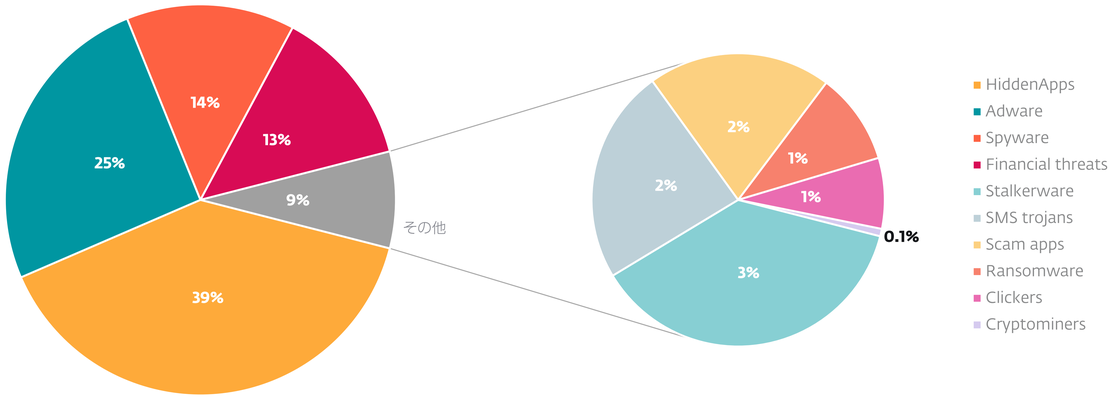
これらの不正アプリは、ソーシャルメディアや SMS メッセージを通じて個人向けローンを提供すると宣伝しており、アプリ自体は専用の詐欺サイト、サードパーティのアプリストア、および（Google Play のポリシーも迂回可能であるため）Google Play からダウンロードできるようになっています。ESET は Google App Defense Alliance パートナーとして、調査結果を Google と共有しており、これらのアプリへの対応を Google と協同で進めています。

2022 年下半期と比較すると、2023 年上半期にはすべての SpyLoan アプリの検出数は約 90% 増加し、Android スパイウェアカテゴリ全体では 19% 増加しました。

スパイウェアは、Android で最も検出数の多い脅威ではありません。Android プラットフォームでは、オンライン広告を介してサイバー犯罪者に利益をもたらす脅威（アドウェア、隠しアプリ、クリッカー）が急増しています。**ESET 脅威レポート 2022 年第 3 三半期**では、クリスマス前にアドウェアや隠しアプリが増加した理由として、無料のモバイルゲームにアドウェアが詰め込まれていたことや、開発者がアドウェアや隠しアプリを簡単に作成・配布できる Android 用開発ツール／リソースが入手可能になっていることを説明しました。2022 年 12 月の時点で、隠しアプリ（+42%）とアドウェア（+19.5%）の検出数が増加した主な原因は、広告を表示するゲームアプリでした。広告から利益を得ているすべてのカテ



2022 年下半期～ 2023 年上半期の **SpyLoan 検出の傾向**、7 日移動平均線



2023 年上半期の **Android の脅威検出カテゴリ**

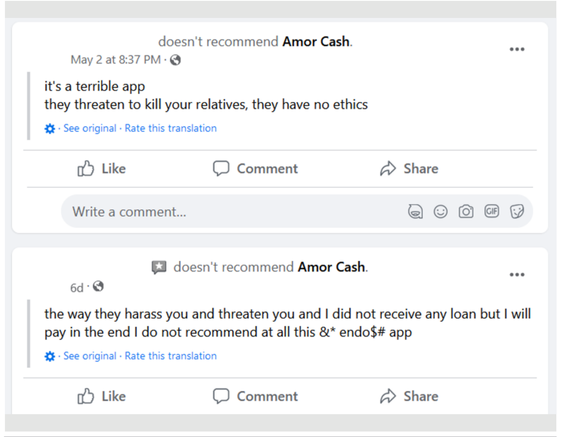
ゴリの検出数を合計すると、Android での全検出における割合は 68.4% になります。

2023 年上半期に他の Android の検出数が目に見えて減少したにもかかわらず（SMS トロイの木馬は 62.5%、ランサムウェアは 50%、クリプトマイナーは 16%）、アドウェアと隠しアプリは蔓延しており、Android での全検出数は 20.2% 増加しました。

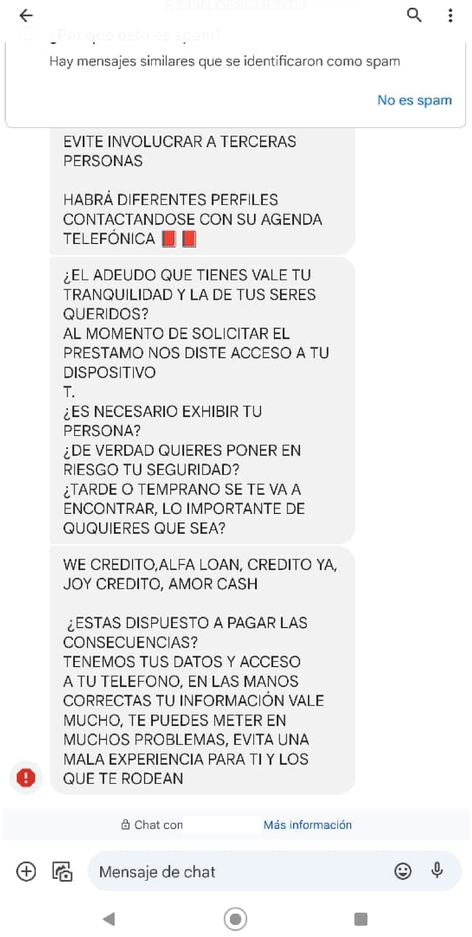
検出数の変化が少なかった唯一の脅威タイプは、バンキングマルウェアとクリプトスティーラーなどの金融関連の脅威です。今期全体では減少傾向にあるものの、4.5% 増加しています。

SpyLoan アプリも金融関連の脅威のタイプではありますが、バンキングマルウェアとは異なり、お金が必要で困っている個人や、一般の金融機関を利用できない借り手の弱みにつけ込んで、法外な高金利で融資する現代のデジタル闇金融の一形態です。

インストールされたアプリは、アカウントリスト、通話ログ、カレンダーイベント、デバイス情報、インストール済みアプリのリスト、ローカル Wi-Fi ネットワーク情報、デバイスにあるファイル情報（写真そのものを実際には送信しない Exif メタデータなど）、連絡先リスト、位置情報、SMS メッセージへのアクセス許可を要求します。ユーザーレビューによると、ユーザーが融資を申し込んだか、あるいは融資を受けるかに関係なく、アプリの実行者は被害者に嫌がらせや恐喝をし、時には殺害予告をすることもあります。また、SpyLoan アプリのユーザーは、金利が非常に高く、融資期間が非常に短い（時には 5 ～ 7 日）こともあると述べています。



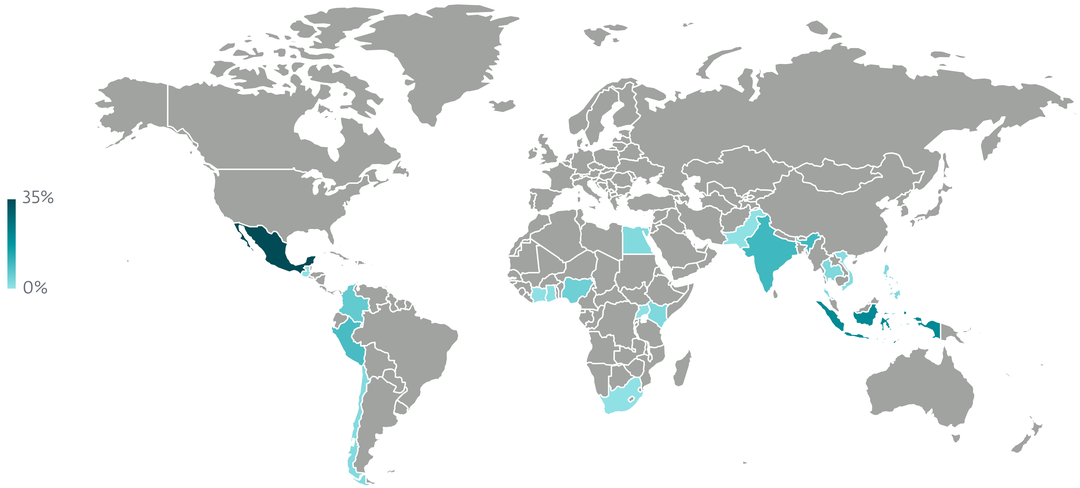
嫌がらせや脅迫を受けたと主張する SpyLoan アプリのユーザー



あるレビュアーが投稿した機械翻訳された脅迫メッセージ：あなたが抱えている借金で、自身、そして愛する人の心の平穏を乱さないでください。本当に自分の安全がどうなっても構わないのですか？その代償を支払う覚悟がありますか？多くの問題に巻き込まれるかもしれません。自分と周り人が嫌な思いをしない選択をしてください。

ESET のテレメトリによると、これらのアプリの実行者の主な活動拠点はメキシコ、インドネシア、香港、タイ、インド、パキスタン、コロンビア、ペルー、フィリピン、エジプト、ケニア、ナイジェリア、シンガポールです。これらの国以外で検出されたアプリは、これらの国のいずれかに登録された電話番号にアクセスできる電話と関連性があると考えられます。

SpyLoan アプリがユーザーを騙すために展開するコミュニケーションは重層的で複雑であるため、今後 WeLiveSecurity.com のブログで説明する予定です。一般的に、SpyLoan アプリは文言やデザインが正規のローンアプリに酷似しています。金融用語や法律用語が使用されている場合もあり、アプリの真偽を判断することが難しくなっています。



2023 年上半期に ESET テレメトリで検出された SpyLoan の地理的分布

ESET のエキスパートの解説

このような不正なローンアプリによってさまざまな課題がもたらされますが、ユーザーが自らを守るために採用できる効果的な手段があります。例えば、公式アプリだけをダウンロードして使用すること、肯定的なレビューは被害者が強要されて書いた可能性があるためアプリの否定的なレビューを読むこと、評判の良いセキュリティアプリを使用すること、などです。SpyLoan アプリの被害に遭った個人は、地元の法執行機関または関連する法的機関に事件を報告し、消費者保護団体に連絡し、民間融資を管理する機関（国立銀行またはそれに相当する機関）に通知する必要があります。不正なローンアプリを Google Play 経由で入手したのであれば、Google Play サポートに支援を求め、アプリを通報し、関連する個人データの削除を要求できます。ただし、データはすでに攻撃者の C&C サーバーに抜き取られている可能性があります。

ESET シニアマルウェアリサーチャー、
Lukáš Štefanko

暗号通貨の脅威

さまざまな顔を持つ暗号通貨の脅威

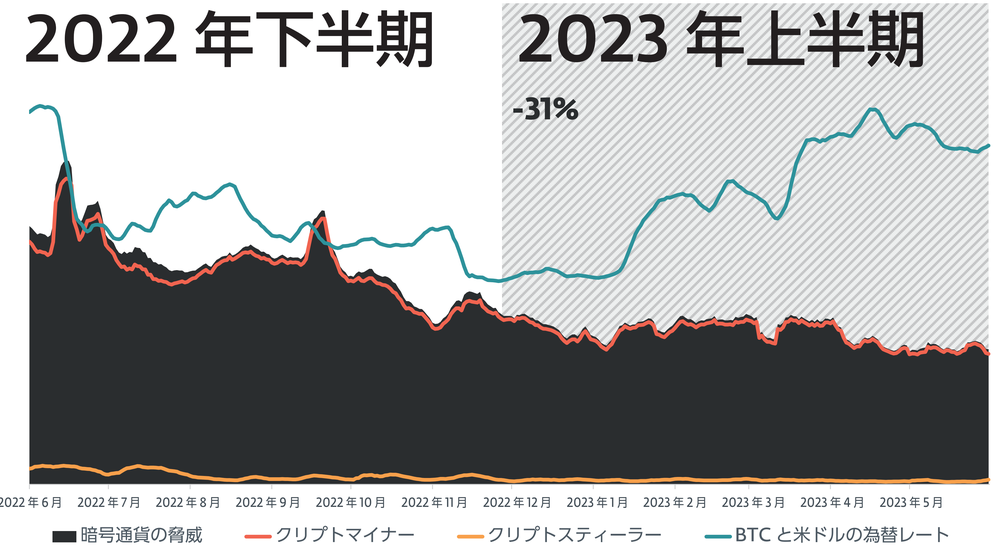
2023 年上半期、ビットコインが復活したにもかかわらず暗号通貨の脅威の検出数は減少しましたが、決して喜ぶことはできません。

ESET が暗号通貨の脅威を追跡し始めてから、これらの脅威が検出される傾向はビットコインの為替レートと概ね一致していました。ビットコインの上昇／下落に合わせて暗号通貨の脅威[1]が増減するのは当然だと思われていましたが、2023 年上半期にその傾向は分かれました。

2023 年上半期、ビットコイン人気は一部で復活しました。2022 年の 11 月から 12 月にかけて、ビットコインは長期的に下落し、1BTC あたり 2 万ドルを下回るレートが続いていましたが、4 月中旬に 3 万ドルの大台まで上昇し、下落する局面も見られましたが、その後も上昇を続けています。ビットコイン価格の最近の上昇は、いくつかの銀行（SVB、シグネチャー銀行、シルバーゲート）が閉鎖され、ユーザーが分散型通貨を支持し、従来の銀行システムを利用しなくなったことへの反動であると考えられます。それでも、世界第 2 位の暗号資産取引所である **FTX** の破綻など、暗号通貨ヘッジファンドの破綻が相次いだ後では、ビットコインの価格の上昇が長続きするかどうかは未知数です。

逆に、暗号通貨の脅威の傾向は 2023 年上半期も高まりませんでした。このカテゴリの検出数は着実に減少し続け、期間全体では 31% の減少でした。そこで浮かぶのは、「暗号通貨マルウェアはどこに行ってしまったのか」という疑問です。サイバー犯罪者は、クリプトマイナーやクリプトスティーラーを使うのを止めただけなのか、それとも別の何かが起きているのでしょうか。

一方、過去数か月間の ESET テレメトリでは、新たな暗号通貨脅威の検出数が減少していることが記録されています。また、最近は暗号通貨関連の犯罪を標的とした**法執行機関による取り締まり**が数多く成功しています。攻撃者が暗号通貨を狙った活動を見直しており、その結果検出件数が減少した理由として、報復を恐れたことが挙げられます。おそらく、暗号通貨の為替レートが常に変動していることも抑止力となっています。一方、このような脅威の状況を語る上で、暗号通貨のみに焦点を当てた脅威だけを検証しても、もはや意味はありません。ここ数年、暗号通貨をめぐる悪意のある活動は



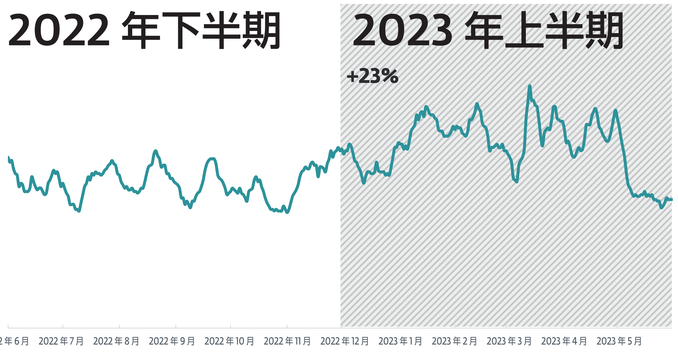
2022 年下半期～ 2023 年上半期の**暗号通貨脅威の検出傾向**とビットコイン / 米ドル為替レート、7 日移動平均線

[1] クリプトマイナーおよびクリプトスティーラー

大きく多様化しています。攻撃者はできる限り多くの利益を得ようしており、暗号通貨だけを狙う脅威ではなく、より広範な機能を持つマルウェアを選択するのは理にかなっています。そのため、今や暗号通貨を盗んだりマイニングしたりするコンポーネントは別のマルウェアに組み込まれるようになっています。

有名な情報窃取型マルウェアの中でも、**RedLine Stealer**、Agent Tesla、および Racoon Stealer は暗号通貨の窃取機能を備えており、例えばトロイの木馬「Fareit」は感染したマシン上で暗号通貨をマイニングできます。これらのマルウェア系統はすべて、合計検出数が数十万件を数える大規模なものであり、暗号通貨が主な目的ではなくても、対象は広範囲に及びます。

他の脅威もまた、暗号通貨マルウェアの流行に乗じています。例えば、暗号通貨の窃取機能は、非常に多くの ClipBanker マルウェアの系統（クリップボード内のデータを盗んだり操作したりする脅威）に統合されており、暗号通貨の脅威と明確に区別できなくなっています。これらの脅威は、2023 年上半期に 23% 増加しました。



2022 年下半期～ 2023 年上半期の **ClipBanker 検出の傾向**、7 日移動平均線

これとよく似た脅威の状況が Android でも起きており、暗号通貨の盗取機能が蔓延しているため、ESET は「バンキングマルウェア」サブカテゴリの分類を金融関連の脅威に変更しました。ClipBanker マルウェア系統と比較すると、Android の金融関連の脅威の傾向は、2022 年下半期と 2023 年上半期にかけて横ばいです。

Android ユーザーを食い物にする暗号通貨の脅威がいかに狡猾であるかを示す例として、ESET の研究者は、チャットメッセージで送信された暗号通貨のウォレットアドレスを攻撃者のアドレスにすり替えるトロイの木馬化された WhatsApp および Telegram アプリの形をしたクリッパーを数十個**発見しています**。多くの場合、改ざんされたアドレスはメッセージの受信者にしか表示されないため、被害者はウォレットアドレスがすり替えられたことを知る機会がありません。

暗号通貨マルウェアを拡散するもう 1 つの経路は、ボットネットです。そうしたボットネットの 1 つが、地下フォーラムで販売されている人気のダウンローダー「Amadey」であり、そのソースコードはすでにオンライン上に流出しています。Amadey の特筆すべき機能は、暗号通貨ウォレットの情報を窃取することです。このボットネットは、2023 年上半期に大きく拡大し、その数は期間中に約 370% 増加しました。ESET が追跡しているもう 1 つのボットネット「Danabot」は、クリプトスティーラーを備えた実行ファイルと、さらには暗号通貨ウォレットのアドレスを改ざんできる LaplasBanker をプッシュしていることが確認されています。

ESET のエキスパートの解説

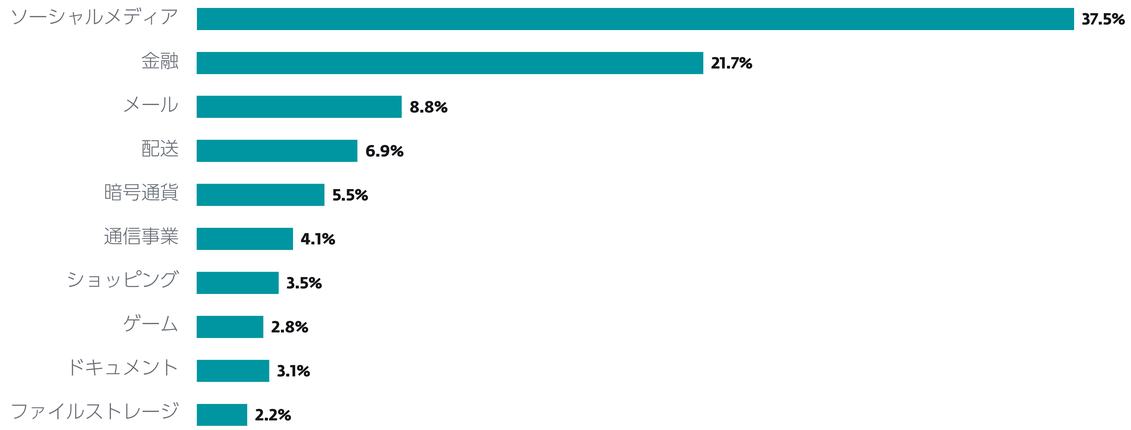
暗号通貨の脅威の衰退は、ビットコインが復調した現在も覆されることはなく、今後も減少が続くと予想されます。しかし、強欲なサイバー犯罪者は暗号通貨が存在する限り、何らかの形で暗号通貨を狙い続けるはずです。時間の経過とともにこのカテゴリのクライムウェアは減少していくかもしれませんが、暗号通貨を狙う機能は他のマルウェアに組み込まれつつあります。このような多目的型の脅威に対しては、さまざまな詐欺やフィッシングと同様に、常に警戒を怠らないようにする必要があります。

ESET シニア検出エンジニア、
RedLine Stealer

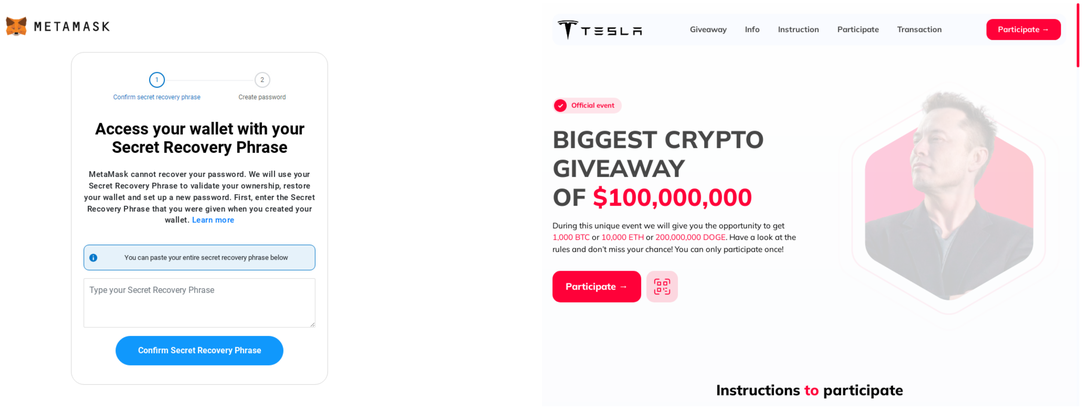
暗号通貨を狙うクライムウェアが時と共に広まってきましたが、サイバー犯罪者の活動はさまざまな暗号通貨詐欺やフィッシングに集約されています。その代表的な例が、悪名高い「豚の屠殺詐欺（pig butchering）」と呼ばれる手口であり、その多くは 2023 年上半期現在も盛んに実行されています。このような手口では、攻撃者はまずソーシャルエンジニアリングの手法を使って標的ユーザーの信頼を獲得し、親密な関係を築いた上で、投資アプリなどの偽の暗号通貨ベンチャーに投資するよう説得します。標的ユーザーがお金を出せなくなると、攻撃者は資金を盗んで姿を消します。こうした詐欺は莫大な利益を上げているようで、米司法省は先日、豚の屠殺詐欺を行うさまざまなグループから 1 億 1,200 万ドル以上の資金を押収しました。

他のマルウェアと同様に、フィッシングサービスも製品化され、攻撃者が別の攻撃者に PhaaS（サービスとしてのフィッシング）を提供するようになっている可能性があります。最近、暗号通貨詐欺に特化した PhaaS 攻撃が、Scam Sniffer によって確認されています。この攻撃は Inferno Drainer と呼ばれる詐欺業者が運営するもので、MetaMask や OpenSea といった有名な暗号通貨ウォレットやマーケットプレイスになりすまして、何百ものフィッシングサイトを作成し、報告時点で 600 万ドル近くの暗号通貨を盗んでいました。この業者は、フィッシングキャンペーンを管理するためのコントロールパネルを提供するほか、売り上げの 30% と引き換えにフィッシングサイトを構築するオプションも提供しています。

ESET のフィッシングフィードによると、暗号通貨をテーマにしたフィッシング詐欺は、2023 年上半期に 5 位にランクインしています。フィードを検索してみると、暗号通貨の交換所のなりすまし、不正な P2E（お金を稼ぐ）ゲーム、暗号通貨プレゼント詐欺などの事例が数多く確認されました。



2023 年上半期における**フィッシングサイトのユニーク URL 数で見た上位 10 のカテゴリ**



ESET フィッシングフィードで確認された暗号通貨をテーマにしたフィッシング／詐欺サイトの例

Emotet ダウンローダー 攻撃手法

新しい攻撃方法を模索する Emotet のオペレーター。キャンペーンは縮小傾向。

悪名高いボットネット「Emotet」は、2023 年上半期には小規模な 3 つのキャンペーンを実施して存続を図っていますが、影響力は低下しています。

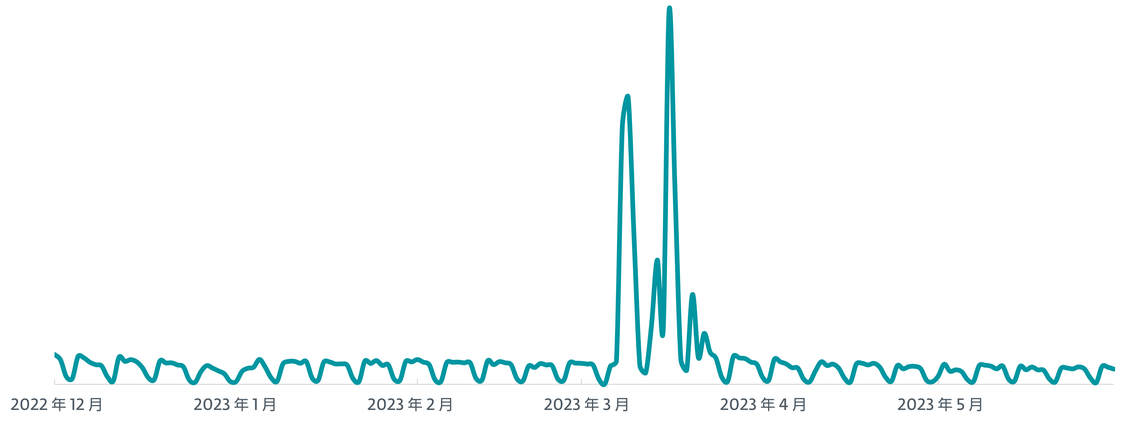
インターネットから入手した Office 文書について、VBA（Visual Basic for Applications）マクロがデフォルトで無効化されるようになってから、Emotet のオペレーターは、VBA と同じような成果が期待できる代替手法を見つけようと躍起になっています。2023 年の上半期には、特徴が異なる 3 つのマルスパムキャンペーンを実施しましたが、これらのキャンペーンでは侵入経路とソーシャルエンジニアリングの手法を変更しながらテストしています。攻撃の規模が縮小しており、手法を絶えず変更していることは、これまでの結果に満足していないためと考えられます。

Emotet ボットネットは数か月間休止した後で、活動を再開しました。最初のキャンペーンは、2023 年 3 月 8 日頃に発生しました。このキャンペーンでは、Emotet ボットネットが悪意のある VBA マクロを埋め込んだ Word 文書を、請求書を偽装して配信しています。検出を回避し、検体の解析を長引かせるために、Emotet オペレーターはファイルサイズを意図的に 500MB 以上に膨らませています。これは、犯罪行為を目的として作成されたプログラムであるクライムウェアや、いくつかの ATP グループが過去に利用してきた手法です。

この一連のマルスパムキャンペーンについて、注意すべきことが 2 つあります。まず、Emotet のオペレーターはリプライチェーン攻撃を使用していないことです。リプライチェーン攻撃とは、被害者の既存の会話に対する返信として悪意のあるメールを配信し、正規のメールのように見せかける手法です。

次に、マイクロソフトがインターネットから送信した文書について、VBA マクロをデフォルトで無効化したにも関わらず、VBA マクロが使用されるという奇妙な状況だったことです。つまり、攻撃を受けたユーザーの多くが、埋め込まれた悪意のあるコードを実行することはなかったはずです。マクロを有効にするために必要なすべての操作が実行されたとしても、信頼できる多層防御ソリューションを導入していれば、Emotet バイナリがダウンロードされるときや、ダウンロード後の操作が実行されるときに、この脅威は検出されブロックされるはずです。

3 月 13 日から 3 月 18 日にかけて行われた 2 回目のキャンペーンを見ると、攻撃者は最初のキャンペーンの欠陥に気が付いた可能性があります。リプライチェーン攻撃の手法を利用



ESET のテレメトリで確認された **2023 年の Emotet キャンペーン**

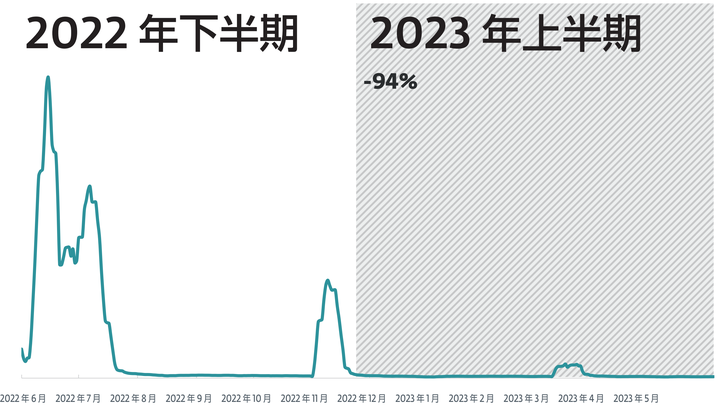
し、VBA マクロから、VBS スクリプトが埋め込まれた OneNote ファイル（`.one`）に切り替えています。標的ユーザーがこれらのファイルを開くと、保護されているように見える **OneNote ページ** が表示され、ファイルの内容を見るには「表示」ボタンをクリックするように求められます。このグラフィック要素の背後には、Emotet の DLL をダウンロードして実行するように設定された VBS スクリプトが隠されています。

OneNote は、この操作によって悪意のあるコンテンツが開かれる可能性があることを警告しますが、ユーザーはこのような確認画面に特に注意せずにクリックすることが習慣になっており、デバイスを侵害される恐れがあります。

ESET のテレメトリから、3 月 20 日に米国における年度末の納税時期に便乗した最後のキャンペーンが開始されたことが特定されました。ボットネットによって送信された悪意のあるメールは、連邦政府機関の内国歳入庁（IRS）から送信されたように装い、`W-9 form` という名前の ZIP ファイルが添付されています。

2023 年の最初のキャンペーンと同様に、この ZIP ファイルには、意図的にサイズを膨らませた ZIP ファイルと同じ名前の Word 文書が含まれており、攻撃を成功させるためには、埋め込まれた VBA マクロをユーザーに有効にさせる必要がありました。繰り返しになりますが、マイクロソフトの新しいポリシーが実行されており、デフォルトでマクロが無効になっているため、この攻撃は成功しなかったはずです。また、米国における納税をテーマにしており、キャンペーンの標的を米国のユーザーに限定していました。しかし、ESET のシステムは、あまり拡散していなかったものの、VBScript が埋め込まれていた攻撃も検出しており、OneNote を使用した別のキャンペーンが同時に進行していたことがわかっています。

全体として、2023 年に検出された Emotet キャンペーンは数万件にとどまっており、2022 年下半期に記録された数百万件の検出数と比較して約 95% 減少しています。最も頻繁に使用された攻撃方法は、武器化された Office ファイル（通常は Word 文書と Excel スプレッドシート）であり、これは検出された攻撃数の 58% を占めています。次は VBA マクロが 29% で、埋め込み VBS スクリプトが 10% でした。



最新の Emotet キャンペーンと 2022 年下半期の過去の活動との比較。

ESET の検出結果で最も攻撃を受けた国を見ると、日本（31%）、イタリア（11%）、メキシコ（5.5%）となっていますが、日本やイタリアは ESET 製品を導入しているユーザー数が多いことから、これらのデータには偏りがある可能性があります。

Emotet のオペレーターが、デフォルトで無効になっている VBA マクロに固執した理由や、いくつかのキャンペーンで効果の高いリプライチェーン攻撃を利用しなかった理由は不明なままです。Emotet による攻撃は成功する確率が高いことがこれまで知られてきましたが、今回のような綻びが見えるのは、高度な技術力のない別の脅威グループが Emotet のボットネットとインフラを 2022 年下半期に買い取ったという噂を裏付けている可能性もあります。

Emotet の概要

Emotet は、最初は 2014 年 6 月に銀行を標的とするトロイの木馬として確認されました。それ以降、犯罪者にマルウェアを展開するサービスを提供するプラットフォームへとその姿を変え、侵害したシステムへのアクセス情報も他の犯罪グループに販売しています。そのため、Emotet がコンピューターで実行されている場合、通常、別のマルウェアもダウンロードされ実行されています。

Emotet はモジュール型のプログラム設計になっており、これまでは、悪意のある Microsoft Word 文書が添付されたスパムメールを通じてメインモジュールが配信されていました。Emotet はその後、追加のモジュールを使用してさらにネットワークに拡散します。ネットワーク共有のユーザー名とパスワードに対してブルートフォース攻撃を実行し、侵害したシステムをプロキシとして利用し、そのシステムからメールアドレスとメッセージを窃取し、さまざまな悪意のあるアクションを実行します。

2021 年に Emotet はテイクダウンされましたが、その後活動を再開しました。2022 年 3 月と 4 月には**スパムキャンペーンを繰り返し**ていましたが、この時期にマイクロソフトはマクロが含まれる Office 文書の**「コンテンツの有効化」ボタンを削除**しました。この環境の変化に対応するため、Emotet の開発者は、マルウェア配信プラットフォームとして最初に利用していた「マクロ」に代わる手法を模索し実験するようになりました。

攻撃方法

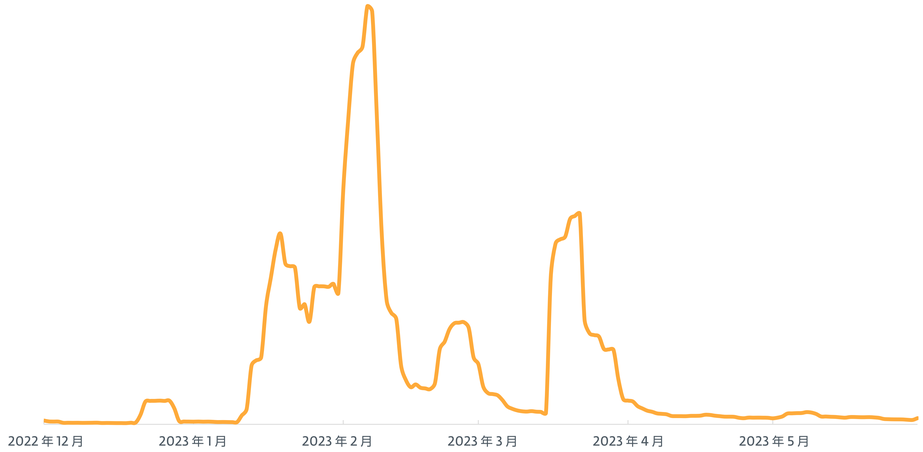
悪意のある OneNote ファイル：マクロに代わる新たな侵入方法

有名ないくつかのマルウェア系統は、拡散のメカニズムとして OneNote を利用する手法をテストしています。

OneNote ファイル（.one）のクリック可能なボタンのように見せかけて、ユーザーにその背後にある悪意のあるファイルやスクリプトを実行させる手法は、単純に見えるかもしれませんが、ESET のテレメトリでは、この手法は 2023 年上半期に多くのサイバー犯罪者によって悪用されており、攻撃者は別のマルウェアを拡散する目的で、武器化した Microsoft OneNote ファイルを配信しています。

2022 年 12 月、OneNote ファイルが攻撃に使用されていることが初めて検出されたときは、その検出数は数百件程度でした。それに比べると、2023 年 1 月から 5 月までの期間では、この手法を使用した攻撃数は劇的に増加し、合計で約 9 万件が検出されています。傾向を見ると、2 月と 3 月に最も多く使用されており、**Emotet**、**RedLine Stealer**、Qbot、Formbook、AsyncRAT、XWorm、Quasar、IcedID、さらに **BlackBasta ランサムウェア**などの多くのマルウェアを侵入させる手法の一部として、OneNote が悪用されるようになっていることがわかります。

サイバー犯罪者が、突如この新しい手法を採用したのはなぜでしょうか？これまでのいくつかの攻撃手段が行き詰まったために、この手法が試みられています。マイクロソフトはインターネットを介して送信される Office ファイルの VBA マクロを無効化し、サイバー犯罪者に長年悪用されてきた抜け穴を塞ぎました。攻撃者はその後、**ISO とパスワードで保護された ZIP ファイルを利用する**ことを試しました。これは、

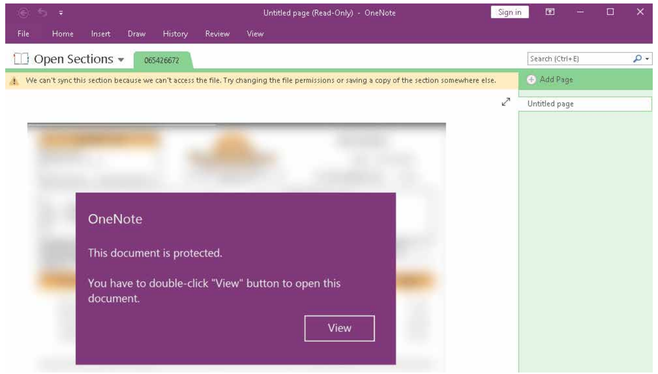


2023 年上半期に ESET のテレメトリで確認された**武器化された OneNote ファイルの検出傾向**

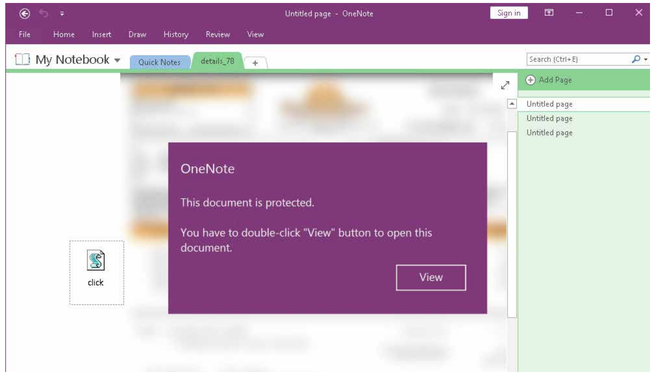
ESET のエキスパートの解説

VBA マクロと同じような対策が実施されるのなら、マルウェアを大規模に拡散するキャンペーンで OneNote ファイルを利用する手法は、大きな成果を得ることはできず、サイバー犯罪者は標的ユーザーのデバイスを侵害する新しい方法を再び探し始めることになるはずです。しかし、このロールアウトは限定されており、Web 版、Windows 10、macOS、およびモバイルプラットフォームでは厳格なセキュリティ設定が除外されていることもあり、武器化した OneNote ファイルを今後も悪用しようとするサイバー犯罪者が残る可能性もあるため、注意が必要です。

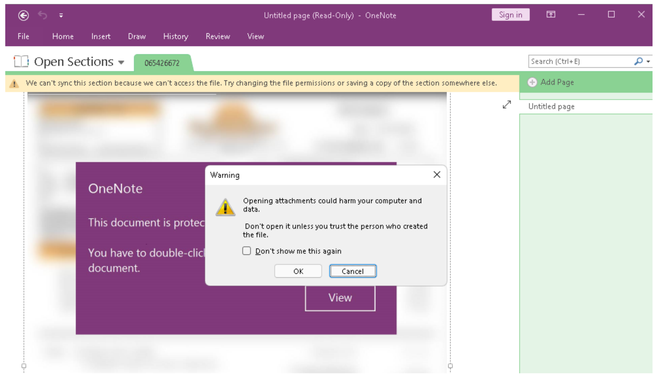
シニア検出エンジニア、Dušan Lacika



「保護されている」OneNote ノートブックで、ユーザーは「表示」ボタンをダブルクリックするように要求される。



通知の下に隠された悪意のある VBScript をクリックすると攻撃者のサーバーにリダイレクトされる。



埋め込みコンテンツの実行に関連するリスクをユーザーに知らせる OneNote の警告。

Mark of the Web（MOTW）の伝搬に関するバグを悪用するものでしたが、これらの問題もすぐに修正されたため、攻撃者は再び新しい手法を模索することになりました。

OneNote ファイルが攻撃者にとって魅力的であるのは、このアプリはデジタルノートブックとして機能する一方で、他のファイルを直接 OneNote ファイルに埋め込み、ダブルクリックするだけで開けるようになっているからです。この機能は、通常、スプレッドシートやその他の文書をドラッグアンドドロップしてメモを修正するために使用されていますが、攻撃者も、VBScript や HTA ファイルなどの悪意のあるコードを埋め込むためにこの機能を利用できることに気が付きました。

攻撃者は、悪意があることを隠すために、バックグラウンドで保護されているコンテンツがあるように見せかけ、「表示」ボタンをダブルクリックしてアクセスするように要求します。このボタンの背後には、悪意のあるスクリプトやファイルが隠されており、リモートサイトにアクセスして、別のマルウェアとユーザーに表示するおとり文書をダウンロードします。

この新しい OneNote による攻撃の脅威を緩和するために、管理者は `.one` ファイルに埋め込まれる特定の添付ファイルまたはすべての添付ファイルを無効にできます。

また、OneNote はデフォルトで警告を表示し、埋め込まれたコンテンツが悪意のある可能性があることを通知します。残念ながら、多くのユーザーはこれらの警告に注意を払うことなく、とにかくクリックして処理を進めようとします。このようなユーザーの習性は、Office 文書の「マクロの有効化」ボタンが長年にわたって攻撃者に悪用されてきた原因にもなっています。

マイクロソフトは、OneNote のセキュリティを強化するため、OneNote ファイルに埋め込まれる 120 種類のファイル拡張子を無効にすることを決定しました。また、表示する通知も更新され、「管理者が OneNote でこのファイルの種類を開く機能をブロックしました」と表示されるようになりました。管理者は、自社環境のユースケースに合わせる必要がある場合、Office ポリシーを通じてこれらの拡張機能を再び有効にできます。ただし、本稿執筆時点では、この変更は OneNote for Microsoft 365 と OneNote のリテール版にのみ適用され、Android、iOS、Win 10、および Web 版の OneNote には適用されていないため、注意が必要です。

推奨される対策

- Windows オペレーティングシステムの最新バージョンを使用すれば、`.one` ファイルで使用される 120 の潜在的に危険な拡張子がデフォルトで無効になります。
- 組織で OneNote ファイルを使用していない場合は、メールサーバーを設定して、`.one` ファイルが添付されたメールメッセージをブロックしてください。
- 厳格なルール設定が適用されていない OneNote バージョンを実行している場合、管理者は、Microsoft Office のグループポリシーテンプレートをインストールし、OneNote 文書に埋め込まれるファイルと特定の拡張子を無効化する必要があります。これまでの攻撃の傾向から、`.js`、`.exe`、`.com`、`.cmd`、`.scr`、`.ps1`、`.vbs`、`.lnk` のファイル拡張子をブロックするように指定することを推奨します。
- 信頼性の高い多層防御のセキュリティソリューションであれば、`.one` ファイルから派生する悪意のあるアクティビティをブロックできます。

メールの脅威 Web の脅威 詐欺 フィッシング

メールの脅威としてセクストーション（性的詐欺）が復活

この半年で、セクストーションに関する詐欺やフィッシングが増加しました。

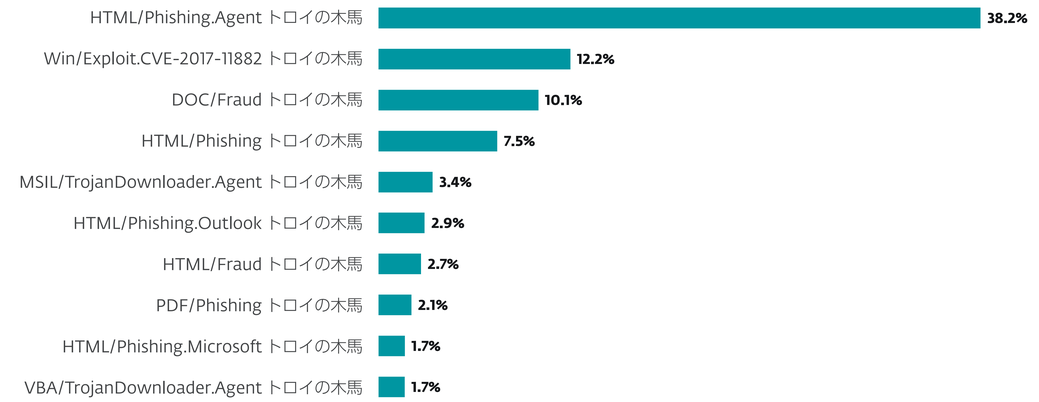
メールの脅威で、2023 年上半期に最も増加したのは、DOC/Fraud のトロイの木馬であり、検出数は 201% 増加しました。この攻撃は主に日本、スペイン、フランスに影響を与えています。これらの脅威は、主にメールの添付ファイルとして配信される、さまざまな詐欺の Microsoft Word 文書として検出されています。セクストーション詐欺が増加したことで、検出数は 2021 年以来の水準に戻っています。

セクストーション詐欺は、ユーザーのコンピューターにマルウェアをインストールし、ユーザーの性的なデータを収集しているという内容のメールを送信します。もちろん、これは虚偽であり、完全に無視できます。

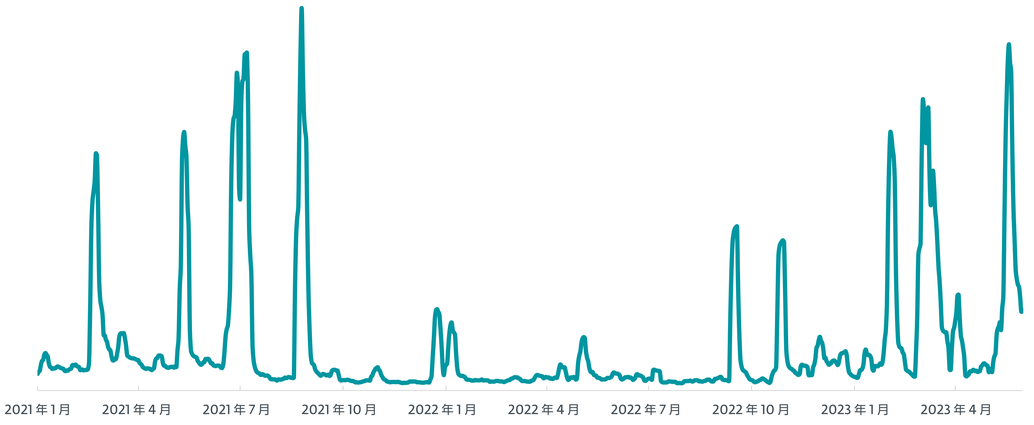
2023 年上半期にこのマルウェア系統で最も拡散した亜種は、DOC/Fraud.AAW です。このマルウェアは、攻撃者がユーザーのコンピューターのカメラで録画したと主張する性的なコンテンツを公開しない見返りとして、1,550 ドル相当のビットコインを支払うように要求していました。続いて上位にランクインした亜種は ATT と ADJ でした。これらも性的なコンテンツが含まれるデータを盗んだと主張する同様の詐欺です。

本稿執筆時点で、これらの恐喝で確認されたビットコインアドレスの 1 つは、**0.08 ビットコイン**（現在、2,000 ドル以上の価値）を集めましたが、その後空になっています。もう 1 つのビットコインアドレスは**全く空のまま**です。

利益をまったく得ていないケースがあるにもかかわらず、ESET のメールスキャナーが検出したメールの脅威の中で、この系統のマルウェアは 3 位にランクインしています。



2023 年上半期に検出された**メールの脅威トップ 10**



2021 年 1 月から 2023 年 5 月までの **DOC/Fraud の検出傾向**

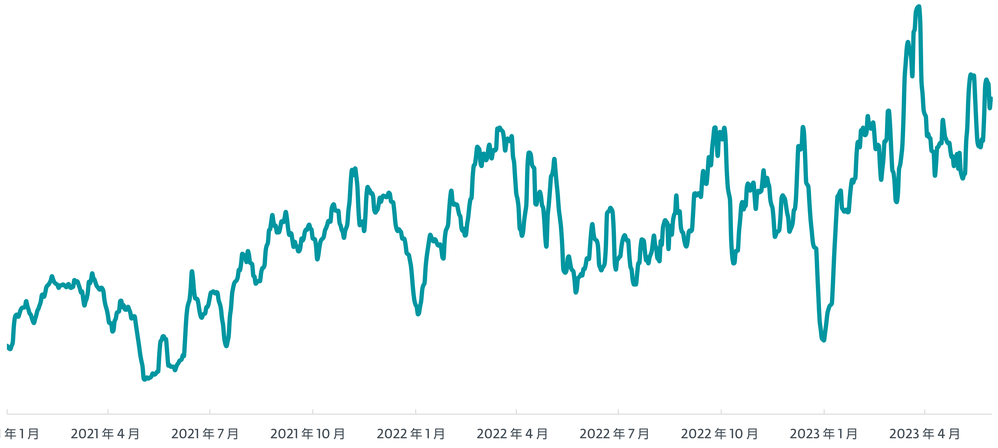
HTML/Phishing.Agent は、メールの脅威として引き続きトップになっており、2023 年上半期における検出数の 38% を占めました。この検出名は、メールの添付ファイルとして送信される悪意のある HTML 文書を示します。このような添付ファイルを Web ブラウザで開くと、通常、銀行や決済関連の Web サイトやソーシャルネットワークプロバイダーを装ったフィッシングサイトが開きます。本レポートの対象期間で、この脅威が多く検出された国は、日本、米国、英国でした。

このマルウェア系統の上位のすべての亜種で、検出数は減少していますが、2023 年 3 月 22 日に HTML/Phishing.Agent の検出数は、2021 年以降で最大のピークを記録しました。

このピークは、この日に初めて登場した DTS と BRZ の 2 つの亜種によってもたらされました。

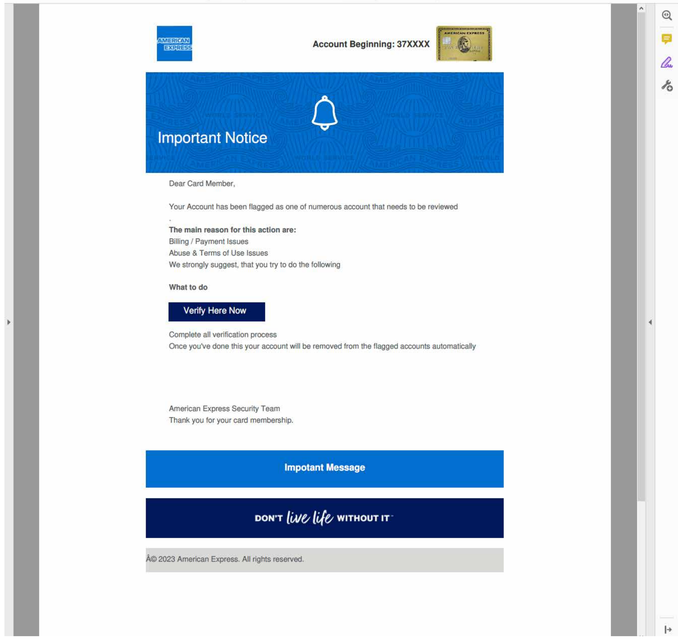
HTML/Phishing.Agent.DTS は、本文のないメールと `RemittanceAdvice.html` と呼ばれる添付ファイルを使用して、Microsoft Outlook の認証情報を窃取するフィッシングの脅威です。この HTML ファイルをブラウザで開くと、適切にレイアウトされていない Outlook のログインフォームが表示されます。

HTML/Phishing.Agent.BRZ は、`DepositRemittance.html` というメールの添付ファイルを使用して拡散する Microsoft 365 のフィッシングの脅威です。この添付ファイルをブラウザで開くと、ユーザー名があらかじめ入力された Office 365 のログインページが表示されます。



HTML/Phishing.Agent の検出傾向 2021 年 1 月から 2023 年 5 月まで

HTML/Phishing.Outlook は、製品特化型のフィッシング脅威であり、メールの脅威のトップ 10 に再びランクインしました。この脅威は、半年前に比べて 30% 増加し、今回は 6 位になりました。最も流行している亜種は AQ で、`Remittance_230323.htm` と呼ばれる添付ファイルを使用して拡散します。この添付ファイルをブラウザで開くと、メールの受信者と同じユーザー名が事前に入力されます。このフォームに入力した認証情報は、正規のサイトですが、侵害されているサイト（ギリシャ旅行の広告サイト）から流出します。



フィッシングで PDF の添付ファイルが悪用される脅威は、PDF/Phishing として追跡されます。この脅威は 88% の大幅な増加となり、メールの脅威の 8 位になりました。2023 年上半期で上位にランキングした亜種の 1 つは、PDF 文書内のリンクからイタリア語のログインページに移動し、アカウントの詳細の入力を求めるものでした。もう 1 つの上位の亜種は、American Express からの通知を装った PDF であり、フィッシングサイトにリンクする「今すぐ確認」ボタンが含まれています。

フィッシングの脅威は Web 脅威の増加にもつながりました。2023 年上半期にブロックされた Web の脅威の数は、前半期に比べて 31% 増加しました。この増加は、ブロックされたフィッシングの脅威が急増して 125% となったことも一因ですが、ブロックされた詐欺が最大の要因となっています。

2023 年上半期の Web 脅威のデータでは、共通のテーマがいくつか見られました。その中の 1 つは、サイバー攻撃者が、正規の Web サイトの広告で使用されるリダイレクトチェーンに悪意のあるドメインを組み入れる手法です。このようなドメインの Web ページは、正規の操作をそのまま行うこともありますが、詐欺、不正な広告、フィッシング、その他の不審なコンテンツを、Web サイトにアクセスしたユーザーに仕掛ける場合もあります。

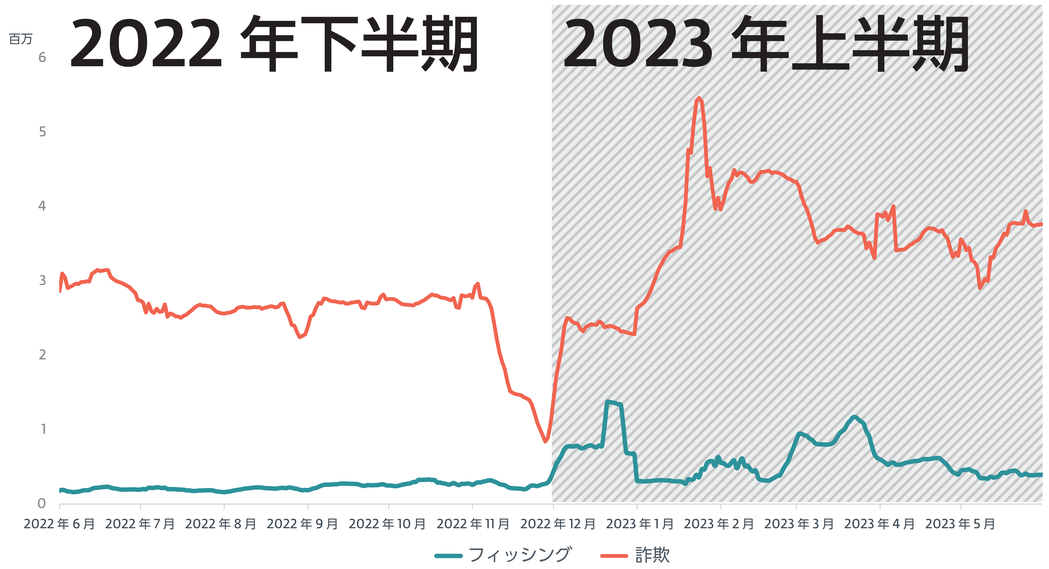
5,700 万以上のブロックを記録している悪意のあるドメインの 1 つは、`pogothere[.]xyz` です。このドメインは本書を公開した時点でも稼働しています。このドメインは、ソフトウェアやゲームのクラック版を提供する不審なサイトの広告リダイレクトチェーンに組み込まれている場合があります。

もう 1 つの例は、`123w0w[.]com` です。このドメインは、YouTube のビデオプレーヤーを装ったランディングページにユーザーを誘導し、ビデオを再生するためのプラグインのダウンロードするように要求します。

`viixikup[.]com` も悪意のあるドメインの 1 つです。通常このドメインは、サイトにアクセスしたユーザーに、押し付けがましい広告や詐欺商品を表示する、望ましくないサイトや有害なサイトにリダイレクトします。

最後のドメインは、`asxcnx[.]com` です。このドメインは、**技術サポートの詐欺サイト**と、Netflix のサイトを偽装してクレジットカードなどの情報を窃取するページにリダイレクトします。

ドイツ語の Netflix になりすます `asxcnx[.]com` のランディングページ



2023 年上半期の**フィッシングと詐欺のブロック数の傾向**、7 日移動平均線

エクスプロイト 攻撃手法 SQL 攻撃

Microsoft SQL Server：ブルートフォース攻撃の魅力的なターゲットへ

MSSQL のパスワード推測攻撃は急増し、Log4Shell の攻撃は特定の地域で増加し続けています。

Microsoft SQL（MSSQL）サーバーは、ネットワークに最初にアクセスする手法としてサイバー犯罪者から注目を再び集めています。ESET のテレメトリデータによると、MSSQL に対するパスワード推測攻撃をブロックした件数は、2022 年下半期には 9 億 4,000 万件でしたが、2023 年上半期には 17 億件と増加傾向にあります。この攻撃が拡大している背景には、リモートデスクトッププロトコル（RDP）へのパスワード推測攻撃が 179 億から 158 億件へ、サーバーメッセージブロック（SMB）プロトコルのパスワード推測攻撃が 4 億 6900 万件から 3 億 9900 万件に減少するなど、広く利用されている他のサービスに対するパスワード推測攻撃が減少していることがあります。

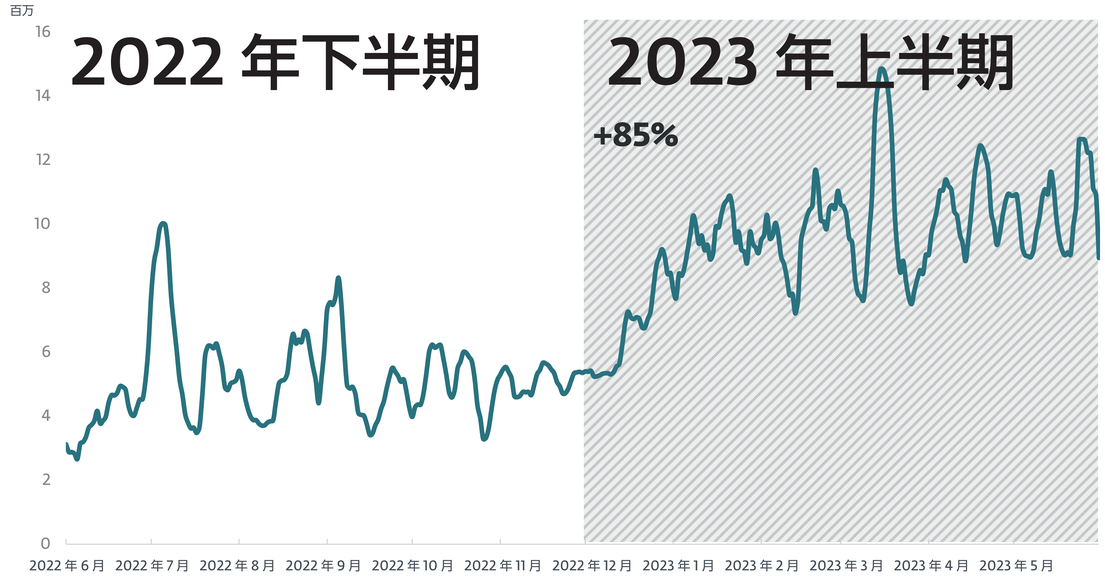
2023 年上半期に、サイバー攻撃者によるネットワーク侵入の手法で最も広く利用された手法は、過去と同じようにパスワード推測であり、次に多かったのは Log4Shell の脆弱性の悪用でした。

2022 年下半期と比較して、外部ネットワークからの攻撃手法の上位リストに変化はありませんでしたが、パスワード推測のカテゴリにおける MSSQL 攻撃の増加傾向は注意が必要であり、詳細に検証する必要があります。

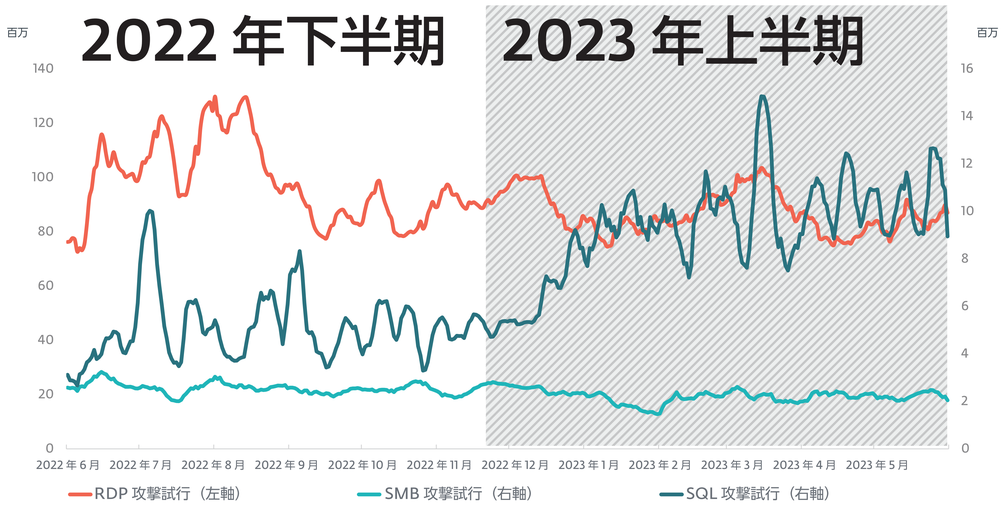
MSSQL へのブルートフォース攻撃

MSSQL は企業に人気のあるリレーショナルデータベース管理システムです。このサーバーがインターネットからアクセス可能な場合、デフォルトではポート 1433 で TCP 接続を受信するため、このポートはブルートフォース攻撃の格好の標的となっています。当然ながら、正規のデータベースユーザーにデータへのアクセスを許可する前には、認証しなければなりません。サイバー攻撃者による侵入を防止するために、すべてのユーザーが強力で一意のパスワードを使用しなければなりませんが、セキュリティ対策が十分ではなく、外部に公開されている MSSQL サービスを見つけ出そうとするサイバー犯罪者の執念が勝る場合もあります。

2023 年 4 月 17 日、AhnLab の研究者が[レポートを発行]し、Trigona ランサムウェアについて公開しました。このランサムウェアは、有効な認証情報を推測して MSSQL サーバーにアクセスします（ESET セキュリティ製品では Win32/Filecoder.OLC として検出されます）。



MSSQL 攻撃試行の検出傾向、7 日移動平均線



RDP、SMB、SQL パスワード推測試行の傾向、7 日移動平均線

ESET のデータでは、MSSQL 攻撃の絶対数は過去 2 年半の間で 84% 増加しています。

マイクロソフトが、**マクロが有効なファイルを開くとき**のセキュリティポリシーを強化したこと、そして、2023 年からは**危険な拡張子のファイルが使用されている OneNote ファイル**のセキュリティポリシーを強化したことから、サイバー犯罪者は、MSSQL への攻撃やその他の侵入方法に注力している可能性があります。

2023 年上半期における MSSQL ブルートフォース攻撃の大半は、トルコ、米国、ポーランドのサービスを対象としていました。IP アドレスを基準とする地理的なデータは、利用されている VPN、レンタルサーバー、プロキシサービスの影響を受けることを考慮しなければなりません。

SQL 攻撃が増加しているにも関わらず、RDP ブルートフォース攻撃が常にパスワード推測攻撃の大部分を占めており、ESET のテレメトリデータでは 1 日平均 8,700 万回の攻撃が行われています。ただし、RDP 攻撃は 2022 年から減少傾向にあります。SMB 攻撃も減少する傾向にあります。

ESET のエキスパートの解説

MSSQL に対するブルートフォース攻撃の増加していることから、データベース管理者はデータベースエンジンをセットアップするときには、混合モード認証よりも、**Windows 認証モード**のほうがセキュリティを強化できることを再認識する必要があります。Windows 認証モードでは、SQL Server の認証は無効になり、データベースユーザーは Windows のユーザーアカウントで接続するため、ブルートフォース攻撃を効果的に防止する**アカウントロックアウトポリシー**によって保護できます。

混合モードを使用しなければならない場合は、強度の高い複雑なパスワードを使用していることを確認し、可能であればデータベースをファイアウォールや VPN の内側に配置してください。

ESET シニア検出エンジニア、Ladislav Janko

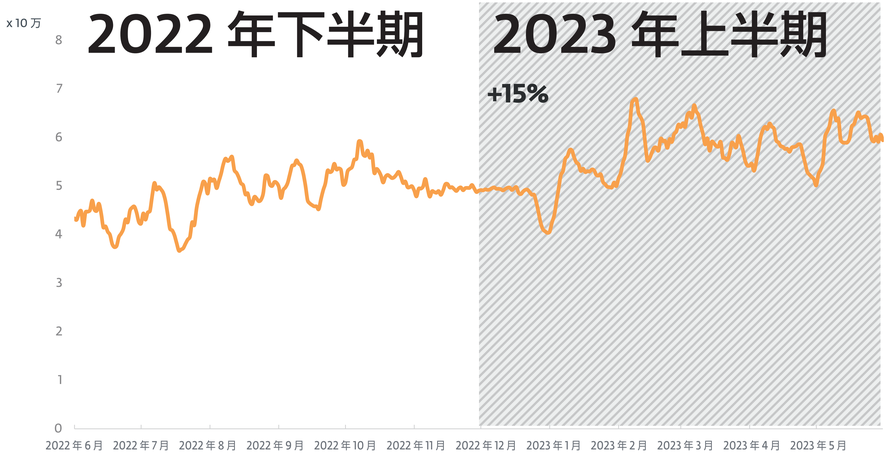
Log4Shell

Log4Shell の脆弱性は、外部からの侵入方法として引き続き 2 位にランクインしています。Log4Shell のパッチは 2021 年 12 月から提供されていますが、この脆弱性を悪用した攻撃試行の回数は 2023 年上半期に 16% 増加しました。

2022 年下半期と比較すると、多くの国で攻撃件数が増加していますが、ポーランドの攻撃件数は爆発的に増加しており、9 月中旬以降、1 日の平均攻撃件数が 3 倍以上に増加しています。

2023 年 2 月 7 日に Log4Shell を悪用する攻撃がピークに達した 2 日後に、米国 CISA（サイバーセキュリティインフラセキュリティ庁）は、北朝鮮とつながりのあるランサムウェア組織が韓国と米国の医療システムを標的にしていることを**警告しました**。被害者のネットワークにアクセスするために使われる手法の 1 つとして Log4Shell のエクスプロイトが使用されています。AhnLab の研究者は、北朝鮮と関連があるグループである Lazarus もこの脆弱性を攻撃していることを**報告しています**。北朝鮮は、Log4Shell のエクスプロイトを悪用する攻撃者の温床となっていると考えられます。

Log4Shell が継続的かつ頻繁に悪用されていることから、CISA は 2023 年 5 月 1 日、CVE-2021-44228 の脆弱性が不完全な形で修正されていることが明らかになった後に、CVE-2021-45046 を「実際に悪用が確認された脆弱性のリスト」に**追加しています**。Log4Shell を悪用する攻撃試行に関する ESET のデータでは、これらの CVE は区別されていません。ネットワークトラフィックが暗号化されていれば、調査して追加の攻撃を特定することはできません。



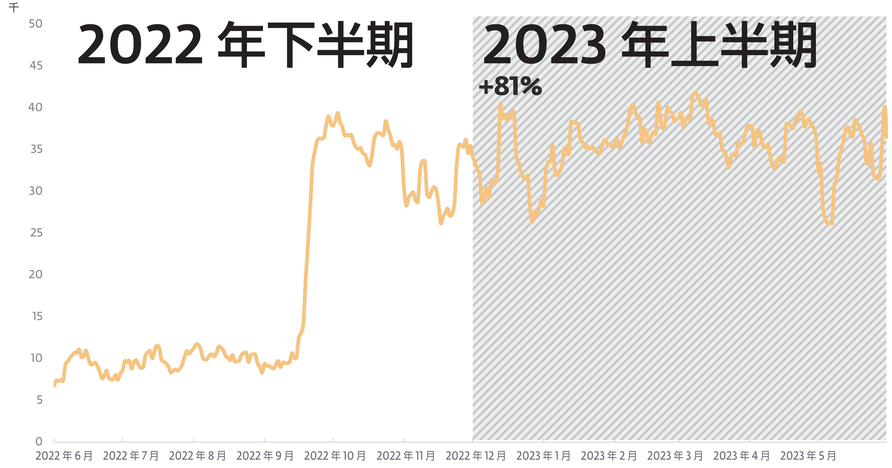
Log4Shell 攻撃試行の検出傾向、7 日間移動平均線

Log4j ライブラリの脆弱なバージョンを使用している場合、攻撃者がトラフィックを暗号化せずにこの脆弱性を攻撃することを期待せず、脆弱性が修正されたバージョンに速やかに更新してください。

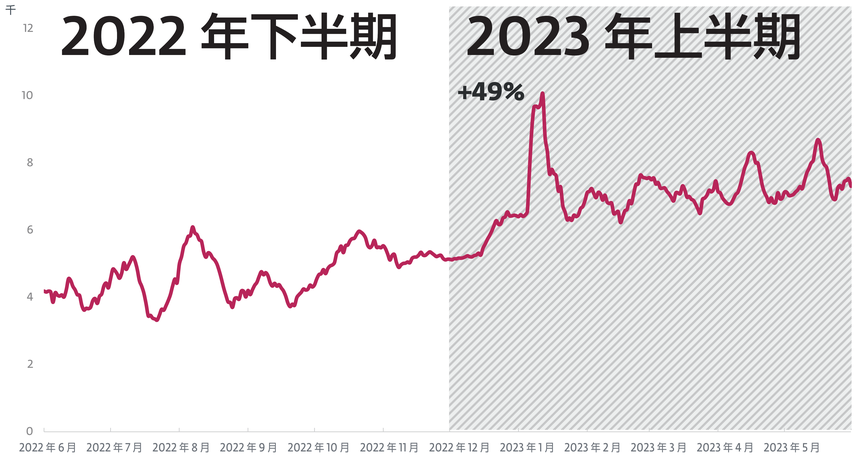
Spring4Shell

Spring4Shell の攻撃は 2022 年 5 月以前のレベルには戻っていないものの、2023 年上半期では着実に増加しており、前年同期と比較して 50% 増加しています。2023 年 1 月 6 日にこの攻撃は急増しましたが、これは主に米国、英国、中国での検出が増加したことが原因でした。

では、どのようなサイバー攻撃者が Spring4Shell エクスプロイトをツールキットとして利用しているのでしょうか？2022 年 12 月、Fortinet の研究者が Zerobot と呼ばれる新しいボットネットを分析した結果を発表しました。Log4Shell エクスプロイトは Zerobot が利用している 31 個のエクスプロイトのリストには含まれていませんが、このレポートでは、Spring4Shell エクスプロイトについて詳しく説明されています。



ポーランドにおける Log4Shell 攻撃試行の検出傾向、7 日移動平均線



Spring4Shell 攻撃試行の検出傾向、7 日移動平均

情報窃取ツール サービスとしてのマルウェア

RedLine Stealer：マルウェアを配信するビジネス

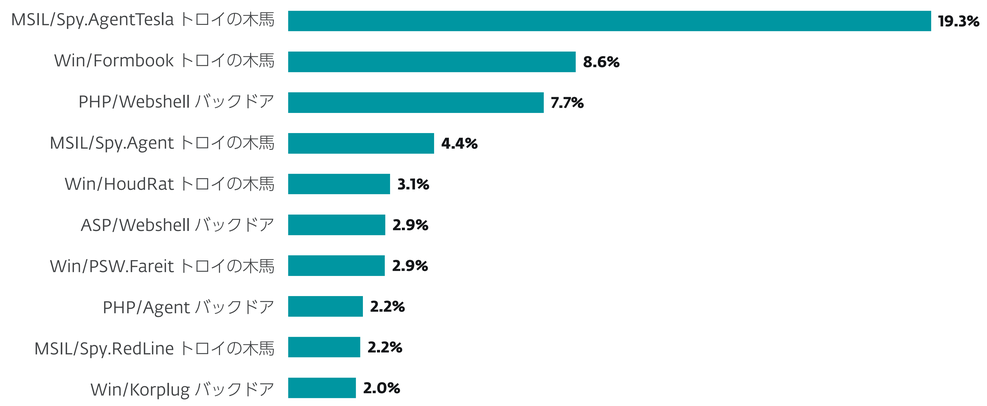
最近、ESET Research は、悪名高い情報窃取ツール「RedLine」の活動を妨害することに成功しました。

RedLine Stealer は、Proofpoint によって 2020 年に検出されてから、その悪名を世に知らしめてきました。この情報窃取型ツールは、ESET 製品では MSIL/Spy.RedLine として検出されますが、地下フォーラムで簡単に入手でき、2 ～ 3 週間ごとにニュースで報道されています。2023 年 4 月、ESET の研究者が Flare Systems と共同で RedLine Stealer を調査し、その活動の一部を一時的に妨害することに成功しました。

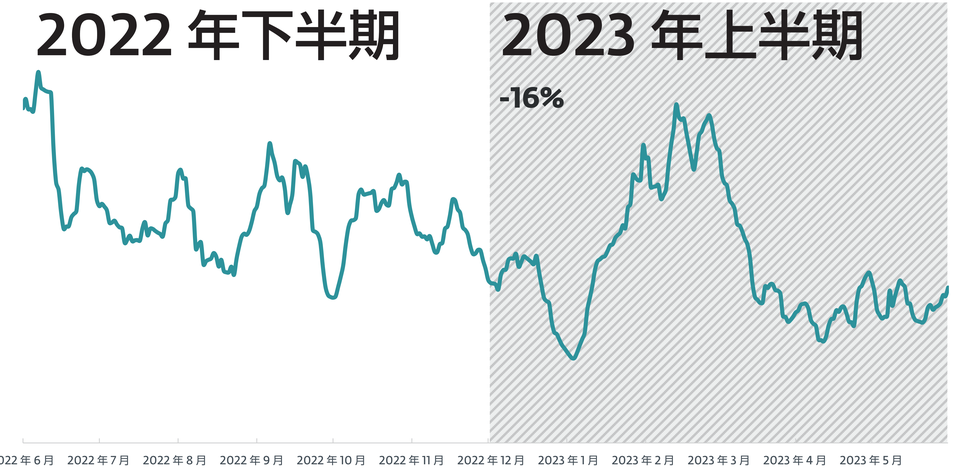
多くのサイバー攻撃者は、マルウェアを持続的なビジネスとして展開できる可能性があることを以前から認識していました。マルウェアを展開するサービス（MaaS）というビジネスモデルが誕生することは必然だったのかもしれません。サイバー攻撃者は、このビジネスモデルによってマルウェアを、手数料を取って、定期的な収益をもたらす商品へと変えたのです。ESET のテレメトリデータを見ると、サイバー犯罪者の間で MaaS が普及していることが一目瞭然です。2023 年の上半期には、ESET の情報窃取型マルウェアの上位 10 の統計に、MSIL/Spy.AgentTesla、Win/Formbook、および MSIL/Spy.Redline の 3 つの系統の MaaS が入っています。これらの 3 つの系統の検出数は数十万件に上り、情報窃取型マルウェアのトップ 10 の検出数の半数以上を占めています。

MaaS とは、通常、サイバー犯罪者がレンタルしている既製のマルウェアソリューションです。MaaS を利用する犯罪者は、料金を支払えば、マルウェアだけでなく、ボットネットや MaaS の作成者が提供しているカスタマーサービスも利用できることが多くあります。MaaS により、高度なソリューションを開発できない犯罪者でも、簡単にマルウェアを利用できるようになっており、悪意のあるキャンペーンが蔓延する結果を招いています。

最近、MaaS の亜種である RedLine Stealer に注目が集まっています。RedLine Stealer は、2020 年に特定されてから、ESET のテレメトリの情報窃取型マルウェア系統の中で、最も拡散しています。MSIL/Spy.RedLine は、2022 年下半期に初めて情報窃取型マルウェアの検出数のトップ 10 にランク



2023 年上半期の**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検出数に占める割合）



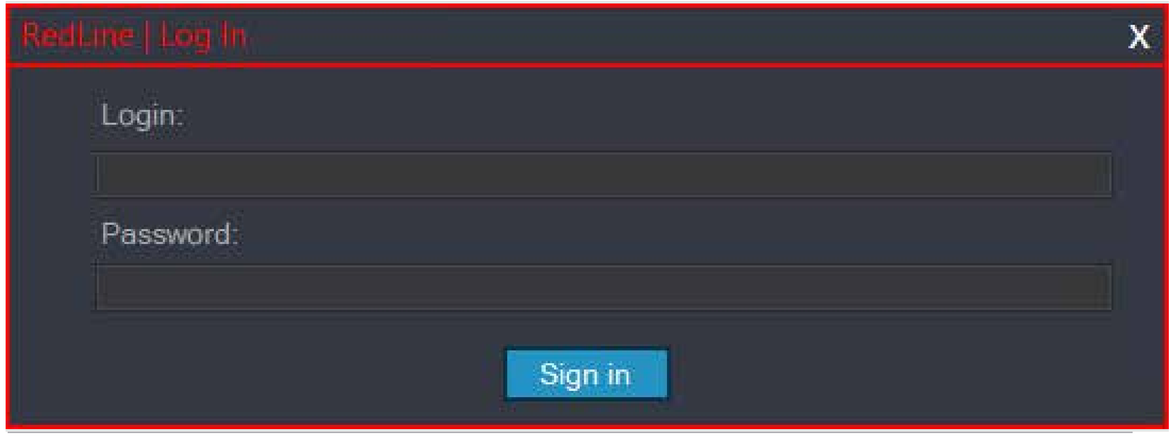
2022 年下半期～ 2023 年上半期の **RedLine Stealer の検出傾向**、7 日移動平均線

インし、2023 年上半期には総検出数は減少しましたが、9 位にランクインしました。

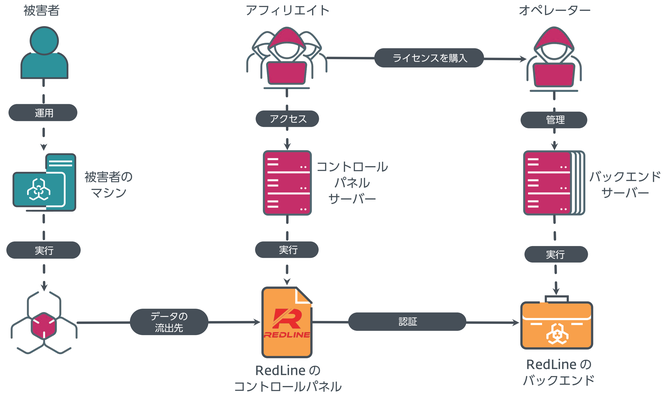
このマルウェアは、地下フォーラムや Telegram チャンネルから購入できます。比較的安価な月額利用料（月額 150 ドルと報告されている）を支払えば、さまざまな情報を盗み出すことが可能です。パスワード、暗号通貨のウォレット情報、さらに Steam や Discord のセーブデータまで、RedLine のオペレーターは、犯罪者の邪悪なニーズを満足させることを目指しています。

RedLine に利用料を支払っているサイバー犯罪者は「アフィリエイト」と呼ばれ、このマルウェアのコントロールパネルを利用して、自分のキャンペーンを管理できます。RedLine のコントロールパネルは GUI を完備しており、マルウェアを簡単に展開できる仕組みになっています。攻撃を成功させるために、このコントロールパネルはこのスパイウェアのバックエンドサーバーと通信します。このバックエンドサーバーは、RedLine のオペレーターが管理しています。

アフィリエイト（サービスの利用者）は、完成しているソリューションを利用でき、大規模なキャンペーンの一部として簡単に取り込んで利用することも可能です。そのため、RedLine マルウェアはいくつかの大規模なキャンペーンでも使用されています。2023 年上半期だけを見ても、生成 AI のブームに便乗し、ChatGPT や Google Bard の無料ダウンロードを装っており、乗っ取った Facebook ビジネスのページの悪意のある広告を介して拡散しています。CronUp は、広告を悪用する別の一連の攻撃を特定しています。RedLine は Google Ads で情報窃取型マルウェアである Ursnif と一緒に配信されます。



RedLine パネルのログインプロンプト



RedLine の動作の概要

Cobalt Strike とランサムウェアを配信する場合もあります。Avast が発見したように、この情報窃取型マルウェアは、Adobe Acrobat Sign を悪用した高度な標的型フィッシングキャンペーンでも使用されています。署名サービスを装った添付ファイル付きのメールが送信されており、添付ファイルの中には、RedLine が含まれる ZIP ファイルを最終的にドロップするリンクが設定されていました。

Flare Systems が Botconf 2023 で ESET と共同で行ったプレゼンテーションでは、キャンペーンと同様に RedLine Stealer の配信方法が多岐にわたっていることを解説されました。先に説明した Google Ads やスピアフィッシングに加え、このスパイウェアは YouTube 動画のリンクや広告、コメント、そして公開されている情報窃取型マルウェアのログサンプルからも拡散しています。このマルウェアは、Windows 11 のアップグレード、ビデオゲームやその他のソフトウェアの

情報窃取型マルウェアのログ

情報窃取型マルウェアのログとは、これらのマルウェアが窃取および収集した大規模なデータであり、通常はクラウドでホストされます。これらのログには、主にユーザーの認証情報が含まれますが、クッキー、文書、銀行口座の支払い詳細など、他の機密情報も含まれることがあります。これらのログは、地下フォーラムやマーケットプレイスで販売され流通しています。

クラック版、モバイルアプリのクローン、Visual Studio などの一般的なアプリケーションなどを偽装して被害者のシステムに侵入します。

4 月に ESET の研究者は、Flare Systems の研究者との共同調査の結果、RedLine コントロールパネルのデッドドロップリゾルバとして使用されている複数の GitHub リポジトリを発見したことを Twitter で公開しました。ESET は合計 4 つの以下のリポジトリを特定し、GitHub の協力の下ですべてのリポジトリをテイクダウンしました。

```
github[.]com/lermontovainessa/Hub
github[.]com/arkadi20233/hub
github[.]com/ivan123iii78/hub
github[.]com/MTDSup/updateResolver
```

コントロールパネルはデッドドロップリゾルバに保存された情報を使用して RedLine のバックエンドサーバーにアクセスします。フォールバックのためのチャネルが存在していなかったため、リポジトリを削除することで、当時使用されていた RedLine コントロールパネルの認証方法が利用できなくなりました。ESET の活動では、MaaS のバックエンドを停止させることはできませんでしたが、RedLine のオペレーターは新しいコントロールパネルのバージョンを配信せざるを得なくなり、一時的に活動を混乱させることができました。

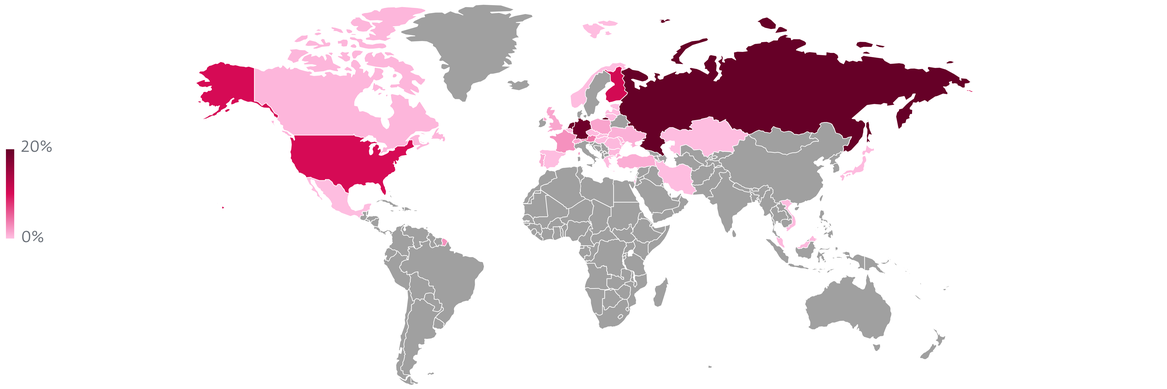
GitHub リポジトリの他に、ESET の研究者は RedLine コントロールパネルの署名に使用されたコード署名証明書も特定しました。これらの証明書は、RAIL AND CIVILS LTD および AMERT, LLC に割り当てていましたが、ESET が報告した後で失効されています。

2022 年 12 月から 2023 年 3 月までの ESET のテレメトリデータを解析した結果、RedLine のコントロールパネルは主にロシア、ドイツ、オランダでホストされていることがわかりました。この 3 か国はそれぞれ、RedLine のすべての C&C の 20% 近くをホストしていました。ESET はまた、米国とフィンランドにある IP アドレスに、このスパイウェアのコントロールパネルが多く存在していることも特定しました。これらの両国で全体の約 10% をホストしていました。

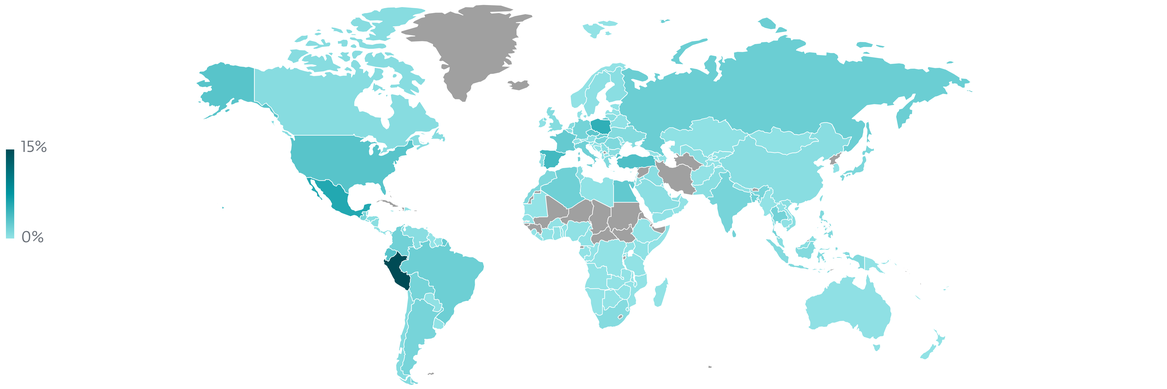
コントロールパネルをホストしている国と、攻撃を受けている国は大きく異なっており、同期間に RedLine の攻撃を最も受けた国は、ペルー（15%）、メキシコ（6%）、ポーランド（5%）でした。

ESET の研究者は、デッドドロップリゾルバをリポジトリと一緒に削除し、RedLine の活動を混乱させることに成功しましたが、この情報窃取型マルウェアの活動が終わったわけではありません。RedLine が突然姿を消したとしても、多くサイバー攻撃者がその代役を務めようとするでしょう。

実際、RedLine のライバルがその地位を奪おうとする動きもみられます。2022 年に META という名前のマルウェアがサイバー犯罪フォーラムで公開され、RedLine よりも優れた製品であると主張しています。サイバー攻撃者が、RedLine から META に乗り換えるかどうかはわかりません。最新の統計でも、META のシェアは大きくは伸びていません。



2022 年 12 月～ 2023 年 3 月までの RedLine パネルの地理的分布



2022 年 12 月～ 2023 年 3 月までの RedLine パネルの地理的分布

macOS サプライチェーン攻撃

macOS が相互に関連する 2 つのサプライチェーン攻撃を受けた初めてのケース

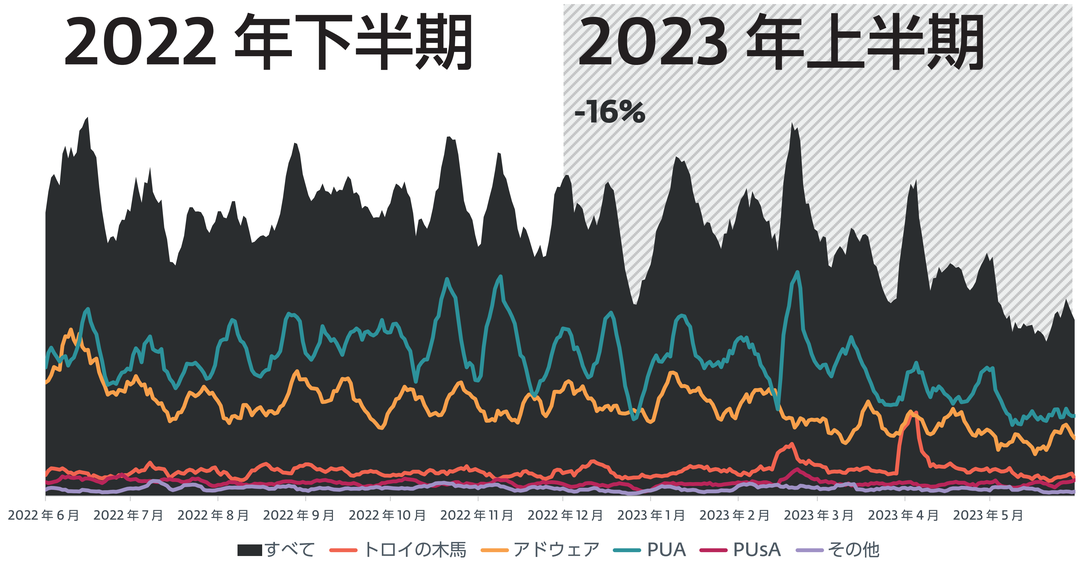
相互に関連する 2 つのサプライチェーン攻撃が初めて実行され、macOS で検出された脅威が急増しました。この攻撃によって、多くの macOS デバイスが侵害されました。

サプライチェーン攻撃とは、サイバー攻撃者が正規のソフトウェアに悪意のあるコードを追加し、そのソフトウェアが正規のルートでユーザーに配信される仕組みであり、サイバーセキュリティの世界で大きな問題となっています。2023 年 3 月、Windows と macOS プラットフォームが、相互に関連する 2 つのサプライチェーン攻撃の影響を受けました。2 つのサプライチェーン攻撃が連携するケースが確認されたのは、今回が初めてです。このサプライチェーン攻撃では、悪名高い Lazarus グループが最初に X_TRADER ソフトウェアに悪意のあるコードを挿入しています。これにより、Lazarus による 3CX への侵入が可能となり、このビジネス用電話システムである 3CX と顧客のセキュリティが侵害されました。

macOS のエコシステムは、その性質と市場シェアが比較的小さいことから、Windows と比較するとマルウェア攻撃を受けることは通常少なくなっています。ESET のテレメトリによると、macOS に対する脅威の全体的な検出数は徐々に減少する傾向にあり、このプラットフォームで検出が多かった脅威は、PUA（望ましくないアプリケーション）でした。2023 年上半期には、PUA は macOS で検出されたすべての脅威の検出件数の 49.3% を占めました。実際、3 月中旬に ESET テレメトリで確認されたスパイクの 1 つは、検出対象の PUA が拡大され、いくつかのアプリケーションが追加されたときに発生しています。

そのため、サプライチェーン攻撃が macOS で検出される脅威の傾向に明らかに影響するのは異例と言えます。このサプライチェーン攻撃は、3 月末から 4 月上旬にかけて発生しました。ESET のテレメトリにおいて、トロイの木馬の検出数が 2023 年上半期に 16.8% 増加し、macOS の全検出数の 11.2% を占めた原因の 1 つも、この攻撃です。

3 月下旬、3CX が開発した Windows と macOS のアプリケーションの両方に悪意のあるコードが含まれていることが明らかになりました。3CX は、従来の電話回線の代わりに VoIP（Voice over Internet Protocol）を利用して通話できる電話システムを提供しており、この機能は 3CX アプリからも利用

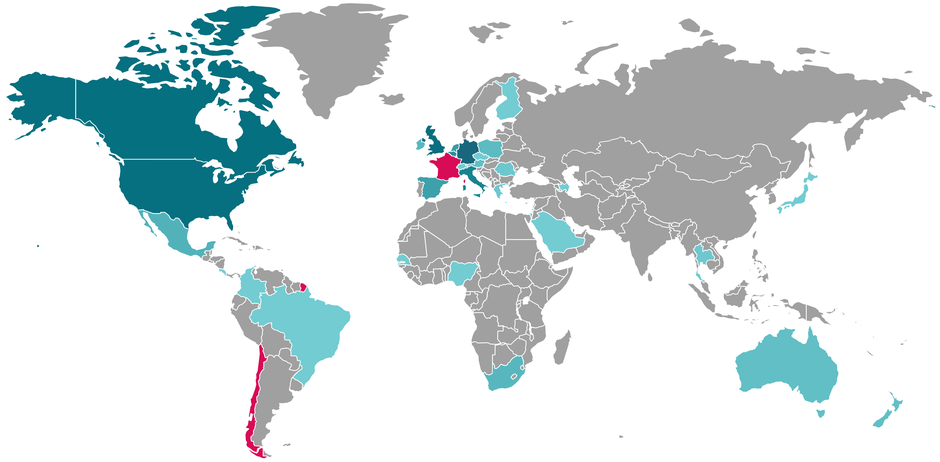


2023 年上半期の **macOS における脅威の検出傾向**、7 日移動平均線

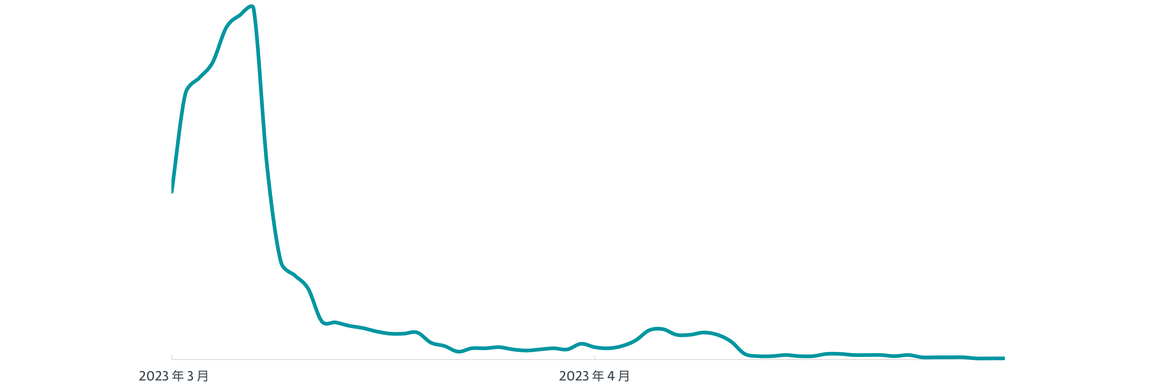
できます。これらのアプリケーションに悪意のあるコードが追加されたことで、攻撃者は侵害されたアプリケーションがインストールされたすべてのコンピューターを乗っ取ることが可能になりました。3CX アプリに有害なコードが追加されたのは 3CX の責任ではなく、ソフトウェアの開発チェーンが侵害されて、サプライチェーン攻撃につながったことがすぐに明らかになりました。

macOS を実行している影響を受けるシステムに関する詳細は、**Twitter** のスレッドと Patrick Wardle 氏の**ブログ**で詳細に解説されています。ESET が、トロイの木馬として動作するように仕込まれた macOS 向けの 3CX アプリケーションを分析したところ（ESET 製品では OSX/NukeSped.P として検出されます）、1 月下旬にデジタル署名されていたことが判明しましたが、2023 年 2 月 14 日まで、ESET のテレメトリではこの悪意のあるアプリケーションの存在は確認されていませんでした。その後、3 月末に発生したスパイクでは、ESET のテレメトリで主にドイツ、英国、フランス、米国、カナダにおいて、侵害された macOS 向けの 3CX アプリの検出数が著しく増加していることが記録されました。

このサプライチェーン攻撃は、3CX の特定の顧客にマルウェアを配信することを目的に、外部のサイバー攻撃者によって組織的に実行されています。ESET Research は、他のセキュリティ研究者と同じように、この攻撃は、北朝鮮とつながりがあり、高度な技術力を有する Lazarus グループによって実施されていることを確信しています。



ESET が検出した macOS 向けの 3CX アプリのヒートマップ。Lazarus が提供しているセカンドステージマルウェアの検出結果は赤で示しています。



OSX/NukeSped.P の検出数、7 日移動平均線

Lazarus は、トロイの木馬化された macOS 向けのアプリを使用して、3CX の特定の顧客を標的として別のマルウェアも配信していますが、ESET のテレメトリでは、このマルウェアはフランスとチリのわずかなケースで確認されているだけです。ESET 製品はこの別のマルウェアを OSX/NukeSped.Q として検出しています。macOS に対してセカンドステージのペイロードが実行されている兆候は、2 月の時点で ESET のテレメトリにすでに存在していましたが、ESET の研究者は、悪意のある特性を示す検体やメタデータを所有していませんでした。Windows と macOS の両方のセカンドステージのマルウェアは、暗号通貨企業を標的にしていたと**考えられます**。

ESET の研究者が、このサプライチェーン攻撃を Lazarus によるものと断定する調査結果を発表したのと同じ日に、3CX とこのセキュリティ侵害のインシデント対応を担当した企業は、3CX のサプライチェーン攻撃が、別のサプライチェーン攻撃によって引き起こされていたことを**公表しました**。今回のケースは、相互に関連する 2 つのサプライチェーン攻撃が行われ、ある攻撃が別の攻撃を助長する仕組みが記録された初めての事例となりました。

最初のサプライチェーン攻撃では、Trading Technologies 社が標的となり、X_TRADER ソフトウェアの古い廃止済みのバージョン r7.17.90p608 に悪意のあるコードが追加されましたが、3CX 社の従業員が個人のマシンにこのバー

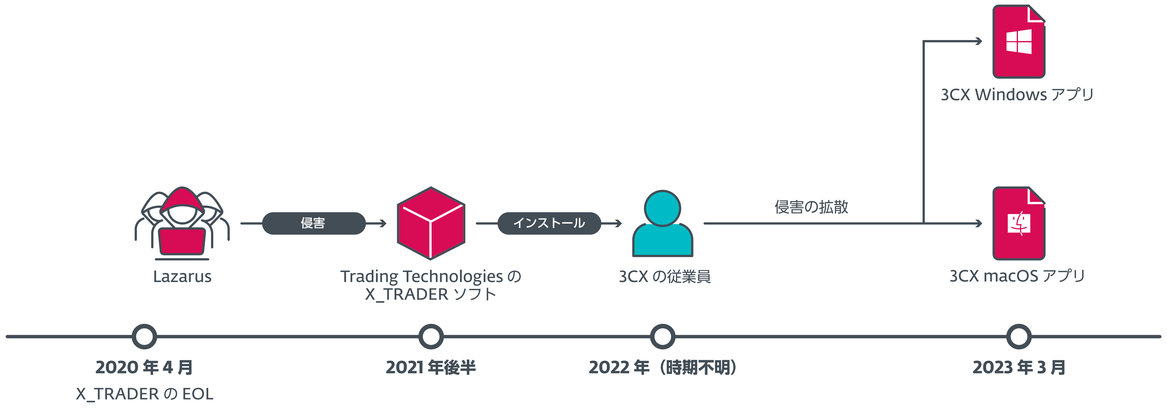
Lazarus グループ：

Lazarus は、少なくとも 2009 年から活動しており、2016 年の **Sony Pictures Entertainment のハッキング**、数千万ドルを盗み出した**サイバー攻撃**、2017 年の **WannaCryptor**（別名：WannaCry）の大規模なインシデントなど、注目度の高いインシデントの首謀者であり、**韓国の公共インフラ**や重要インフラに対する破壊的な攻撃を行ってきました。ESET Research が新たな **Lazarus の Linux に対するペイロード**を発見したことで、このサイバー攻撃者と 3CX の侵害が関連していることがさらに強力に裏付けられました。

ジョンの X_TRADER をインストールしています。Trading Technologies は、暗号通貨取引など、さまざまな投資分野の電子取引を可能にする幅広い製品とサービスを提供しています。

X_TRADER は、金融機関やプロのトレーダーに高度なトレーディング機能とツールを提供していました。Trading Technologies が 2020 年 4 月に X_TRADER のすべてのサポートを停止し、製品の EOL を **2018 年 9 月**に発表していたにもかかわらず、3CX の従業員は、2022 年のある時期に悪意のあるコードが追加されたバージョンをインストールしました。ESET のテレメトリでは、2022 年に悪意のある X_TRADER インストーラの 2 つのインスタンスが、1 つは 8 月に英国で、もう 1 つは 12 月に米国で検出されています。

WIZVERA VeraPort（Lazarus が関与）から **NotPetya**、**SolarWinds**、そして最近発生した 3CX/Trading Technologies のインシデントなど注目を集めた一連のサプライチェーン攻撃は、近年、個別のコンピューターや企業ネットワークといった従来の枠を超えて脅威が拡大していることを示しています。ソフトウェアを開発および配信する仕組みが複雑化しており、多くの組織がサードパーティのソフトウェアやハードウェアプロバイダーの製品やサービスを多用するようになっています。このため、サイバー攻撃者がこのような信頼関係を悪用し、検出を困難にして、既存の防御メカニズムを回避しています。今回の 3CX のサプライチェーン攻撃は、Windows でも Mac でも、あらゆるプラットフォームのセキュリティがこのような手法によって侵害される恐れがあることを示しています。



相互に関連するサプライチェーン攻撃の概略図

ランサムウェア

同じコードを利用する異なるランサムウェア ソースコードの漏えいにより、無数の亜種が登場

ソースコードが漏えいしたことで、多くの犯罪者がランサムウェアを簡単に利用できるようになった一方で、既存の検知手法が新しいマルウェアに対しても高い効果を発揮するようになりました。

最近、Babuk、Conti、LockBit 3.0 など、いくつかの悪名高いランサムウェア系統のソースコードが公開され、パブリックドメインに流出しました。このため、多くのコードが重複する新しいマルウェアの亜種や系統が無数に出現しています。高度なスキルがない攻撃者でも簡単にランサムウェア攻撃を始めることができるようになっています。これによって、サイバーセキュリティの最前線では多くの攻撃が発生し、混乱も生じている可能性もありますが、防御側にとってプラスとなる要素も生まれています。

Babuk（別名 Babyk）のソースコードは、防御側にプラスの効果をもたらしている典型的な例です。同グループが 2021 年 9 月に**コードを公開**してから、このコードは、新たなランサムウェア系統の基盤としてサイバー犯罪者に注目されるようになっています。サイバー犯罪者にとって、このコードが魅力的である理由は、Linux と VMWare ESXi システムを攻撃できることです。Babuk をベースとする有名なランサムウェア系統には、RAgroup、Nokoyawa、Buhti、および Rorschach があります。

LockBit 3.0 ランサムウェアの「作成ツール」も、**組織に不満を持つ内部関係者**によって公開されたと言われているコードの 1 つです。このマルウェア系統は、過去に流出したソースコードを基に構築されており、LockBit 3.0 Black と Green の亜種は、それぞれ Black Matter と Conti をベースにしています。Buhti ランサムウェア組織は、Windows 向けの亜種を作成するために、公開されている LockBit 3.0 Black を利用しています。Rorschach と命名された別の新興のランサムウェア系統では、LockBit 2.0 の古いコードと Babuk が混在していることも確認されています。

身代金を要求するメモにも変化が見られます。これまでは、各サイバー攻撃者がそれぞれ固有の身代金メモを使用していましたが、現在のサイバー犯罪者は相互に模倣し合っており、同じようなメモが使用されるようになっています。身代金を要求するテキストファイルがドロップされ、ランサムウェアを特定するのに役立つ場合もありますが、このメモが表示されたということは、ユーザーのデータがすでに暗号化されていることを意味します。

ソースコードが共有され、類似する身代金メモが使用されるようになったことで、ランサムウェアを追跡する一般的な作業は煩雑化するかもしれませんが、防御者はサイバー攻撃者の活動を特定するために、汎用的な検出機能とルールセットを使用することが可能になります。これらのルールを使用するだけで、新しく登場したランサムウェアを含む広範な亜種を特定できるようになっています。

ESET のテレメトリでは、2022 年下半期から 2023 年上半期にかけてランサムウェアの検出数は 10% 以上増加しています。しかし、米国のあるネットワーク環境で 1

Babuk ランサムウェアの概要

Vasa Locker を進化させた Babuk（または Babyk）ランサムウェアは、2021 年に発見されました。大企業を攻撃したことでその悪名を世に知らしめましたが、このランサムウェア攻撃の最も有名な被害者は、**コロンビア特別区首都警察**です。このサイバー犯罪組織は、同警察機関から 250GB のデータを入手したと主張し、400 万ドルを支払わなければ、公表すると脅迫しました。しかし、その結果、このサイバー犯罪組織は他の法執行機関の注目を集めることとなり、活動停止に追い込まれ、分裂しました。**Windows、NAS、および ESXi の亜種**を含むこのマルウェアのソースコードが 2021 年 9 月に公開されたことで、新しいランサムウェア系統の基盤として悪用されるようになっています。

日に多数の Win/Filecoder.BlackBasta が検出されたことが、この増加の主な原因です。この時期のスパイクを除外すれば、ランサムウェア攻撃の検出数は両期間でほぼ同じになっています。

この検出傾向のデータには、ESET が最終的なペイロードとしてランサムウェアを検出したインスタンスのみが含まれています。RDP ブルートフォース攻撃、脆弱性の攻撃、マルスパム、または、ドロッパー、ダウンローダー、情報窃取型マルウェアなど、初期段階で検出された攻撃は、このランサムウェアのデータセットには含まれません。

注意すべき新たなランサムウェア

Buhti

このランサムウェア系統には、Windows と Linux システムの両方に対応する亜種があり、それぞれが流出した異なるソースコードを基盤として構築されています。Windows の亜種では、修正された LockBit 3.0 の作成ツールを使用しており、Linux（および VMWare ESXi）では「オープンソース化された」の Babuk コードを使用しています。

Cactus

Cactus ランサムウェアは、ネットワークに最初のアクセスするために VPN デバイスの既知の脆弱性を攻撃します。その後、パスワードで保護された 7-Zip アーカイブからランサムウェアのバイナリを抽出し、検出を回避するために効果的に暗号化を使用します。これは、2017 年に WannaCryptor（別名 WannaCry）によって使用されている既知の手法です。

MalasLocker

新たに登場した MalasLocker ランサムウェアは、従来のランサムウェアとは、その性質を異にしています。MalasLocker のオペレーターは、身代金ではなく、攻撃者が指定する非営利団体に寄付するように被害者に要求します。

MoneyBird

Agrius と呼ばれるイラン政府とつながりのあるサイバー攻撃者は、標的ユーザーのデータを破壊するために MoneyBird と呼ばれる新しいランサムウェアの亜種を展開しています。イスラエルの組織を標的とするワイパー型マルウェアのキャンペーンは、これまでにも検出されています。

MortalKombat

このマルウェア系統を操っているオペレーターは、ポート 3389 を利用するリモートデスクトップアクセスにブルートフォース攻撃を行い、Laplas と呼ばれるクリッパーマルウェアが含まれるバンドルとして MortalKombat を展開します。

RAgroup

RAgroup ランサムウェアは、流出した Babuk のソースコードを基にして作成されおり、主に韓国と米国の企業を標的としています。断続的な暗号化を使用し、対象となるファイルの一部のみを暗号化することで、攻撃を高速化しています。この詳細は、次のコラムの「White Phoenix」を参照してください。RAgroup のオペレーターはまた、窃取したデータをリークサイトで販売しています。

Rorschach

Rorschach は、今日のランサムウェア市場で最も高速に暗号化する能力があり、高度なカスタマイズが可能で、Babuk、Lockbit 2.0、Yanlouwang、DarkSide と共通点があります。

Trigona

Trigona ランサムウェアは、**インターネットに接続している Microsoft SQL Serverst** にブルートフォース攻撃を仕掛けてアクセスし、ランサムウェアをインストールして被害者のデータを暗号化します。

逮捕／活動停止／復号鍵の解放

復号鍵の提供：**Hive ランサムウェア**

最も活発に活動していたランサムウェア集団の 1 つであり、Hive と命名されたランサムウェア組織は、法執行機関にそのシステムが侵入され、破壊されました。この法執行機関によるテイクダウンは、ドイツ、オランダ、米国の当局が主導し、欧州警察機構（ユーロポール）と 13 か国の支援を受けました。これにより、Hive のサーバーとダークウェブのリークサイトが押収されています。当局によると、このテイクダウンにより、約 1 億 3,000 万ドルの身代金が救済され、過去に被害を受けた組織やユーザーに復号鍵が作成されています。このテイクダウンによって逮捕者は出ていません。

復号ツール：**White Phoenix**

データを暗号化するには時間がかかり、防衛側が不審な処理に気が付くことができる場合も多くあります。防御側に検出されることを避けるため、ランサムウェア組織は最近、断続的に暗号化する手法を使い始め、標的のデータの一部だけを暗号化するようになりました。White Phoenix と呼ばれる新しい復号ツールは、このアプローチを利用して、一部のファイル形式を復元します。完全には復号することはできませんが、場合によっては、重要なデータを復号化でき、身代金を支払わずに済む場合もあります。

復号ツール：**MegaCortex ランサムウェア**

2023 年上半期には、MegaCortex ランサムウェアの復号ツールが公開されました。このツールは単体で実行でき、被害を受けたユーザーのシステムで影響を受けたデータを自動的に検索して復元します。MegaCortex は、主に 2019 年に活動していましたが、2020 年には活動を停止しています。2021 年 10 月、欧州警察機構は、MegaCortex などの複数のランサムウェアを展開し、1,800 件のランサムウェア攻撃に関与したとして 12 人を逮捕しました。

復号ツール：**ESXiArgs ランサムウェア**

米国 CISA（サイバーセキュリティインフラセキュリティ庁は、ESXiArgs ランサムウェアによって暗号化されたファイルを**復元するスクリプト**を公開しました。このランサムウェア系統は、主に、パッチが適用されていない、サービスが終了している、また、古い VMware ESXi サーバーの既知の脆弱性を悪用して拡散します。CISA によると、このランサムウェア系統を操っていたサイバー攻撃者は、全世界で 3,800 台以上のサーバーに侵入し、設定ファイルを暗号化して仮想マシンを使用不能にしました。

刑罰：**Ryuk を支援したロシア人が有罪に**

Ryuk ランサムウェアのマネーロンダリングに関与したロシア国籍の Denis Dubnikov は、米国の裁判所から、既に服役している実刑期間を除く禁固刑を**言い渡されました**。さらに、Dubnikov には 1 万ドルの罰金が科せられ、2,000 ドルが没収されています。同じような犯罪については、最高で 20 年の懲役刑に処せられる可能性もありますが、有罪答弁の後で、裁判所は Dubnikov を仮釈放することを決定しています。

制裁：**TrickBot、Ryuk、Conti のアフィリエイト**

2023 年の 2 月に米国と英国は、TrickBot マルウェア、Ryuk、Conti ランサムウェアの攻撃に関連した 7 名について、**歴史上初となる制裁**を共同で発表しました。この制裁の結果、制裁の対象となったこれらの個人に属する米国および英国内のすべての財産および資金がブロックされ、当局に報告されました。この制裁により、両国の個人および企業は、制裁を受けた個人との取引を行うことができなくなっています。

逮捕：**DoppelPaymer グループ**

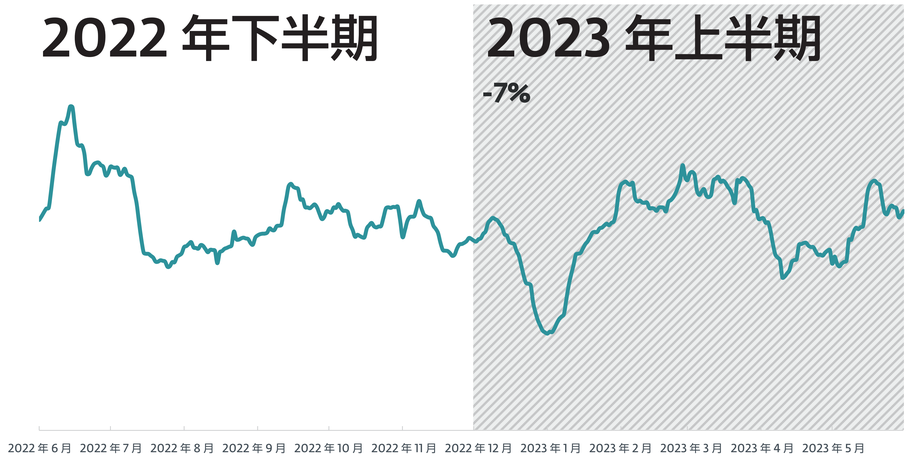
2023 年 2 月に、法執行機関は、ランサムウェアグループである「DoppelPaymer」の中心メンバーとされる 2 人を逮捕するため、ドイツとウクライナの 3 カ所を**家宅捜索**しました。ドイツの捜査当局は、「この犯罪グループの首謀者」に対してさらに 3 件の逮捕状を出しています。DoppelPaymer グループは、ドイツだけでもデュッセルドルフの病院など 37 の企業を攻撃しています。同グループによる米国人の被害者は、2019 年から 2021 年の間に少なくとも 4,000 万ユーロを支払っています。

懸賞金：**LockBit、Babuk、Hive**

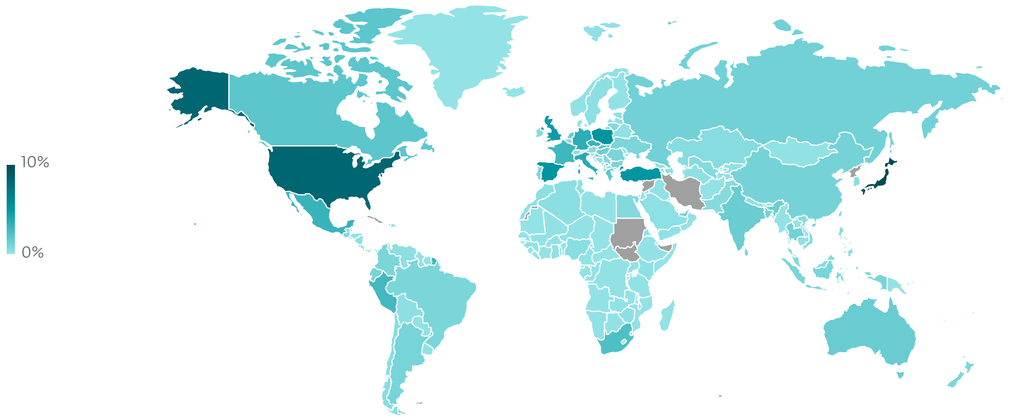
米国当局は、LockBit、Babuk、Hive ランサムウェアに関与し、ロシアで活動している Mikhail Pavlovich Matveev を、重要インフラに対するサイバー攻撃で**起訴**しました。さらに、逮捕につながる情報の提供者に対して 1000 万ドルの懸賞金を提供しています。これら 3 つのグループによる被害者の身代金支払額の総額は 2 億ドルにのぼり、身代金要求額はその 2 倍に達しています。

脅威テレメトリ

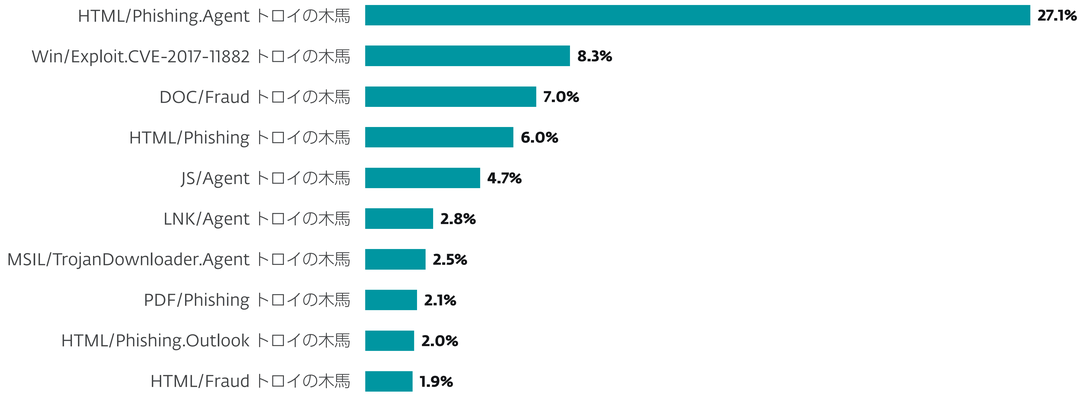
すべての脅威



2022 年下半期～ 2023 年上半期の**脅威全体の検出傾向**、7 日移動平均線

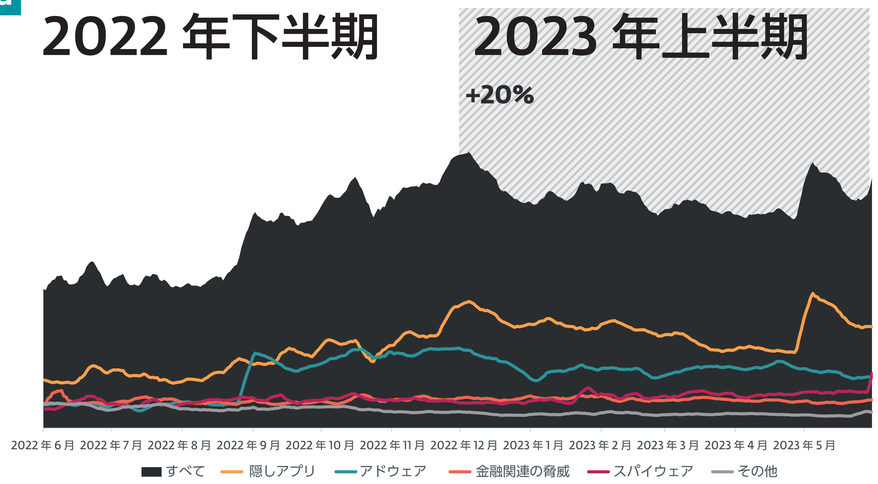


2023 年上半期における**マルウェア検出の地理的な分布**

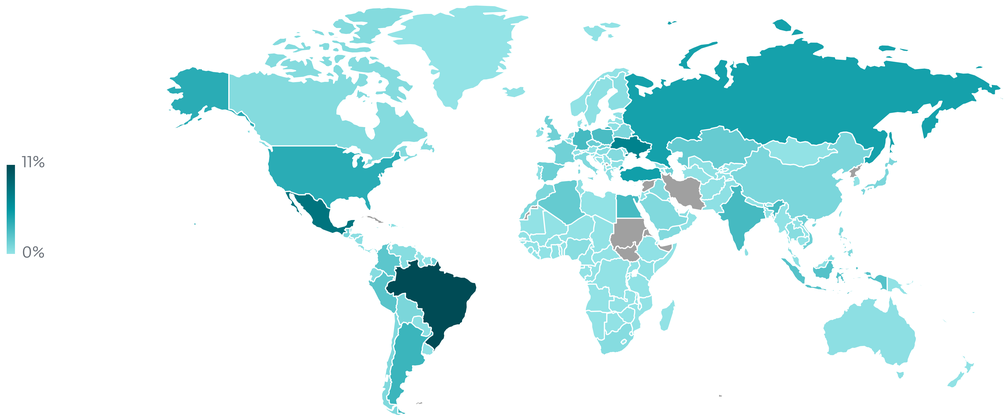


2023 年上半期の**マルウェア検出率トップ 10**（マルウェア検出数に占める割合）

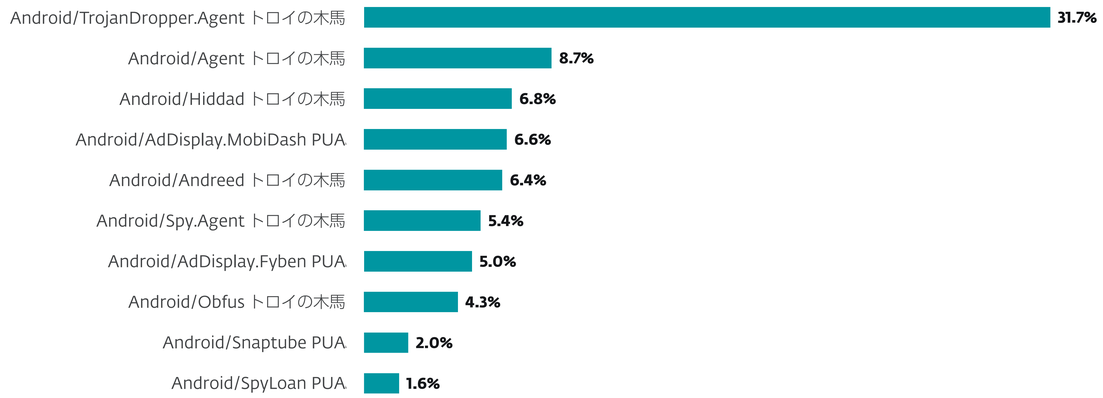
Android



2022 年下半期～ 2023 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）

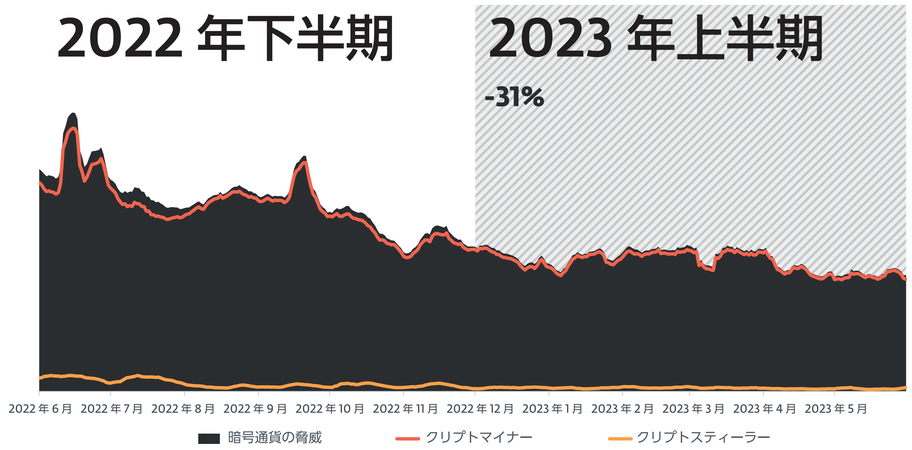


2023 年上半期における **Android に関連する脅威検出の地理的な分布**

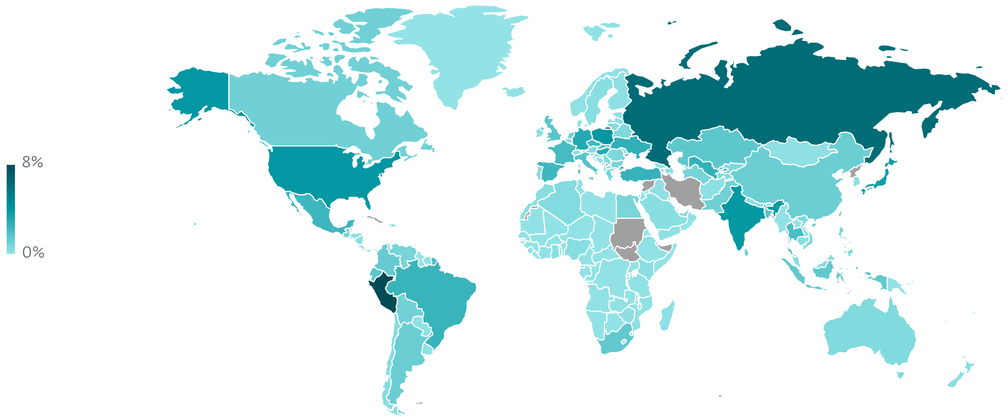


2023 年上半期の **Android の脅威の検出率トップ 10**（マルウェア検出数に占める割合）

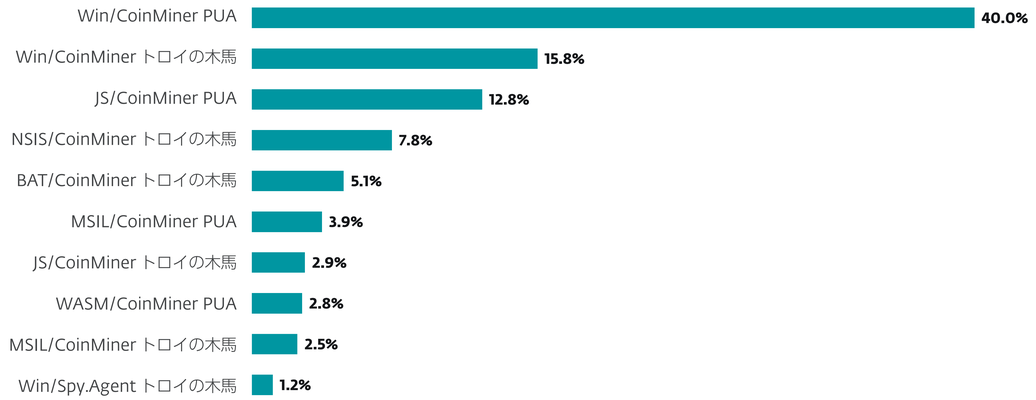
暗号通貨の脅威



2022 年下半期～ 2023 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

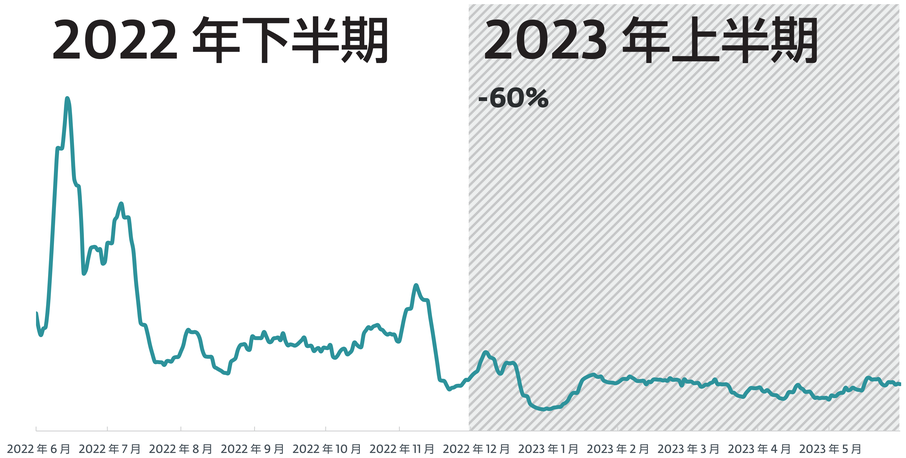


2023 年上半期における**暗号通貨の脅威の検出数の地理的な分布**

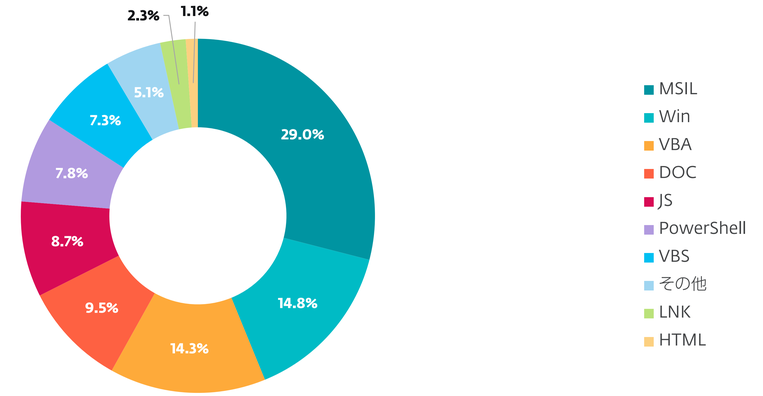


2023 年上半期の**暗号通貨の脅威の検出率トップ 10**（マルウェア検出数に占める割合）

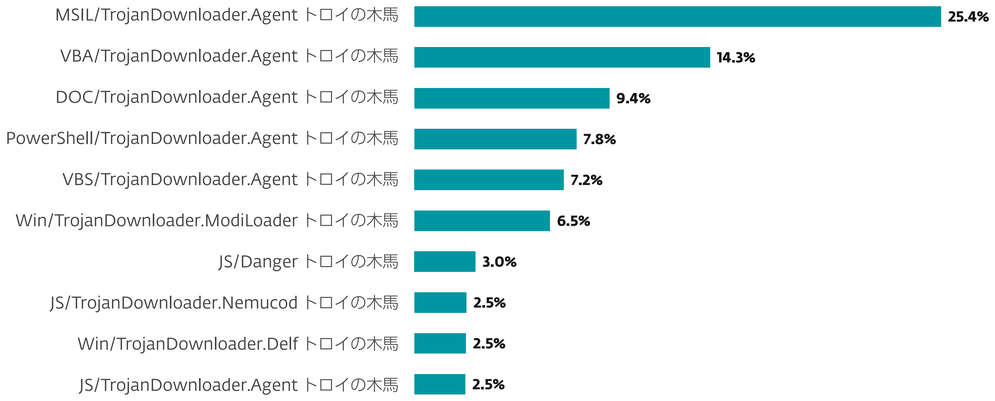
ダウンローダー



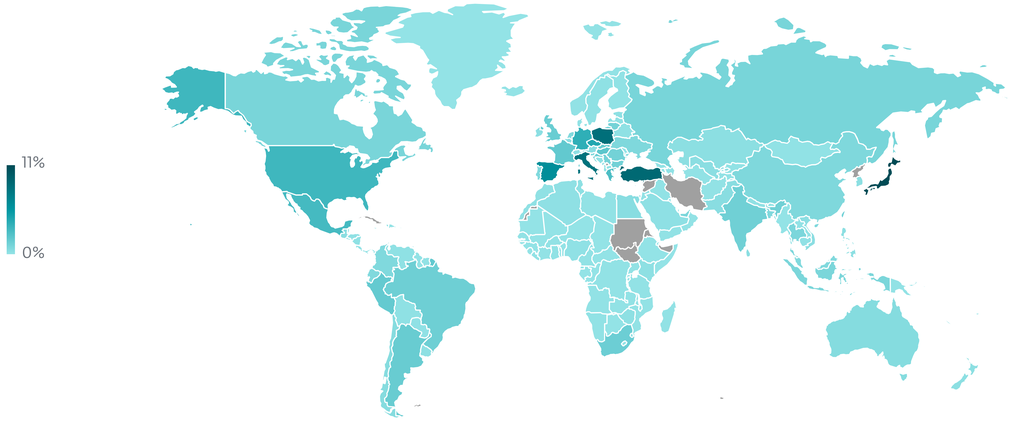
2022 年下半期～ 2023 年上半期の**ダウンローダーの検出傾向**、7 日移動平均線



2023 年上半期の**ダウンローダータイプ別の検出率**

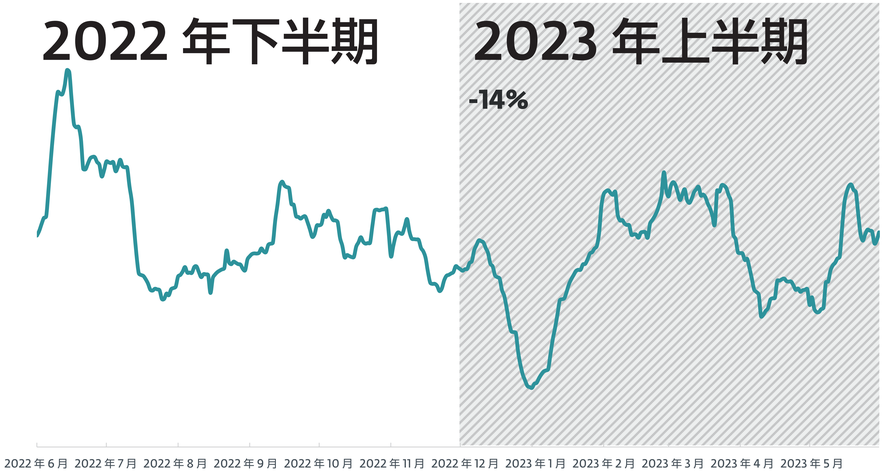


2023 年上半期の**ダウンローダーの検出率トップ 10**（マルウェア検出数に占める割合）

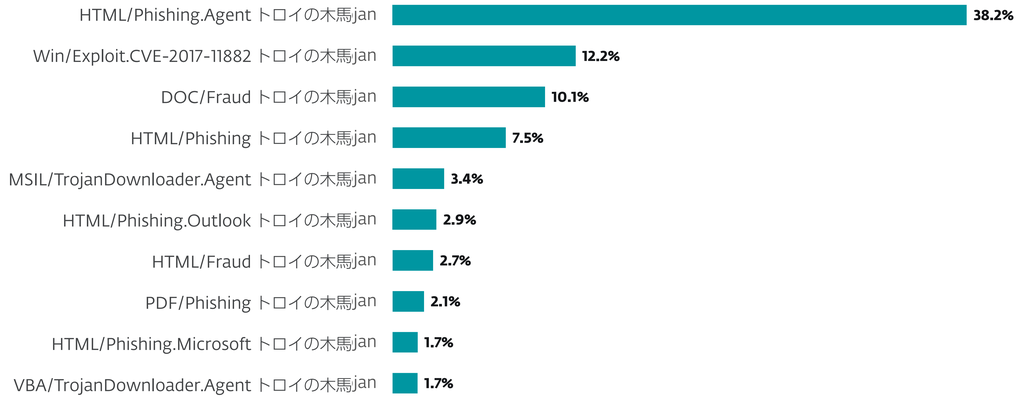


2023 年上半期における**ダウンローダー検出数の地理的な分布**

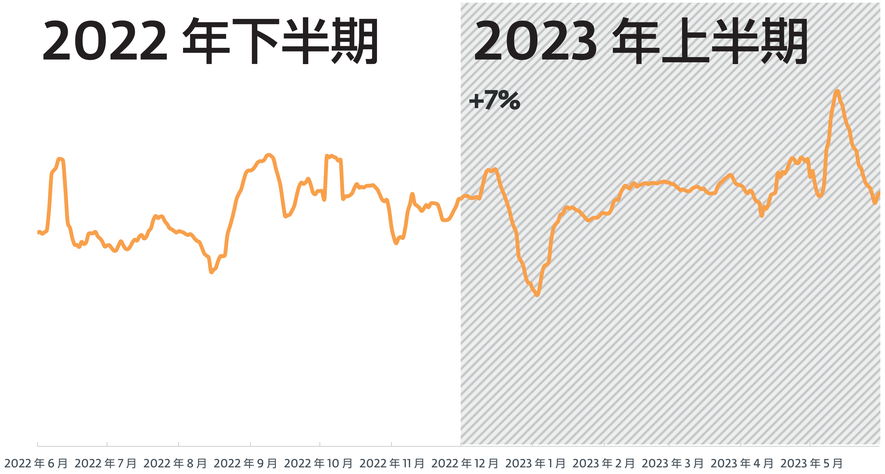
メールの脅威



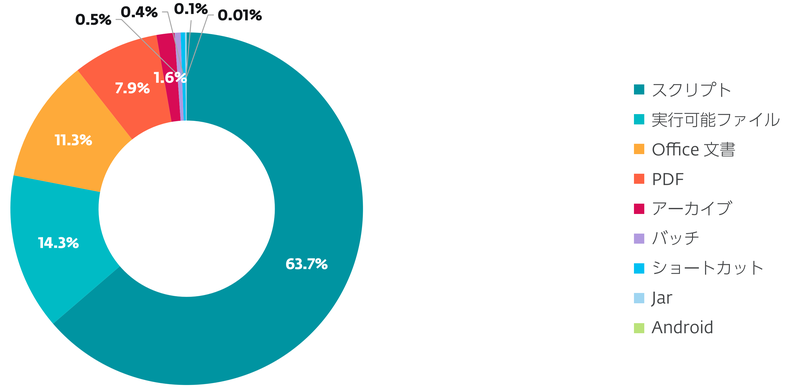
2022 年下半期～ 2023 年上半期の**悪意のあるメールの検出傾向**、7 日移動平均線



2023 年上半期に**検出されたメールの脅威トップ 10**

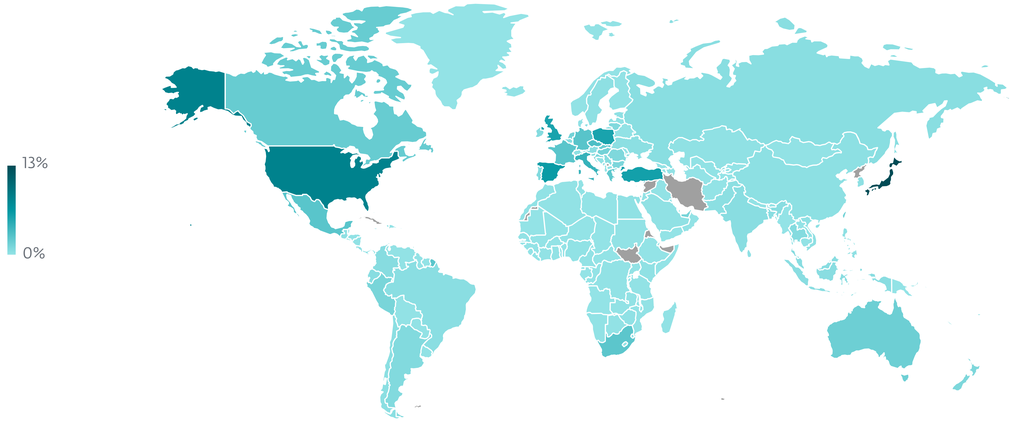


2022 年下半期～ 2023 年上半期の**スパムの脅威の検出傾向**、7 日移動平均線



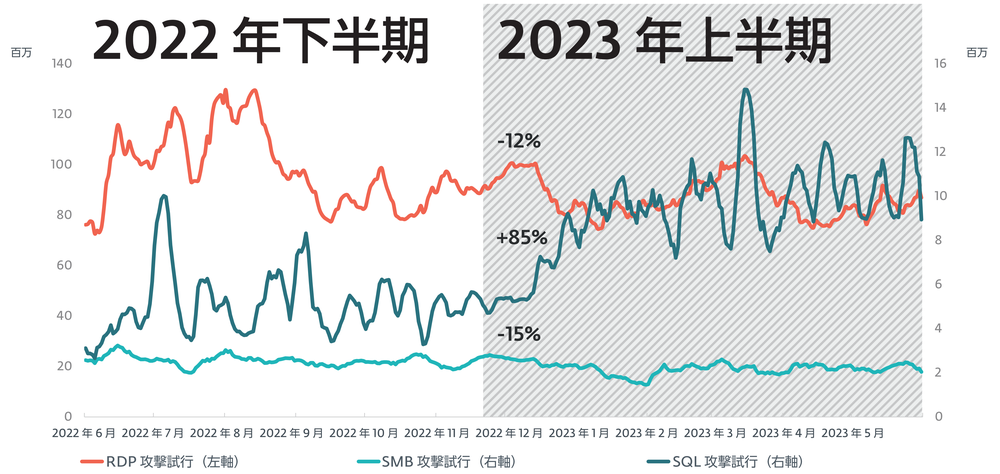
2023 年上半期の**主な悪意のある電子メールの添付ファイルタイプ**

メールの脅威

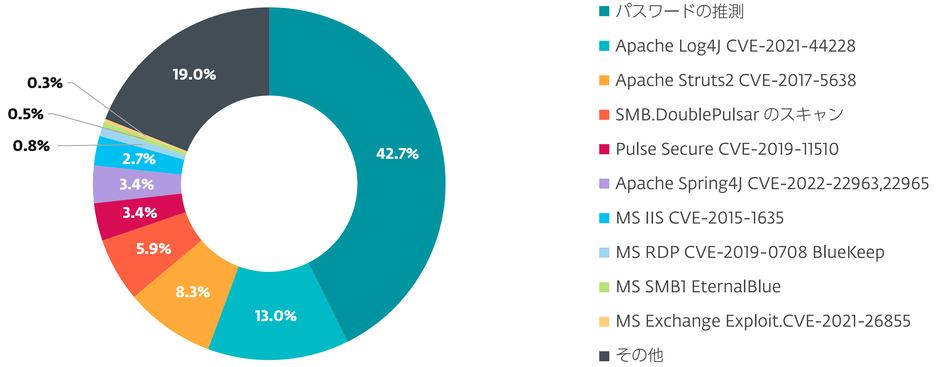


2023 年上半期における**メール脅威の検出数の地理的な分布**

エクスプロイト

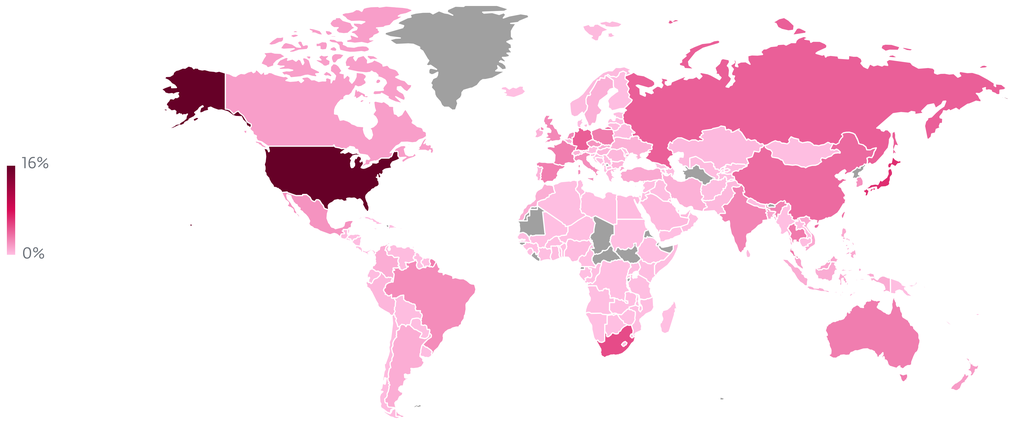


2022 年下半期～ 2023 年下半期における **RDP、SMB、SQL 攻撃試行の傾向**、7 日間移動平均線

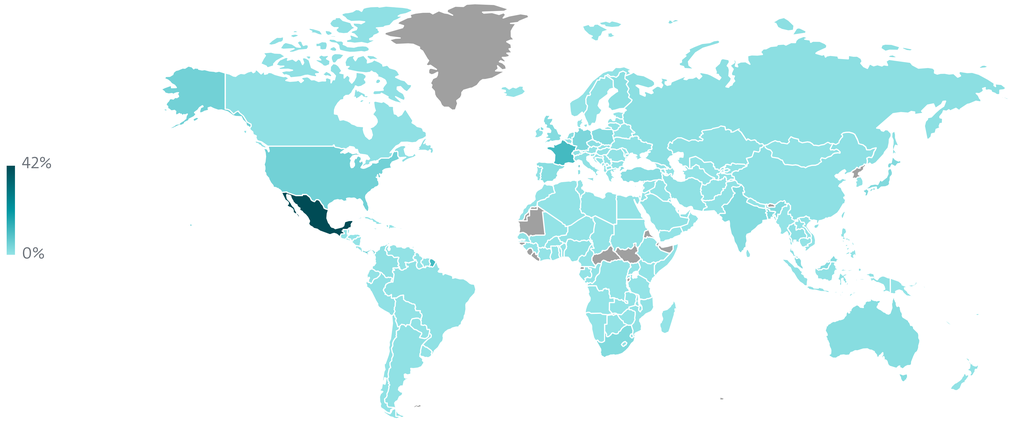


2023 年上半期にユニーククライアントから報告された**外部からのネットワークへの侵入方法**

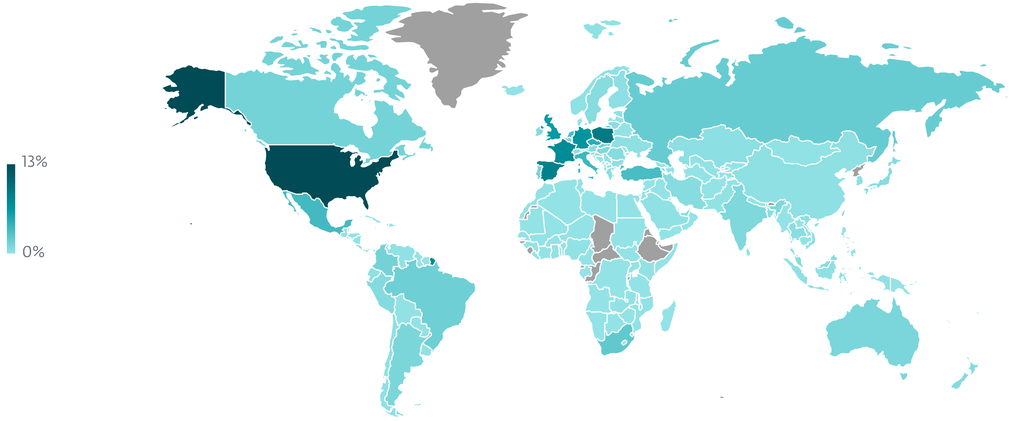
エクスプロイト



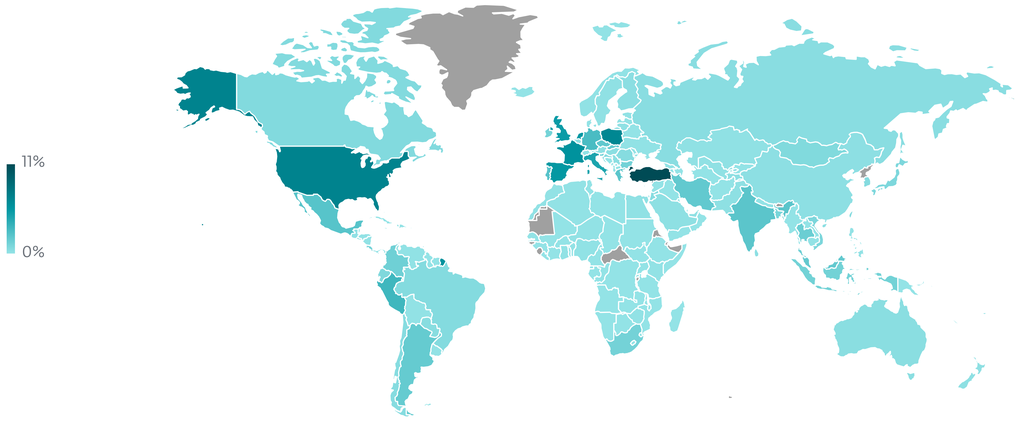
2023 年上半期に **RDP パスワード推測攻撃を実行したソースの地理的な分布**



2023 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**

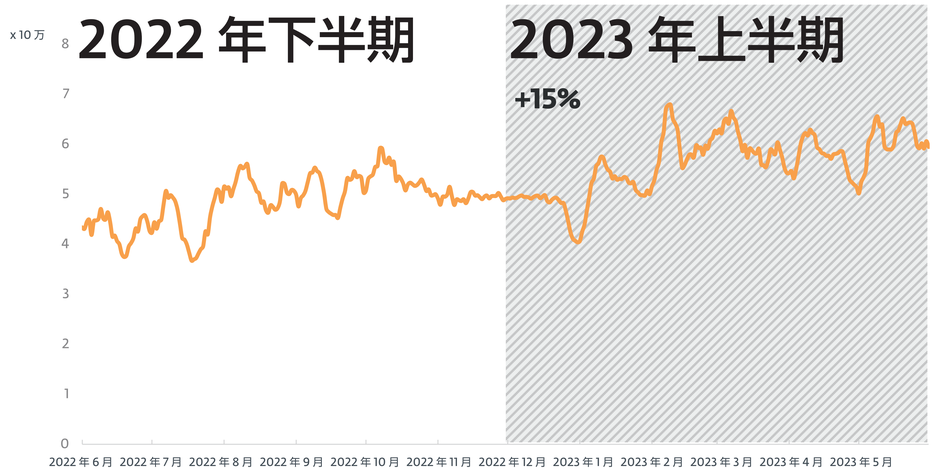


2023 年上半期に **RDP パスワード推測攻撃が実行された標的の地理的な分布**

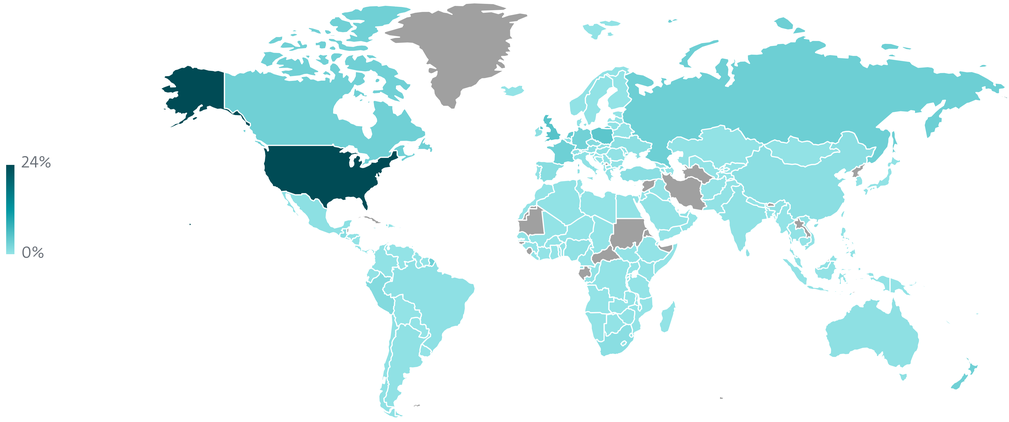


2023 年上半期に **SQL パスワード推測攻撃が実行された標的の地理的な分布**

エクスプロイト

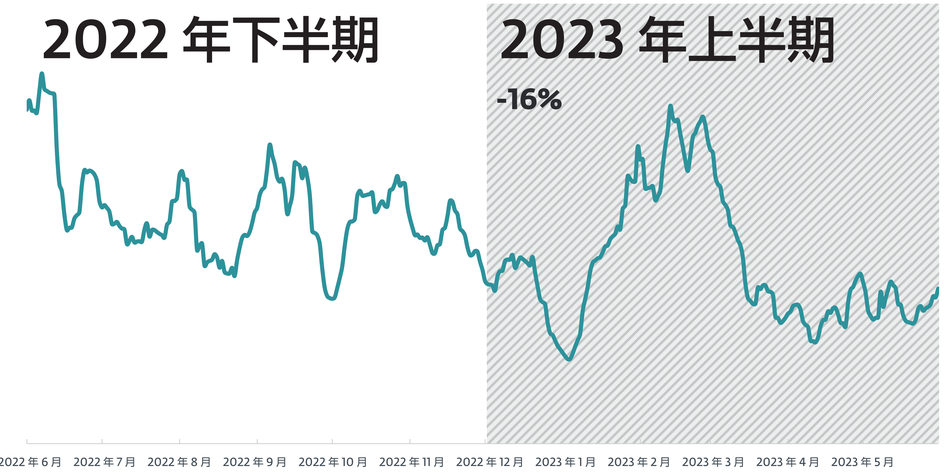


2023 年上半期における **Log4Shell 攻撃試行の検出傾向**

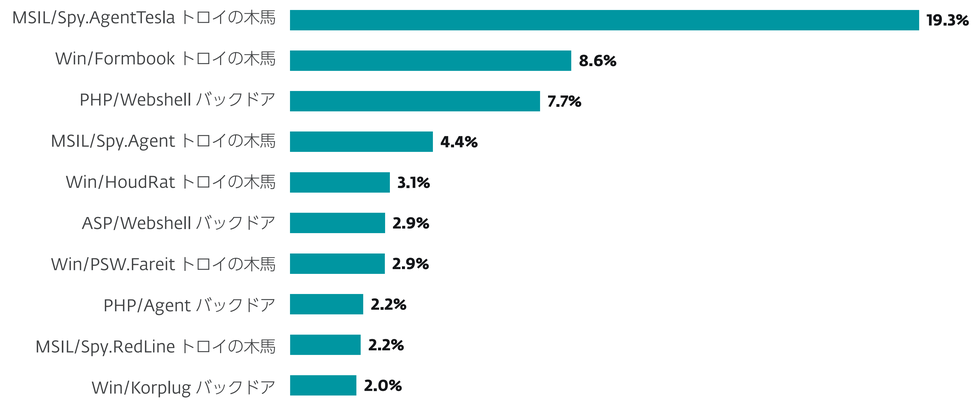


2023 年上半期における **Log4Shell 攻撃試行の地理的分布**

情報窃取型マルウェア

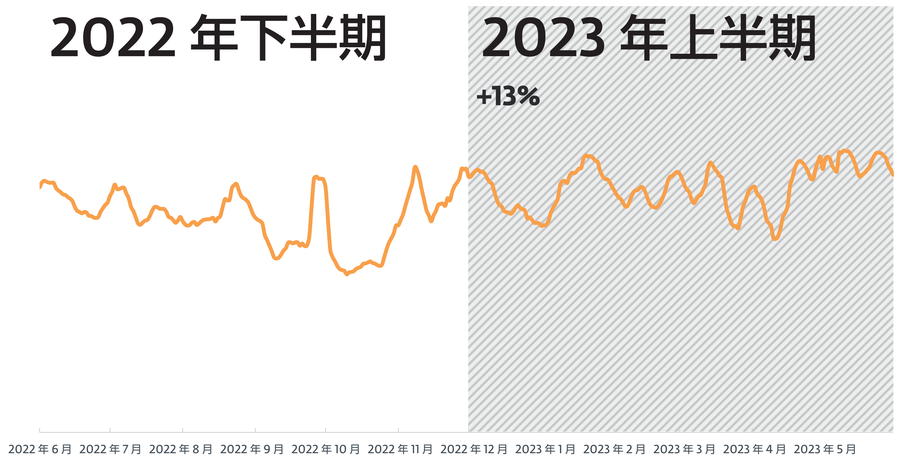


2022 年下半期～ 2023 年上半期の**情報窃取型マルウェアの検出傾向**、7 日間移動平均線

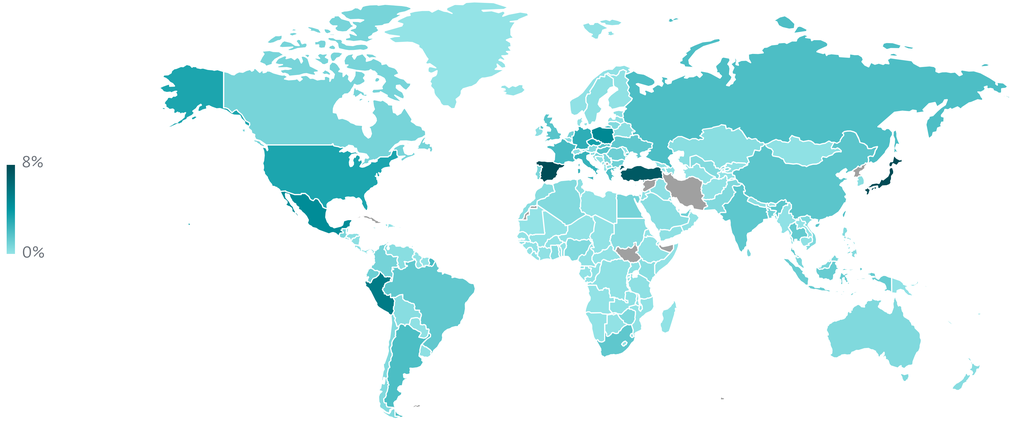


2023 年上半期における**情報窃取型マルウェアのトップ 10**（情報窃取型マルウェアの検出に占める割合）

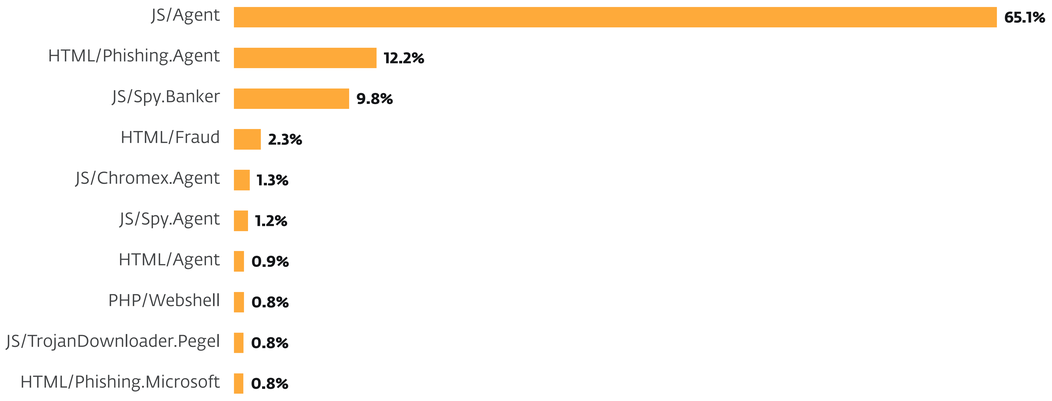
情報窃取型マルウェア



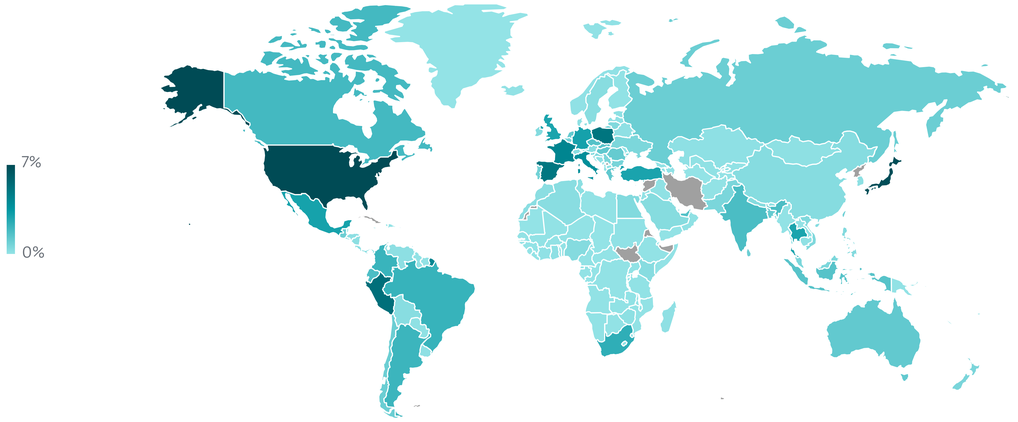
2022 年下半期～ 2023 年上半期の**オンライン情報窃取型マルウェアの検出傾向**、7 日移動平均線



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**

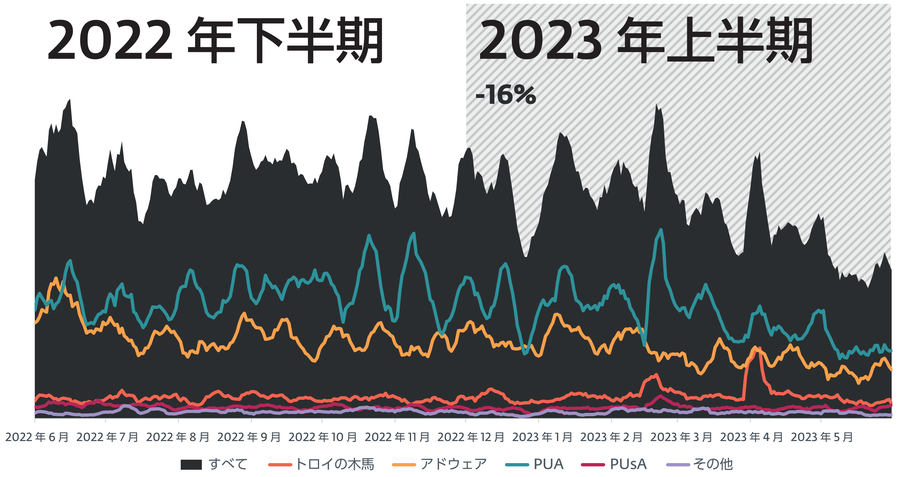


2023 年上半期における**オンライン情報窃取型マルウェアのトップ 10**（マルウェアの検出に占める割合）

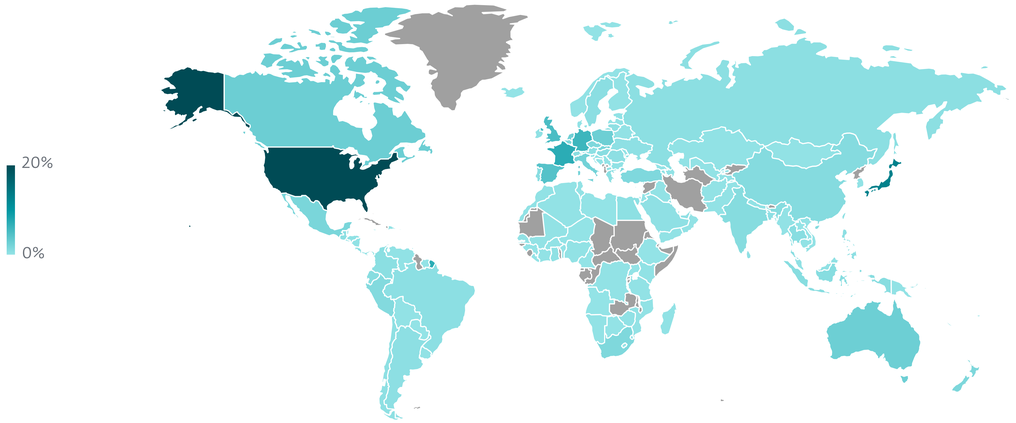


2023 年上半期における**オンライン情報窃取型マルウェアの検出の地理的な分布**

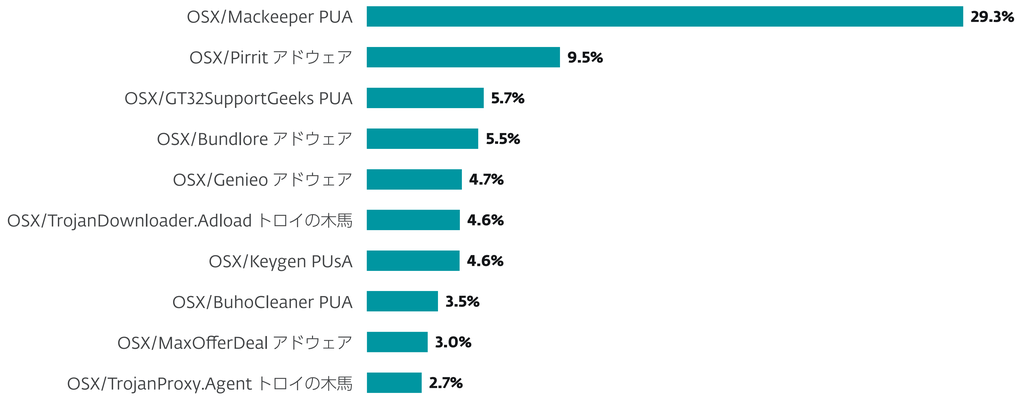
macOS



2022 年下半期～ 2023 年上半期の **macOS への脅威の検出傾向**、7 日移動平均線

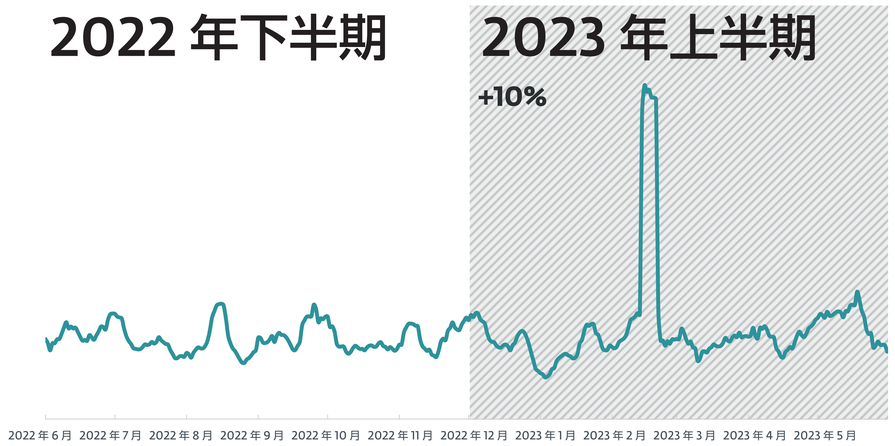


2023 年上半期における **macOS への脅威の検出の地理的な分布**

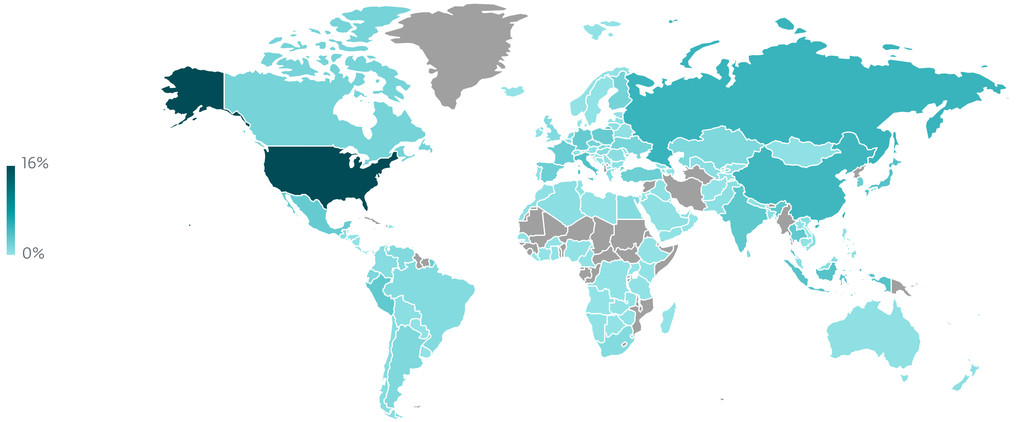


2023 年上半期の **Mac の脅威検出率トップ 10**（MacOS の脅威検出数に占める割合）

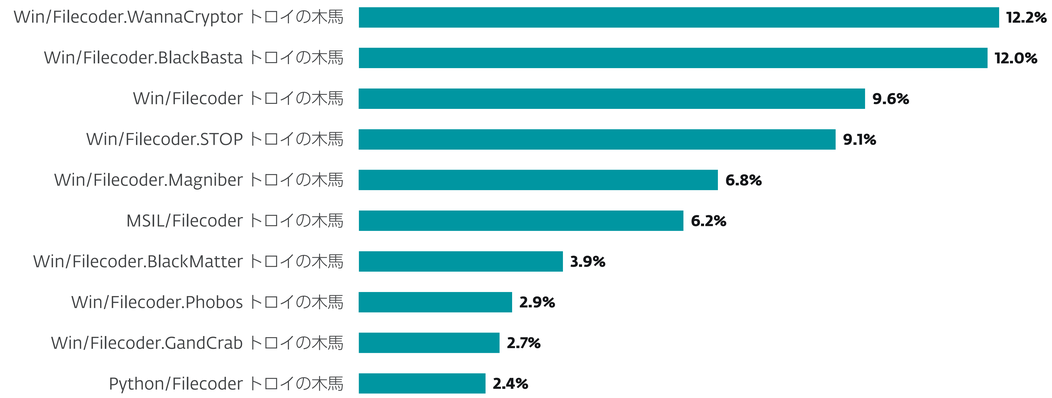
ランサムウェア



2022 年下半期～ 2023 年上半期の**ランサムウェアの検出傾向**、7 日移動平均線

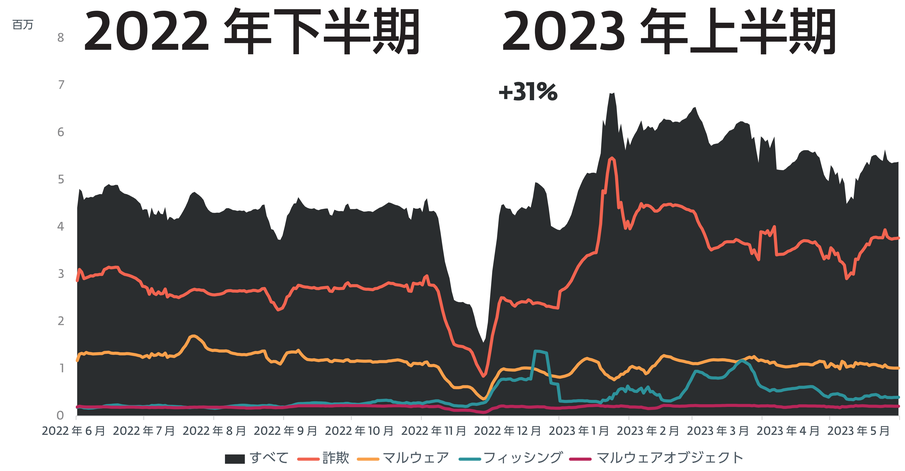


2023 年上半期における**ランサムウェアへの検出の地理的な分布**

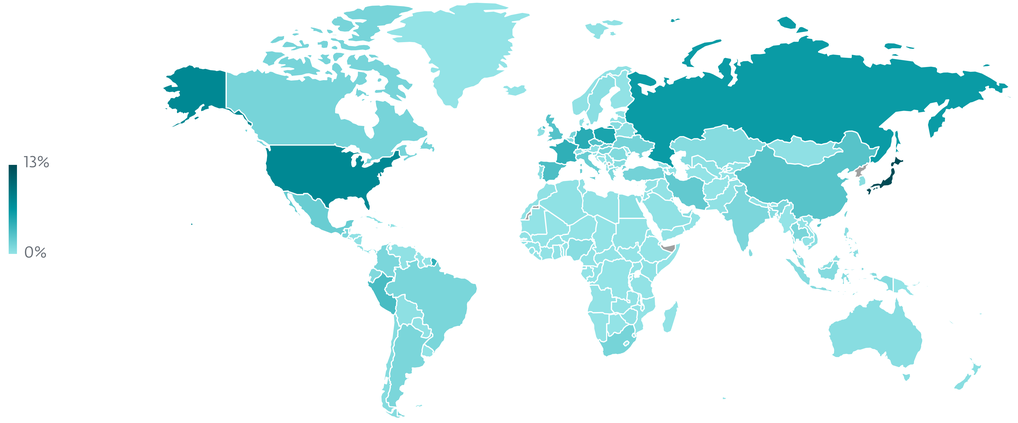


2023 年上半期の**ランサムウェア検出率トップ 10**（ランサムウェア検出数に占める割合）

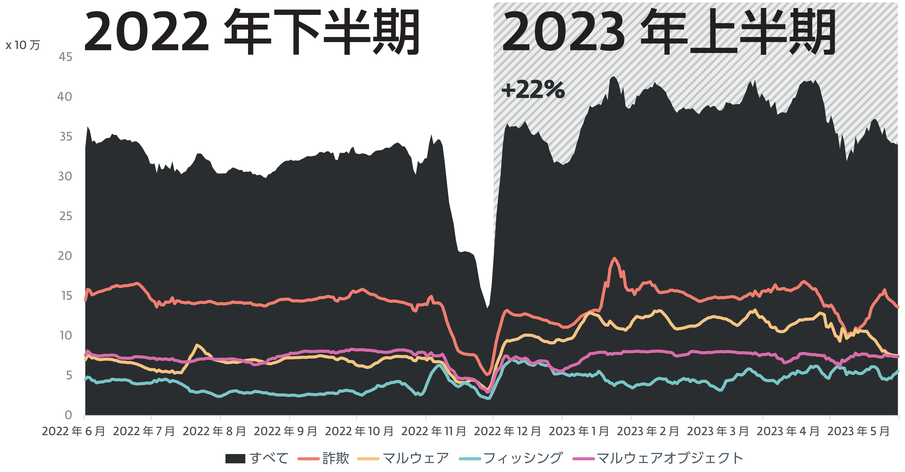
Web に関する脅威



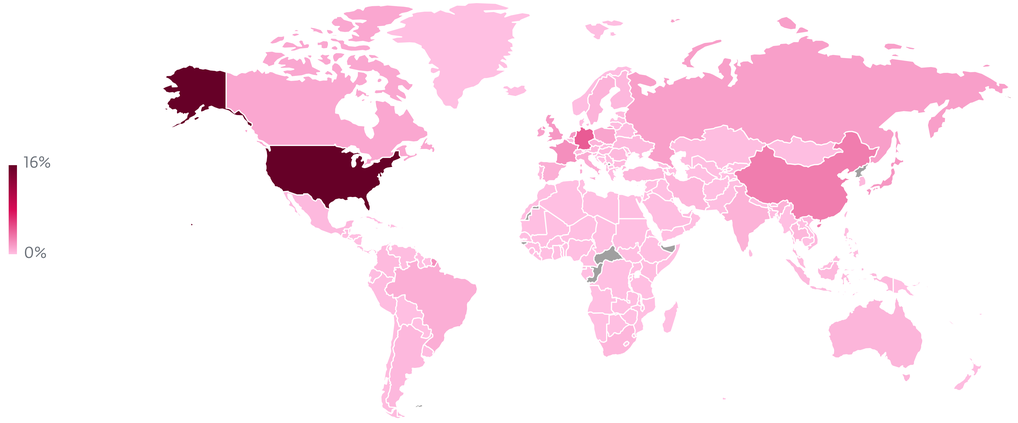
2022 年下半期～ 2023 年上半期に**ブロックされた Web 脅威の傾向**、7 日移動平均線



2023 年上半期に**ブロックされた Web 脅威の世界的な分布**



2022 年下半期～ 2023 年上半期に**ブロックされたユニーク URL の傾向**、7 日間移動平均線



2023 年上半期に**ブロックされたドメインホストの地理的な分布**

調査レポート

ファイルやプログラムを暗号化するツール「AceCryptor」の技術的な分析結果と、サイバー攻撃者による運用を解説

ESET の研究者は、広く悪用されているクリプター（ファイルやプログラムを暗号化するツール）の詳細を明らかにしました。このクリプターは、数十のマルウェア系統で使用されており、「クリプター・アズ・ア・サービス（サービスとしてのクリプター）」として運用されています。

トロイの木馬化された Android アプリ：画面を録画する正規のアプリが 1 年後にファイルを漏えいする不正なアプリであることが判明

ESET の研究者が、音声を記録してそのファイルを外部に送信する AhMyth をベースにした新しい Android RAT である「AhRat」を発見しました。

APT グループの Evasive Panda、中国の人気ソフトウェアのアップデートからマルウェアを配信

ESET Research は、Evasive Panda と呼ばれる APT グループが実行している、中国の国際 NGO を標的としたキャンペーンを発見しました。

Linux マシンを攻撃するマルウェアの分析結果から、3CX 社のサプライチェーン攻撃への Lazarus グループの関与が裏付けられる

「DreamJob 作戦」で使用されたことが新たに発見された Linux マルウェアとの類似性から、北朝鮮とつながりのあるサイバー攻撃グループ「Lazarus」が、コミュニケーションソフトウェアを開発・販売している 3CX 社のサプライチェーン攻撃を実行していることが明確になりました。

2022 年第 4 四半期～ 2023 年第 1 四半期の ESET APT 活動レポート

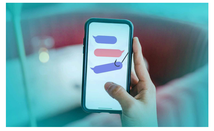
ESET Research は、2022 年 10 月から 2023 年 3 月までに分析した一部の APT（持続的標的型攻撃）グループの活動内容をまとめて報告しました。

インスタントメッセージを改ざんし、暗号通貨ウォレットを狙うトロイの木馬化された Telegram と WhatsApp アプリ

ESET の研究者は、インスタントメッセージを改ざんし、OCR を使用して暗号通貨を盗む Android と Windows のクリッパーを分析しました。

仕掛けられた時限爆弾：APT グループ「Tick」による東アジアの DLP ソフトウェア開発会社を狙った攻撃を発見

ESET Research は、APT グループ「Tick」による東アジアの DLP（情報漏洩防止）ソフトウェア会社に対するキャンペーンを発見し、同グループが使用しているこれまで検出・報告されていないツールを発見しました。



恋愛詐欺？それともスパイ行為？ APT グループ「Transparent Tribe」によるインドとパキスタンの高官を標的とした攻撃

ESET の研究者が、安全と考えられていた Android のメッセージングアプリがトロイの木馬化され、CapraRAT バックドアを配信していたサイバースパイキャンペーンを分析しました。

Qt と MQTT を利用する APT グループ「Mustang Panda」の最新バックドア「MQsTTang」を解説

ESET の研究者が、Mustang Panda が使用している MQTT プロトコルで通信する新しいバックドア、MQsTTang の詳細を解説します。

「BlackLotus」UEFI ブートキット：いま、そこにある現実の危機

最新の状態にした UEFI システムであっても、UEFI セキュアブートをバイパスする初の UEFI ブートキットが実環境で悪用されていることが確認されました。

WinorDLL64：Lazarus が利用している膨大な数の攻撃ツールの 1 つ

標的の地域、攻撃の内容やコードの類似点から、このツールは北朝鮮政府とつながりのある APT グループによって使用されている可能性があります。

セキュリティアップデートになりすますマルウェア：東南アジアと東アジアを標的とする偽のインストーラ

ESET の研究者は、トロイの木馬化されたインストーラを使用して、Google の検索結果に表示される広告にリンクされた悪意のある Web サイトから配信され、ファイルを削除するコマンドを実行する FatalRAT マルウェアのキャンペーンを確認しました。

Android ユーザーを標的とする StrongPity のスパイキャンペーン

ESET の研究者は、トロイの木馬化した Android Telegram アプリを配信している StrongPity キャンペーンを確認しました。

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
Ján Šugarek
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Michal Malík
Milan Fránik
Patrik Sučanský
Peter Kálnai
Tomáš Procházka
Vladimír Šimčák
Zoltán Rusnák

本レポートのデータについて

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 30 年間にわたり世界中の個人および法人に向けて、業界をリードする革新的な IT セキュリティソフトとサービスを開発し、サイバーセキュリティ脅威に対する包括的な多層防御ソリューションを提供してきました。ESET は長年にわたり、マルウェアの予防、検出、対応を行う機械学習とクラウドテクノロジーのパイオニアとして活動しています。ESET は、科学的な研究開発を世界的に推進している非公開会社です。

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