BlackBerry | Cybersecurity

グローバル脅威インテリジェンスレポート

実情を踏まえた
実践的なインテリジェンスで、
サイバーレジリエンスを強化

調査期間：2022 年 9 月 1 日～ 11 月 30 日

目次

はじめに

*脅威インテリジェンスは、**「攻撃者に不意打ちを食らわせるための技術」**と考えることができます。実践的な脅威インテリジェンスプログラムの最大のミッションは、サイバー攻撃という形で行われる奇襲を予測し、軽減し、予防することです。*

この使命を果たすには、事前対応型のアプローチを採用して、いくつもの重要な疑問を解き明かす必要があります。こうした疑問には、「所属している組織に影響を及ぼす可能性が最も高い脅威アクターは何か？」、「脅威アクターの目的や動機は何か、どの程度の能力があるか？」、「脅威アクターはどのように行動するか、目的達成に使用するサイバー兵器は何か？」といったものがあります。そして究極的には、「組織のサイバー防御能力の強化をもたらす、導入可能な実践的対策は何か？」という疑問の答えに到達しなければなりません。

私たちのチームはこのたび「**BlackBerry Cybersecurity グローバル脅威インテリジェンスレポート**」を初めて公開することになりました。本レポートの目的は、標的型攻撃、サイバー犯罪の成功を狙う脅威アクター、各種キャンペーンなど、本レポートの対象組織を狙うさまざまな行為に関する実践的なインテリジェンスを提供し、十分な情報に基づいた意思決定と効果的な対策を迅速に講じていただくことです。

今回の第 1 版では、BlackBerry Threat Research & Intelligence チームに所属するトップクラスの脅威リサーチャーおよびインテリジェンスアナリストによるレポートを掲載しています。彼らは、技術的脅威に関する知識はもちろん、地域および世界レベルでの地政学的発展と、そうした進化が各地域の組織の脅威モデルに及ぼす影響についても深い知見を有する専門家集団です。同チームは本レポートの作成にあたり、BlackBerry の人工知能（AI）を基盤とする製品および解析機能から収集したデータとテレメトリに加え、公開および非公開の情報源によるインテリジェンスを補完的に活用しました。本レポートの対象期間は 2022 年 9 月 1 日～ 11 月 30 日の 90 日間です。

本レポートの主な調査結果は以下のとおりです。

- **数字で見る 90 日間の動向。**BlackBerry がお客様に対する影響を未然に防御したマルウェアのユニークサンプル数や、それらの攻撃の地理的分布など、90 日の調査期間における動向を統計で振り返ります。たとえば、BlackBerry のテクノロジーは、新しい悪意あるサンプルを 1 時間あたり平均 62 件阻止しています。つまり、新しいサンプルを 1 分あたり約 1 件阻止していることになります。
- **最も一般的な武器。**Emotet をはじめとする悪意あるローダーの復活、サイバー脅威環境において存在感を増し続ける Qakbot、GuLoader のようなダウンローダの増加など、サイバー攻撃で最も多く使用される武器に関する情報を提供します。

- **リモートアクセスにより増加するインフォスティーラ。**コロナウイルスの影響によりリモートワークやハイブリッドワークが増加したことで、内部ネットワークに外部からアクセスするニーズはますます高まっています。その結果、情報窃取型マルウェア（インフォスティーラ）で企業の認証情報を窃取し闇市場で販売するという、リモートアクセスがもたらす新たな脆弱性を利用する攻撃者の動きが活発化しています。本レポートでは、調査期間において最も蔓延したいくつかのインフォスティーラを紹介します。
- **「絶対に安全」なプラットフォームは存在しない。**脅威アクターによる戦略の標的となるプラットフォームは、各種のサーバー、デスクトップ、モバイルなど多岐にわたります。たとえば、一般に信じられている意見とは異なり、macOS は「より安全性が高い」プラットフォームではありません。実際、macOS を狙うマルウェアや脆弱性は数多く確認されています。その他のトピックとしては、Linux プラットフォームに対する攻撃の増加傾向、Go 言語などの主流ではないプログラミング言語を利用したクロスプラットフォームマルウェアの開発手法、Android や iOS を搭載したモバイルデバイスを侵害する脅威の詳細な解析情報などを取り上げます。
- **BlackBerry 独自の業界分析。**BlackBerry は、サイバーセキュリティ業界と IoT（モノのインターネット）業界の両方で確固たる地位を確立しています。本レポートではこの強みを活かし、その他の脅威レポートではあまり取り上げられない、自動車業界をはじめとするさまざまな業界に対する脅威に光を当てています。今回の第 1 版で提供される BlackBerry が確認したサイバーセキュリティトレンド情報の対象には、自動車業界に加えて医療業界や金融業界も含まれます。
- **最大の脅威アクターとその対策。**BlackBerry が収集したテレメトリからは、数多くの脅威アクターの活動も明らかにされています。本レポートでは、こうした脅威アクターが採用する最も一般的な戦術、技術、手順（TTP）に関する情報を紹介するとともに、MITRE ATT&CK や MITRE D3FEND に紐付いた、適用済み対策の公開リストへのリンクを記載しています。BlackBerry の目標は、現在の組織における防御体制や脅威モデルを、こうした実践的な情報に基づいて今まで以上に簡単に更新できるようにすることです。
- **まとめと今後の展望。**最後に、BlackBerry がまとめた結論を述べるとともに、2023 年のサイバー脅威に関する見通しを紹介します。

本レポートは、**BlackBerry Threat Research & Intelligence チームが誇る全世界の優秀なリサーチャー**によって完成を迎えることができました。市場で初めてとなる調査レポートを数多く生み出し続けるだけでなく、BlackBerry のデータと Cylance の AI を基盤とする製品とサービスの改善にも継続的に取り組んでいる彼らに、あらためて感謝を申し上げます。

Ismael Valenzuela
BlackBerry Threat Research & Intelligence 担当バイスプレジデント
@aboutsecurity

BLACKBERRY CYBERSECURITY 脅威インテリジェンス執筆者

Dmitry Bestuzhev

Pedro Drimel

Jacob Faires

Dean Given

Eoin Healy

Geoff O'Rourke

Jose Luis Sanchez

数字で見る過去 90 日間の動向

攻撃の合計数

2022 年 9 月 1 日～ 11 月 30 日の 90 日間で、BlackBerry の Cylance® Endpoint Security ソリューションはマルウェアベースのサイバー攻撃を 1,757,248 件阻止しました。脅威アクターは、BlackBerry のテクノロジーで保護されている顧客に対し、1 日あたり平均約 19,524 件の悪意あるサンプルを展開しました。これらの脅威に含まれるマルウェアのユニークサンプル数は 133,695 件です。つまり新しいマルウェアサンプルは 1 日あたり平均 1,485 件、1 時間あたり 62 件となり、新しいサンプルが 1 分あたり平均 1 件阻止されていることになります。

以下のグラフは、2022 年 9 月 1 日～ 11 月 30 日の間で Cylance Endpoint Security ソリューションが未然に防御した、サイバー攻撃の推移を示しています。第 4 週（9 月 29 日～ 10 月 5 日）と第 7 週（10 月 20 日～ 10 月 26 日）における件数の急増は、脅威アクターがマルウェアサンプルを再利用したことが原因です。

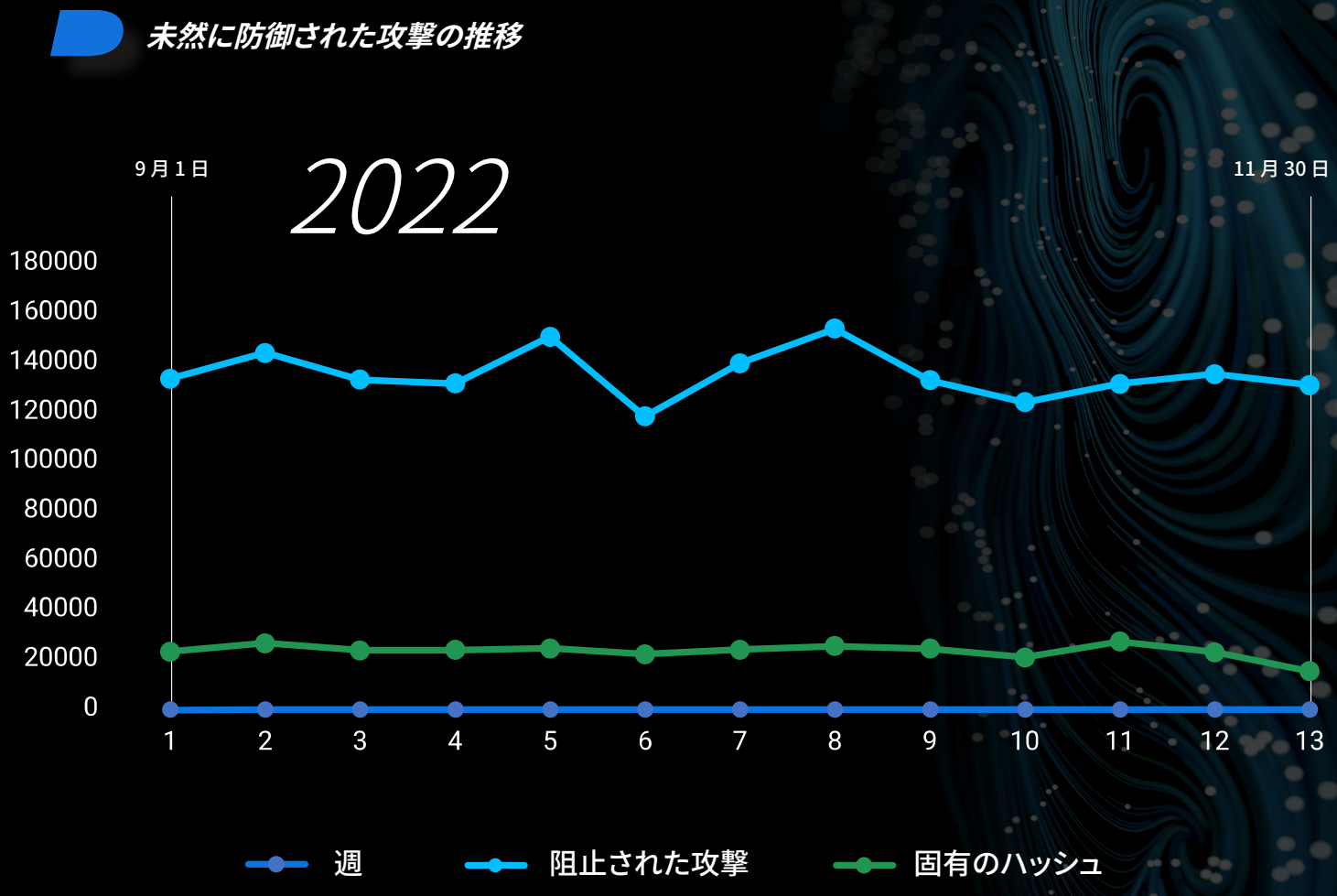


図 1：BlackBerry が未然に防御したサイバー攻撃の件数の推移（2022 年 9 月 1 日～ 11 月 30 日、週単位）

CYLANCE ENDPOINT SECURITY ソリューションが未然に防御した攻撃の地理的分布

一般に、最も多く脅威に遭遇しているのは、インターネット普及率が高く、経済規模が大きく、人口が多い国です。BlackBerry のテレメトリでは、調査期間中に脅威アクターが全世界の BlackBerry クライアントを標的にしていたことが確認されています。

BLACKBERRY がサイバー攻撃を防御したお客様の所在国

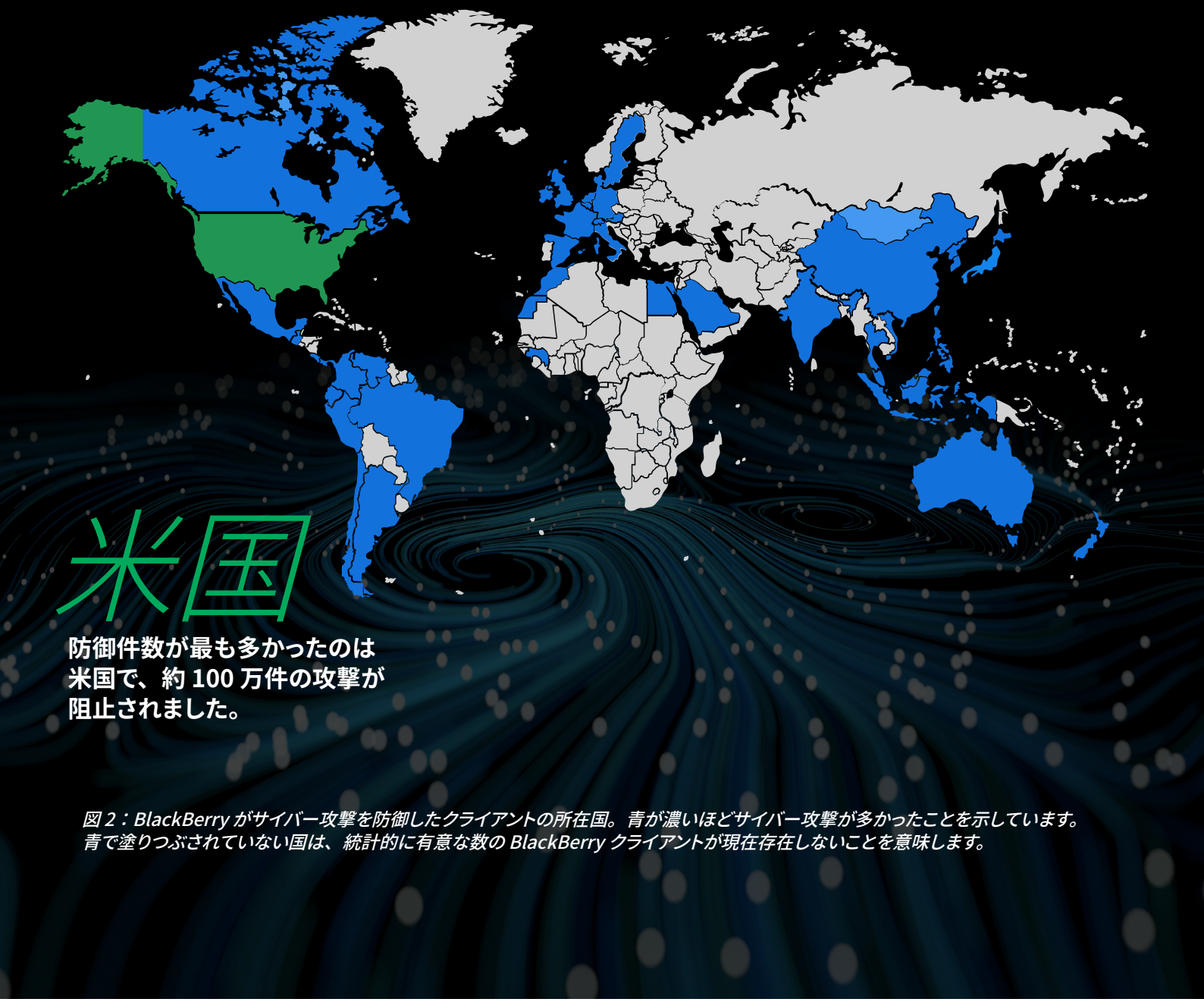


図 2：BlackBerry がサイバー攻撃を防御したクライアントの所在国。青が濃いほどサイバー攻撃が多かったことを示しています。青で塗りつぶされていない国は、統計的に有意な数の BlackBerry クライアントが現在存在しないことを意味します。

図 3 は、CYLANCE ENDPOINT SECURITY ソリューションが未然に防御したサイバー攻撃の数が最も多かった 10 か国を示したものです。

第 4 四半期にサイバー攻撃を受けた上位 10 か国

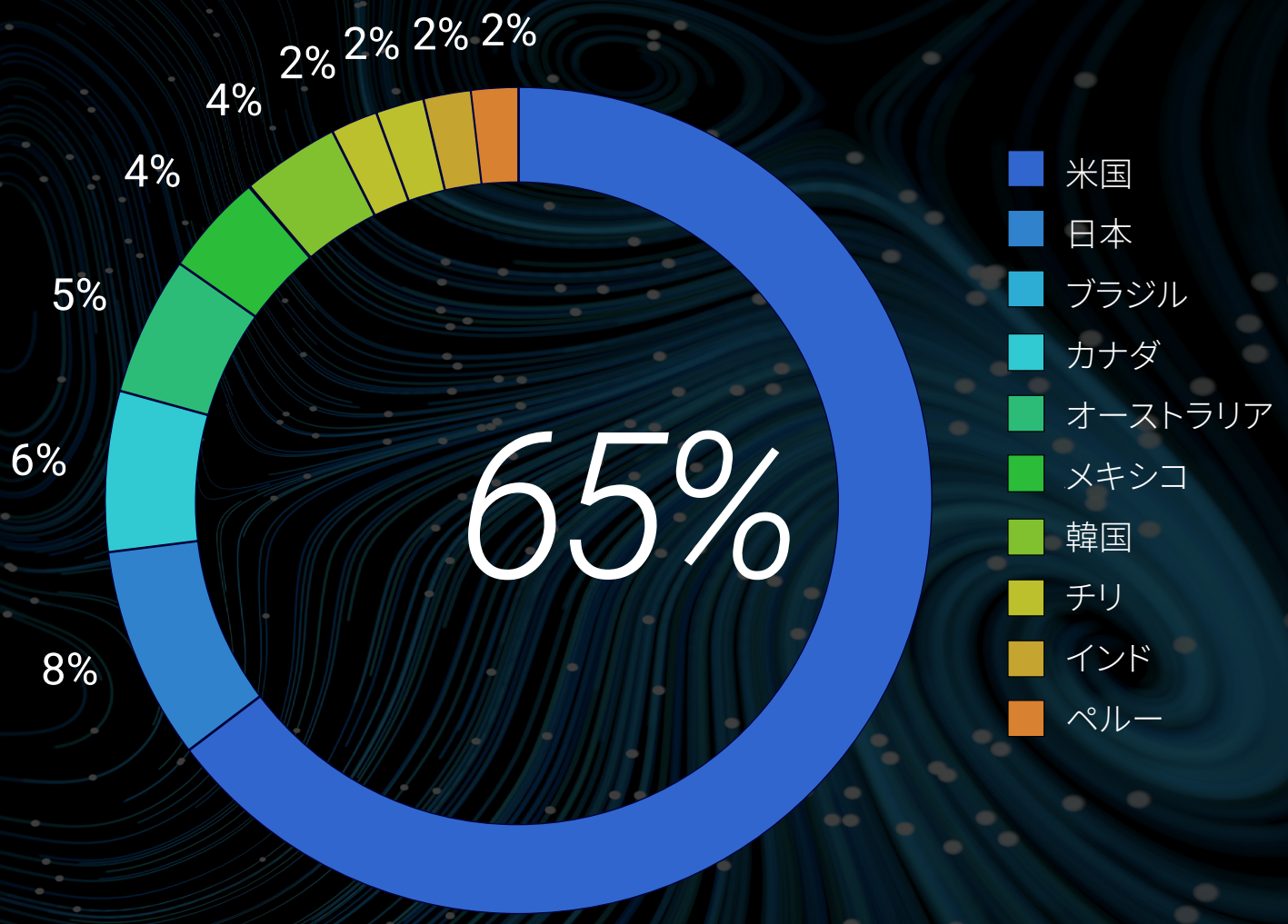


図 3：BlackBerry クライアントがサイバー攻撃の標的にされた上位 10 か国

図 4 は、悪意あるユニークサンプルによる BLACKBERRY クライアントへの攻撃頻度が最も高かった国を示しています。

マルウェアのユニークサンプルが使用された上位 10 か国

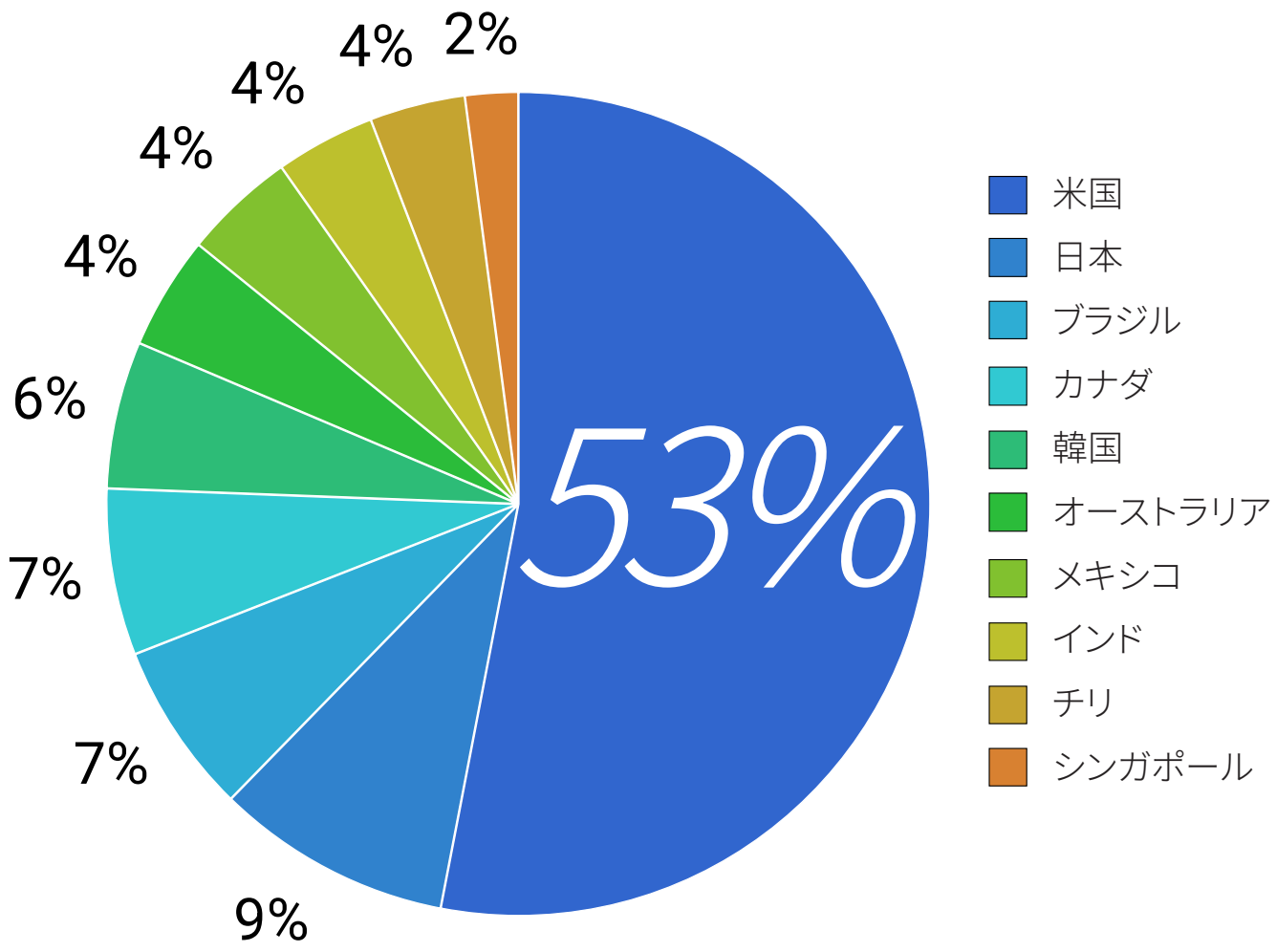


図 4：BlackBerry クライアントへのサイバー攻撃で、悪意あるユニークサンプルが使用された上位 10 か国

調査期間中の攻撃に使用されたマルウェアの種類

2022 年 9 月 1 日～ 11 月 30 日の期間中、脅威アクターは多種多様なマルウェアを駆使して、金銭的、地政学的、軍事的、戦術的な目標の達成を試みました。ここからは、確認されたマルウェアファミリーのうち、最も幅広く使用されたものや注目すべきものを、オペレーティングシステム（OS）ごとに整理して説明します。

重要な指摘としては、最も攻撃されている OS が Windows® であることは変わらないものの、Windows ユーザーは、サイバー攻撃の対象外だと信じているその他の OS のユーザーに比べて、マルウェア攻撃への備えを適切に講じている場合が多いことです。しかし BlackBerry® のテレメトリデータを確認すると macOS®、Linux®、モバイルユーザーも頻繁に攻撃を受けており、どのプラットフォームも感染から無縁だとは言えないことがわかります。

WINDOWS

マルウェアは実行先の OS を選ばないものの、依然として最も多くの攻撃を受けているのが Microsoft® Windows® です。その理由としては、幅広く普及している OS であること、開発者向けドキュメントが充実していること、サイバー犯罪者コミュニティの経験が長年蓄積されていること、各種フォーラムでヒントや手法が活発に共有されていることなどが挙げられます。

ダウンローダ

ダウンローダとは、被害者を誘導することによって自身を開かせた後に、別のマルウェアをダウンロードするファイルのことで、これらの多くは、あたかも正規のデジタル文書や実行ファイルであるかのように偽装しています。一般的なダウンローダには、以下のようなものがあります。

- Emotet：現在使用されているものの中で、最も蔓延している脅威の 1 つです。2014 年に初めて活動が確認され、2021 年 4 月の警察当局による停止措置で息を潜めたものの、2021 年末に復活しました。直近の四半期では、Emotet は 4 か月の空白期間を経て復活しています。使用されている手法は、悪意ある Microsoft® Office ドキュメントを配布するフィッシングキャンペーンなど、以前から確認されているものです。このドキュメントは、Microsoft の公式ディレクトリにドキュメント自身をコピーするよう被害者を誘導し、ユーザーの許可を得ずにマクロを自動実行します。Emotet は、バンキング型トロイの木馬である IcedID をドロップすることで知られています。IcedID は、複数のランサムウェアグループとの強いつながりが確認されています。
- Qakbot：通常は、フィッシングメール経由で感染します。このフィッシングメールには通常ハイパーリンクが含まれており、このリンクから悪意ある Web ページへのリダイレクトが行われ、その Web ページに含まれるパスワード保護された ZIP ファイル内に、ISO ファイルが格納されています。この LNK ファイルは JavaScript ファイルを実行し、この JavaScript ファイルが、.DAT 拡張子を持つ悪意ある Qakbot の DLL を実行します。Qakbot の注目すべき特徴は、伝播の手段として既存のメールスレッドを使用することです。受信者への返信機能を使用することで、標的となる被害者に、既存のメールスレッドに登場したリンクや添付ファイルが、信頼できる送信元から送られていると信じさせることができます。Qakbot は数多くのランサムウェアグループで頻繁に使用されており、直近の四半期では、米国拠点の企業を 2022 年に相次いで狙った、Conti のリブランドが疑われる Black Basta との関連が確認されています。

- GuLoader：リモートから実行ファイルをダウンロードして実行します。主に Redline や Raccoon などのインフォスティーラをダウンロードして実行することが知られています。GuLoader は通常 Google Cloud™ や OneDrive® などのクラウドベースサービスにペイロードをアップロードしています。また、BlackBerry が検知した GuLoader のうち Telegram ボットを使用していた例もあります。

ランサムウェア

LockBit：2022 年も引き続き最も活発で成功を収めた RaaS（Ransomware-as-a-Service）です。90 日という本レポートの対象期間において、この脅威グループが停滞している兆候は確認されませんでした。LockBit は進化を続けており、現在のバージョン 3.0 には、解析を困難にする複数のアンチデバッグ手法や、現在停止中の BlackMatter ランサムウェアから流用した文字列暗号化などの手法が採用されています。

インフォスティーラ

コロナウイルスの影響によりリモートワークやハイブリッドワークが増加したことで、内部ネットワークに外部からアクセスするニーズはますます高まっています。攻撃者は、こうしたリモートアクセス認証の拡大にすばやくつけ込みました。企業の機密情報を窃取し、闇市場で販売するために、以前はサイバー詐欺に多く使用されていた情報窃取型マルウェア（インフォスティーラ）を採用したのです。多くの場合、窃取された認証情報を初期アクセスブローカー（IAB）やランサムウェア作戦のアフィリエイトが悪用することで、情報が流出した組織のネットワークへの侵入やランサムウェアの展開が行われます。

今回の調査期間中に確認されたインフォスティーラには以下のようなものがあります。

- Redline：確認されている中では、最も活発かつ広範にわたり使用されているインフォスティーラです。Redline は、ブラウザー、暗号資産ウォレット、FTP、仮想プライベートネットワーク（VPN）ソフトウェアなど、さまざまな標的から認証情報を窃取する能力を備えています。
- Raccoon インフォスティーラは MaaS（Malware-as-a-Service）として機能し、新人のサイバー犯罪者でも月 100 ドルという低価格で強力な機能を使用できます。Raccoon は Redline ほど広く展開されていない

REDLINE

ブラウザー、暗号資産ウォレット、FTP、仮想プライベートネットワーク（VPN）ソフトウェアなど、さまざまな標的から認証情報を窃取する能力を備えています。

ものの、依然として有力な脅威と見なされています。BlackBerry では、最初に感染した Redline によって Raccoon がドロップされた例を複数検知しています。Raccoon は、暗号資産ウォレット、ブラウザー拡張機能、Discord、Telegram から認証情報を窃取し、スクリーンショットを撮影します。また、ローダーの役割も担い、追加のペイロードを起動できます。

2022 年 9 月に発生した脅威アクターによる Uber の侵害[1] では、その攻撃に Lapsus$ グループが関わっていると発表されました。このインシデントでは Uber が迅速に対処して攻撃を停止させたため、ランサムウェアは展開されていません。

ファイル感染型ウイルス

ファイル感染型ウイルスは、別の実行ファイルに感染することで動作し、ネットワーク共有やリムーバブルデバイスを通じて拡散します。2003 年に初めて確認され、20 年後の現在も確認されているファイル感染型ウイルスが Neshta です。Neshta は、BlackPOS と呼ばれる POS（Point-Of-Sale）マルウェアとの関連が以前から指摘されています。BlackPOS は、消費財、エネルギー、金融、製造といった業界を狙った 2018 年の攻撃で非常に多く使用された、POS システムからクレジットカードデータを抜き取るマルウェアです。BlackBerry では、Neshta に関する詳細なレポートを 2019 年に発表し、その後も同種のトラフィックを毎年確認しています。

リモートアクセス型トロイの木馬

リモートアクセス型トロイの木馬（RAT）は、キーボード入力の記録、感染した端末の Web カメラへのアクセス、ブラウザーの認証情報を窃取、さらに感染したデバイスやネットワーク内のその他のコンピューター上でさまざまなプログラムの実行を可能にします。今回の調査期間中に確認された RAT には以下のようなものがあります。

- njRAT：2015 年に初めて確認され、現在も使用されている最も有力な RAT の 1 つです。njRAT は、金銭を目的とする脅威アクターに加えて、標的型攻撃の場合により多く使用されています。njRAT ビルダーは幅広く入手可能で、脅威アクターが必要としている攻撃モデルに容易に適合させることができます。中東の脅威アクターに多く使用されており、BlackBerry 独自のテレメトリから特定された njRAT のインスタンスにも、ヨルダンで活動しているコマンドアンドコントロール（C2）サーバーが関連付けられたものがありました。
- FlawedAmmyy：2018 年に登場した FlawedAmmyy は、Ammyy Admin の流出したソースコードを基盤に開発されています。Ammyy Admin は、Microsoft Windows マシンのリモートコントロールや診断を行うために企業や消費者が使用する、正規のリモートアクセスツールです。FlawedAmmyy は主にサイバー犯罪グループ TA505（ランサムウェア作戦に独自の Cl0p ランサムウェアを使用することで知られる）との関連が指摘されていますが、複数のサイバー犯罪脅威アクターに広く使用されていることも確認されています。

BLACKBERRY のリサーチャーによれば、MACOS を使用しているお客様のうち

34%

もの組織が DOCK2MASTER をネットワーク上で使用しており、組織が所有するデバイスの 26% で DOCK2MASTER が発見されたとのことです。

MACOS/OSX

macOS は、最も普及している企業向けプラットフォームではないものの、インストールされる企業システムの数は増え続けています[2]。macOS は Windows との比較で「より安全性が高い」プラットフォームという評価を得ているものの、macOS がマルウェアや脆弱性と完全に無縁というわけではありません。

アドウェア / スパイウェア

macOS に影響を与える脅威の中で、圧倒的に多く確認されているのがアドウェアとスパイウェアです。これらのアプリケーションは正規のソフトウェアを偽装していますが、その隠された目的はユーザーを利用することにあります。標的型攻撃を通して脅威がコンピューターに展開される場合とは異なり、アドウェアやスパイウェアの場合、それらを正規のアプリケーションだと信じ込んだ多くのユーザーが、その危険性に気付かずに（多くは無償で）インストールしています。90 日の調査期間中 macOS で最も多く確認

された脅威は、悪意あるアプリケーション Dock2Master でした。BlackBerry のリサーチャーによれば、macOS を使用しているお客様のうち 34% もの組織が Dock2Master をネットワーク上で使用しており、組織が所有するデバイスの 26% で Dock2Master が発見されたとのことです。ユーザーが訪問する Web ページに密かに広告を直接挿入し、ユーザーとシステムのデータを収集し、闇市場で販売する Dock2Master は、望ましくない可能性があるアプリケーション（PUA）として公式に指定されています。

ブラウザーハイジャッカー

ブラウザーの検索エンジンを変更したり、その他のブラウザーの設定を変更したりするブラウザーハイジャッカーは、2000 年代前半ほどの勢いはないものの、現在も数多く存在が確認されています。ブラウザーがハイジャックされた場合の最も顕著な影響は、デフォルトの検索エンジンがユーザーの同意なく変更されることですが、それ以外にも、ブラウザーに保存されているユーザーの ID 情報の窃取や、表示された Web ページへの広告の挿入などによって、インストールされたブラウザーハイジャッカーからの収益化が行われる場合があります。直近の四半期で活動が確認されたブラウザーハイジャッカーには OriginalModule があります。その他、InstallCore を使用して複数のプラットフォームを標的にする SearchInstaller も確認されました。

プロキシマルウェアとプロキシエージェント

プロキシマルウェアは、感染したシステムをプロキシサーバーに変え、ユーザーの代わりに攻撃者によるアクションの実行を可能にするトロイの木馬の一種です。プロキシエージェントは、プロキシマルウェアであると同時に、感染したマシン上でローカルコマンドを実行するといった RAT と同様の追加機能を備えています。プロキシマルウェアは、その他のマルウェアに比べてサポートする機能が少ない傾向にあり、必要とするライブラリの数も少なくなるため、標的となる被害者の範囲は広くなります。この種のマルウェアではかなりの確率で Go 言語 プログラミング言語が使用されています。これは、Proxit などのプロキシライブラリをサポートしていることで、新人のサイバー犯罪者でも簡単に開発できるためです。

BlackBerry では、悪意あるスパム（マルスパム）のようなクロスプラットフォーム攻撃の一環において macOS システムを標的とする場合、Go 言語を採用する例が増えていることに注目しています。これらの攻撃を複数のプラットフォームで効果的に動作させるには、すべてのプラットフォームに存在するシンプルな機能を利用する必要があります。確認されたプロキシマルウェアのサンプルの大半は、複数のプラットフォーム向けに提供されているブラウザーを攻撃するプロキシエージェントでした。

LINUX

Linux は、高性能でありながら柔軟性を備えた、あらゆる場所で活躍するオープンソースオペレーティングシステムです。実際、パブリッククラウドサービスの 90% 以上が Linux 上で稼働しています[3]。その結果 Linux は、ベンダーその他の業界関係者が公開した弱点や脆弱性をすばやく武器化して悪用するサイバー犯罪者にとっても魅力的なターゲットとなっています。

ボットとボットネット

ボットとは、人間の介入なしにコマンドを実行する自律的プログラムを意味し、ボットネットとは、1 つの脅威アクターが制御するボットのグループを意味します。通常ボットネットは、構成上の不備やパッチ未適用の脆弱性を利用し、セキュリティ上の欠陥があるコンピューターに悪意あるコードをインストールして、被害者のコンピューターをボットネットに追加します。今も悪名高い Mirai ボットネットワークが 2016 年に登場し、大規模な分散型サービス妨害（DDoS）攻撃を展開して以来、さらに数多くの Linux ボットネットが出現しています。

ブルートフォース戦術を使用し、構成上の不備やデフォルトの認証情報を悪用してシステムに侵入する、ShellBot をはじめとする有名なインターネットリレーチャット（IRC）ボットネットは、2022 年末時点でも確認されています。[4] また、リモートコード実行（RCE）の脆弱性[5] CVE-2022-22947[6] を悪用してシステムに侵入し、ボットネットの規模を拡大する Sysrv ボットネットも確認されています。

マルウェアとツール

今回の調査期間中、BlackBerry が確認および特定したマルウェアと悪意あるツールは他にもあります。SSH ツール（セキュアシェルプロトコルに基づき、リモートアクセスを可能にする）は、認証情報のブルートフォースやネットワークのスキャンによる横展開の可能性を探るために、多くは悪意あるコードと組み合わせて使用されます。90 日の調査期間中、FTL（Faster than Lite）ツールの使用が増加しました。このツールは主に脅威グループ OutLaw[7] が頻繁に悪用しており、ShellBot にバンドルされていることが指摘されています。

BlackBerry のテレメトリでは、横展開を行う手段として Go 言語 ベースの SSH ブルートフォースツール Spirit を悪用する同様のキャンペーンを観測しています。Spirit は通常、Pwnrig や Tsunami などの IRC ボットと共にドロップされます。BlackBerry ではさまざまな感染の痕跡から、これらのボットはハッキンググループ 8220 Gang によるものだと強く確信しています。

現在広く知られるようになった Log4j の脆弱性は、今回の調査期間中も、さまざまなマルウェアファミリーや脅威アクターによって頻繁に悪用されています。たとえばトロイの木馬 Kinsing は、Java Log4j パッケージの脆弱性 [8] CVE-2021-44228[9] を悪用して Linux プラットフォームで RCE を実行しています。さらに最近では、Oracle WebLogic Server の脆弱性 [10] CVE-2020-14882[11] を悪用していることも確認されています。このトロイの木馬は、デバイスのセキュリティエージェントとクラウドサービスエージェントを無効化し、被害者のシステムに侵入済みの競合するマルウェアや暗号資産マイナー（クリプトマイナー）を停止した後に、独自のクリプトマイナーを実行します。

クリプトマイナーとクリプトジャッキング

クリプトジャッキングとは、脅威アクターが被害者のデバイスに悪意ある暗号通貨マイニングソフトウェアをインストールし、ユーザーの同意なく暗号通貨コインを採掘する、広く普及している攻撃の 1 つです。クリプトマイナーは、過去 10 年にわたってサイバー脅威環境から消えることなく被害を生み出し続けています。あらゆる主要コンピューティングシステムに影響を与えるクリプトマイナーは、発見されるまでに長い時間を要することがあります。

調査期間中は暗号通貨全体で価値の低下が見られたものの、クリプトマイナーが大規模に展開されることは、脅威アクターに莫大な金銭的利益がもたらされることを意味します。市場の動きとは関係なく、こうした Linux ベースの脅威アクターの大部分にとって、暗号通貨を狙うことは依然として王道のやり方です。

直近の四半期では、Linux デバイスを標的とした脅威のうち、かなりの割合をクリプトマイナーが占めています。暗号通貨の採掘はますます多くのリソースを必要とするようになっており、それに合わせてコストも上昇しています。そのため攻撃者は、こうした問題を解決するために、数多くの被害者の環境に侵入し、マイナーを展開して、コンピューティングリソースを盗用するようになりました。前述の ShellBot と Sysrv ボットは、いずれもシステムに侵入して

直近の四半期では、LINUX デバイスを標的とした脅威のかなりの割合をクリプトマイナーが占めています。

クリプトマイナーを展開し、システムリソースを乗っ取るものです。

通常、侵害後の被害者の環境にクリプトマイナーが侵入する場合、ドロップされたペイロードを使用するか、PwnRig クリプトマイナーで多く確認されているように [12]、CVE-2022-26134[13]（Atlassian Confluence）や CVE-2019-2725[14]（WebLogic）などの脆弱性を悪用します。クリプトマイナーは、cron ジョブ（特定の時間にプログラムを実行することを予約する機能）などの標準のバックグラウンドリソースに潜伏し、可能な限り長い間検知から逃れようとします。

直近の四半期では、CryptoNight 関連での検知が行われる例が確認されています。CryptoNight は、Monero や Webchain など一部の暗号通貨で、ネットワークの安全確保や取引の検証に使用されるマイニングアルゴリズムです。また、Webchain マイナーや、いくつかの XMRig ベースのマイナーの利用急増も確認されています。XMRig は、Bitcoin や Monero などの暗号通貨のマイニングで多く使用されるオープンソースのユーティリティで、現在、脅威アクターが頻繁に悪用するコインマイナーの 1 つです。

モバイルデバイス

モバイルデバイスは、オンラインバンキング、モバイル決済、メッセージングアプリ、ソーシャルネットワークなど、ラップトップやデスクトップのコンピューターを置き換える機能を数多く提供し続けています。実際、2022 年のすべてのインターネットトラフィックの 59.54% はモバイルデバイスから生まれています [15]。

Android

2022 年は、全世界のモバイルデバイスの約 71% が Android™ オペレーティングシステムを採用しています。今回の調査期間中に確認された脅威には以下のようなものがあります。

- Lotoor：適切な目的と有害な目的の両方に使用できるツールです。Android の所有者は、デバイスのルート化や追加機能のロック解除に Lotoor を使用できる一方で、Google が搭載したセキュリティ機能の回避や、永続的マルウェアの埋め込みにも、このツールを使用できます。
- AdvLibrary：感染したデバイスに未承諾広告を表示し、有料広告の発信トラフィックを発生させることで、インターネットトラフィックによる収益化を図ります。被害者が直接、金銭的損失を被ることは通常ありませんが、データトラフィックの増加に伴う追加費用が発生する場合があります。サイバー犯罪者には、広告のクリックや広告の対象となる悪意あるサイトへのトラフィックが発生することで、AdvLibrary による収益が発生します。

iOS

一般には、iOS® はその他のモバイル OS に比べて安全性が高いと考えられています。iOS のゼロデイ攻撃はコストが高く、無秩序な攻撃に使われることはほとんどありませんが、iOS は、iPhone® デバイスを「脱獄」あるいはロック解除する攻撃と無縁ではありません。これは、Apple® 本来のセキュリティ機能を削除し、デバイスへの完全なアクセスを可能にする、危険性を高める行為です。iPhone 所有者によっては、不要なデフォルトアプリを削除するなどの目的で意図的に iPhone を脱獄することがありますが、脱獄した iPhone は攻撃に対して脆弱な状態です。

さまざまなレベルの脅威アクターが、iPhone の脱獄を利用して被害者のデバイスにマルウェアをインストールします。たとえば、iOS ユーザーを標的とした潜在的な悪意あるマルウェアのファミリーに Vortex があります。Vortex は、Android 向けの Lotoor に似た、iPhone の脱獄を可能にするツールです。サイバー犯罪者は、これをマルウェアのインストールに使用します。この手法は、ゼロデイ脅威を仕掛ける技術的能力を持たない中堅レベルの脅威アクターの間で最も一般的で、BlackBerry では、iOS デバイスの脱獄を目的とした Vortex を、直近の四半期で少なくとも 2 バージョン確認しています。

業界ごとに特化した攻撃

サイバー攻撃の標的になる可能性はどの業界にもありますが、自動車業界、医療業界、金融業界のそれぞれが抱えている、サイバー犯罪者側から見たチャンスを確認していきましょう。

自動車

100 年の歴史を持つ自動車業界では、今後を左右するような技術革新が今まさに進行中です。技術の飛躍的な進化により、新しい種類の自動車、システム、サービスの開発が実現しています。このようなデジタルトランスフォーメーションは数多くのメリットをもたらす一方で、サイバーセキュリティの新たな課題も生じさせています。

自動車が常時接続するようになり、自律性がさらに高まるに従って、サイバー脅威や脅威アクターに対する脆弱性も高まっている可能性があります。さらに、自動車製造のシステムがますます複雑化していることも、サイバー攻撃のリスクを高めています。

これまでの自動車業界は、大規模な脅威が注目を集めているときも、その影響を比較的受けずに済んでいました。しかし現在は、数々の悪意ある組織が、自動車メーカーだけでなく業界全体をターゲットに、操業の停止、機密データの窃取、サプライチェーンへの侵入を試みるようになっています。BlackBerry では、自動車業界を標的とする悪意ある組織の数や、そうした組織が業務に支障を生じさせている例が 2022 年に増加していることを確認しています。

こうした脅威から自動車とドライバーの両方を保護するために、自動車業界の各企業がコネクテッドカーにおける潜在的なリスクを把握し、厳格なサイバーセキュリティ対策を施していく必要があります。

最近の脅威の傾向

自動車業界はグローバル規模で広がっているため、監視および保護すべきエンドポイントも膨大な数になります。この業界は、製造用の材料を調達する企業から、自動車販売店、自動車の所有者まで、バリューチェーンのあらゆる組織で構成されています。この重要なグローバルビジネスを適切に運用し続けるには、複雑なサプライチェーンに伴う、非常に広い範囲のデジタル攻撃対象領域を保護する必要があります。

2022 年 9 月 1 日～ 11 月 30 日の期間中に行われた攻撃は、高度なスピアフィッシングからコモディティ化したマルスパムまで多岐にわたります。これは、高度なサイバー攻撃者と新人のサイバー攻撃者の両方が、自動車業界を常に標的にしていることの表れです。

ダウンローダ

ダウンローダマルウェアは、ほぼすべての種類のサイバー攻撃で広く確認されていますが、その外観、ファイルの種類、システムへの侵入手法の相対的な洗練度は、さまざまに異なります。悪意ある脅威アクターは、サイバー攻撃の最初の段階として、何も知らない被害者を誘導してこのダウンローダをインストールさせます。コードが実行されたら、ダウンローダはさらに悪質なコードとペイロードをインストールして、より広範なサイバー攻撃を実行します。

GuLoader：今回の調査期間中に確認された、自動車業界を標的とするダウンローダの代表的な例です。このマルウェアは 2019 年に初めて確認され、現在も進化を続けています。GuLoader の多くは、正規のデジタル文書や実行ファイルを偽装して、別のコモディティマルウェアをダウンロードします。

インフォスティーラ

高価値で独占所有権のあるデータを取り扱う自動車業界は、窃盗を目的とするサイバー犯罪者にとって格好の標的です。またこれらのデータの商品価値が車両本体よりも高くなることは珍しくありません。

インフォスティーラマルウェアは、金銭的目標や戦術的な目標の達成に役立つデータを、被害者のシステムから探索して不正に抜き出す、悪意あるコードの一種です。インフォスティーラを Remcos などの RAT と組み合わせることで、コモディティマルウェアとして使用することが可能になります。このマルウェアが、被害者のシステムのアクセスと制御を不正に乗っ取るためのサービスとして、その他の脅威アクターに販売されることもよくあります。

ランサムウェア

ランサムウェアはあらゆるセキュリティチームが最も避けたい脅威であり、自動車業界のサプライチェーンを狙うランサムウェアが壊滅的な被害につながることは脅威アクターも認識しています。自動車業界でランサムウェアの攻撃が発生した場合、サプライチェーンのどの段階で攻撃を受けたとしても、製造と流通が停止し、自動車業界のエコシステム全体の収益と信用が低下することにつながりかねません。

BlackCat：2022 年を通じて確認された RaaS で、特に悪名高いランサムウェア攻撃のいくつかでこの BlackCat が使用されています。BlackCat の標的には中小企業が選ばれることが多く、BlackCat を使用するサイバー犯罪グループは、主に金銭的な動機から、製造業を中心に攻撃を行う傾向があります。BlackCat ランサムウェアは、環境に侵入し、貴重なデータを抜き出した後、接続された複数のシステムを暗号化します。

48%

の盗難自動車にキーレス技術が搭載されていたことが判明しています。

ALPVH（BlackCat ランサムウェアの背後にいる脅威グループ）が頻繁に使用するのが二重脅迫の手口です。侵害された被害者のデータを、リークサイト（窃取された個人情報や機密性が高いと思われる文書を公開する Web サイト）を通じて公開してしまうのです。その目的は、さらに価値の高いデータが今後公開されたり競合他社に売却されたりすることへの恐怖を利用して、侵害を受けた組織に身代金支払いのプレッシャーを与えることにあります[16]。

デュアルユースツール

一般にデュアルユースアプリケーションとは、脅威アクターによって悪用または乱用されうる性能や機能を備えた、正規のツールやソフトウェアを意味します。正規のツールを悪用してセキュリティシステムを迂回して検知を回避する脅威アクターの行為は、「環境寄生型（LotL）」という用語で呼ばれます。

脅威アクターが侵害した環境内で横展開し、貴重なデータを抜き出し、「許可済みの」ツールとしてマルウェアを利用する場合でさえ、悪意あるコードの代わりにデュアルユースツールに頼る例は増え続けています。システム管理者は、有効なユースケースやビジネス上の正当性がないデュアルユースツールをすべて削除する必要があります。

自動車業界が直面している脅威の全体像

現代の自動車には「スマート」機能やインターネット接続機能が数多く搭載されています。さらには新機能の受信や管理にソフトウェアアップデートを使用するソフトウェア定義型車両（SDV）も登場し、脅威アクターの攻撃対象としての自動車の魅力はますます高まっています。実際、コネクテッドカーの走行台数は 2023 年までに 7 億 7,500 万台に達するという試算があります[17]。一方の攻撃者は、生産、製造、出荷、販売のあらゆる段階でいかなる種類の混乱も許されないことを熟知しているため、サイバー攻撃の試行回数は増加すると予測されます。

ここ数年は自動車に対する各種の直接攻撃が確認されており、特にキーレスエントリー対応車両の脆弱性の高さが指摘されています。英国を拠点とする保険会社 LV= General Insurance のデータによると、盗難被害にあった自動車の 48% にキーレス技術が搭載されていたことが判明しています[18]。ユーロポールは 2022 年 10 月、不正ソフトウェアを使用して物理的なリモコンキーを持たない車両を

盗んでいた、キーレスエントリー自動車およびキーレススタート自動車専門のヨーロッパの自動車盗難グループを解体に追い込んだことを発表しました[19]（発表は、このエクスプロイトが報告され、パッチが適用された後に行われています）。

過去 5 年間を総合的に振り返ると、データ漏洩、ランサムウェア、持続的標的型攻撃（APT: Advanced Persistent Threat）グループによる攻撃など、自動車業界はほぼ途切れなくサイバー攻撃に悩まされ続けてきたといえます。脅威の数は 2022 年に急増しましたが、新車への組み込み技術が普及したこともあり、その勢いは今後も続くと考えられます。たとえば 2017 年にはある自動車メーカーがランサムウェア WannaCry の被害を受け[20]、一時的に製造停止に追い込まれました。2019 年には、複数の情報筋によりベトナムの自動車業界の支援勢力との関連が指摘されている[21]、APT32（別名 OceanLotus）というグループが登場しています[22]。このグループは、その他の自動車メーカーのネットワークを標的とする侵害行為を行っています[23]。攻撃の件数は 2020 年～ 2022 年にかけて増加しています。攻撃の大半はランサムウェアが占めており、2022 年に注目を集めた例だけでも、ヨーロッパ最大規模の自動車ディーラー[24]、オランダの特殊車両メーカー[25]、米国のタイヤメーカー[26] がランサムウェア攻撃の被害にあっています。

以下の図は、2022 年に自動車業界で報告された大規模な攻撃の例を時系列で示したものです。

2022 年に発生した自動車業界への大規模な攻撃

図 5：2022 年に発生した自動車業界への大規模攻撃のタイムライン

サプライチェーン攻撃

コロナウイルスの蔓延、そしてロシアによるウクライナ侵攻が明らかにしたのは、サプライチェーンがいかに脆弱であるかということです。自動車業界も、その他の業界が直面する遅延、欠品、混乱と無縁ではいられません。

自動車業界の複雑さを知る数多くの企業が、ジャストインタイム（JIT）サプライチェーン戦略を採用して、複数のベンダー、部品、メーカーで構成される巨大なエコシステムを維持しています。同時にこのことによって、脅威アクターに悪用されうる攻撃対象はかなり大きな範囲に広がっています。JIT 戦略の特性は、必要とされて初めて製品が製造されることです。つまり必要な部品や材料がすぐに調達できなければ、製造工程に遅延や停止が発生する可能性があります。これは、サプライチェーン内部でサイバー攻撃の被害が発生すると、自動車生産が事実上停止することを意味します。

悪意ある敵対者は、侵入への厳重な防御が講じられている自動車メーカーを直接狙うのではなく、特にサイバーセキュリティが弱い会社を中心に、自動車メーカー傘下のさまざまなベンダーを攻撃することがあります。たとえば 2022 年 3 月には、プラスチックや電子部品のサプライヤー企業のファイルシステムが侵害されたことで、日本のある自動車メーカーにおいて推定 1 万 3,000 台の製造工程に遅延が発生しました。Automotive News Europe に引用された広報担当者の説明によると、この自動車会社のサプライチェーンには、4 つの階層にわたり 6 万 社もの企業が含まれているとのことです [27]。これほどの規模のサプライチェーンでは、たった一部分にサイバー攻撃を受けただけで、その他の企業が必要とする部品や材料の提供に影響が生じる可能性があります。

今後の展望

これまで説明してきたように、複雑に拡大したサプライチェーンとビジネスエコシステムを擁する自動車業界は、サイバー攻撃にとって魅力的なターゲットとなっています。しかし自動車業界では、より強力なセキュリティとレジリエンスの構築に向けた取り組みが進められています。2022 年、スウェーデンの国営研究機関 RISE は、自動車サイバーセキュリティ専門の RISE Cyber Test Lab の創設を発表しました。この組織は、ヨーロッパにおける自動車サイバーセキュリティの最先端ハブになることを目指し、2023 年には本格的なテストを開始する予定です。また、NHTSA が提唱する最先端車両の安全確保に向けたサイバーセキュリティベストプラクティスでは、2022 年の改訂版において、車両ライフサイクル全体にわたるサイバーリスクの防御、検知、対処に、自動車メーカーとサプライヤーが協力して取り組むことを強く推奨しています [28]。このガイダンスは、自動車サイバーセキュリティエンジニアリングのグローバル規格である ISO/SAE 21434 に基づいています。

医療

医療機関の機密データや高価値な情報が脅威アクターに狙われる医療業界では、直面するサイバー脅威の数は増え続けています。このことは医療機関にとって重大な問題です。サイバー攻撃が成功すれば、患者の機密データの損失や開示、金銭的損失、さらには患者に対する直接的物理的な被害など、深刻な影響をもたらす可能性があります。耐用年数の長い医療技術が至るところで使用され、複雑で相互に入り組んだ医療システムが稼働し、膨大な量の機密データの収集と保存を日々繰り返している医療業界は、これらの脅威に対して特に脆弱な状態にあります。現在のサイバー脅威環境の危険性を理解し、潜在的な被害から組織と患者を事前対応的に保護することが医療機関には欠かせません。

全体的に見ると、医療業界にとって最大の脅威がランサムウェアであることは変わりません。ランサムウェアを利用する脅威グループは依然として活発に医療機関を攻撃しています。10 月には CommonSpirit Health がランサムウェア攻撃を受け、60 万人を超える患者のデータが漏洩しました [29]。過去には、病院に対する攻撃を行わないことを表明した Maze のような RaaS グループもありましたが、そうした約束が守られる保証はありません。さまざまな RaaS グループが数多く存在し、またアフィリエイトモデルが一般的になっていることから、攻撃実行グループとマルウェア開発グループが同一でない場合も多く、追跡と特定は簡単ではありません。

今回の調査期間における BlackBerry のテレメトリによると、Cylance Endpoint Security ソリューションは、医療業界を狙うマルウェアのユニークサンプルを 7,748 件阻止しています。これは 1 日あたり平均 80 件以上のユニークサンプルが阻止されていることになります。最も使用されて

60 万人

を超える患者のデータ漏洩が、COMMONSPIRIT HEALTH に対する 10 月のランサムウェア攻撃で発生しました。

いるトロイの木馬は Qakbot でした。サイバー犯罪者が少なくとも 2012 年から使用している Qakbot は、医療業界にとって大きなリスクをもたらす存在です。2022 年における Qakbot の使用は、Black Basta ランサムウェアの展開を試みるアフィリエイトによるものが大半を占めています。Emotet は、最近の 4 か月の空白期間以降はそれほど多くのキャンペーンで利用されておらず、TrickBot は Bumblebee マルウェアの改良を優先していると見られています。RaaS アフィリエイトや IAB による医療ネットワークへのアクセスを可能にするトロイの木馬として Qakbot が依然として最も活発に利用されている背景には、こうした事情があると考えられます。

今回の調査期間では、Meterpreter（攻撃者にインタラクティブシェルを提供する Metasploit ペイロード）と BloodHound も活発な活動が確認されました。たとえば BlackBerry が検知した攻撃では、SharpHound（攻撃後のネットワーク内部における横展開で多く使用される BloodHound のコレクター）の実行と同時に Meterpreter が使用されていました。サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）は、ネットワーク管理者やシステム管理者自身で故意に BloodHound を実行し、現在の環境における潜在的な攻撃経路を把握することを推奨しています[30]。

BlackBerry では、TinyNuke が Netwire RAT をドロップする行為も確認しています。ZeuS と同様の機能を持つバンキング型トロイの木馬として登場した TinyNuke は、現在では VNC サーバーデバイスコントローラやリバース SOCKS の機能を備えた、フル機能のトロイの木馬に進化しています。Kimsuky Group による使用も確認されている[31] TinyNuke の背後には朝鮮民主主義人民共和国（DPRK）があると言われています。この攻撃を調査した BlackBerry は、TinyNuke が Netwire RAT をダウンロードして実行し、多くの RAT が使用する DuckDNS がホストするドメインへの接続が行われていることを突き止めています。

BlackBerry のリサーチャーは、通常は Mustang Panda を含む複数の国家支援の脅威アクターが使用する PlugX RAT を、未知の脅威アクターが展開した事例も確認しています（詳細については BlackBerry の公開レポートを参照）。これは、医療業界に対する攻撃が、純粋なサイバー犯罪者と国家支援の脅威アクターの両方にとって魅力的であることを意味します。また、Redline や Raccoon などのインフォスティーラで特に医療業界を狙ったものは確認されていませんが、サイバー犯罪者によるインフォスティーラの展開に多く利用される GuLoader ダウンローダは確認されています。

金融業界

これまで金融業界は、金融制裁の対象地域を拠点とするサイバー犯罪者や国家支援の脅威アクターに狙われてきました。今回の 90 日の調査期間では、金融業界を標的に利用されたマルウェアのユニークサンプル 9,721 件を Cylance Endpoint Security ソリューションが阻止しています。つまり 1 日あたり平均約 108 件の悪意あるユニークサンプルが検知されたことになります。

国家支援の脅威アクターを含むさまざまな脅威アクターは、Cobalt Strike をはじめとする商用のペネトレーションテスト（ペンテスト）ツールを利用します。このため、

これらの攻撃がサイバー犯罪者によるものか正当なテスト作業によるものかを判断するのが難しくなっています。アクセスを奪取したサイバー犯罪者は、この混乱に乗じて、より多くの時間をかけてネットワーク内で活動できます。BlackBerry は 2022 年、商用の攻撃者シミュレーションソフトウェア（Cobalt Strike など）とペンテストソフトウェア（Metasploit、Mimikatz、Brute Ratel）が金融機関内部で使用された例を複数確認しています。Brute Ratel は敵対的攻撃のシミュレーションツールです。Mimikatz は、パスワードや認証情報などの機密情報をシステムメモリから抽出する目的で、攻撃者とセキュリティ専門家の両方に使用されています。現時点では、Mimikatz や Brute Ratel が存在するだけでは、ある攻撃が正当なペンテスト活動によるものか、実際の攻撃によるものかは区別できません。

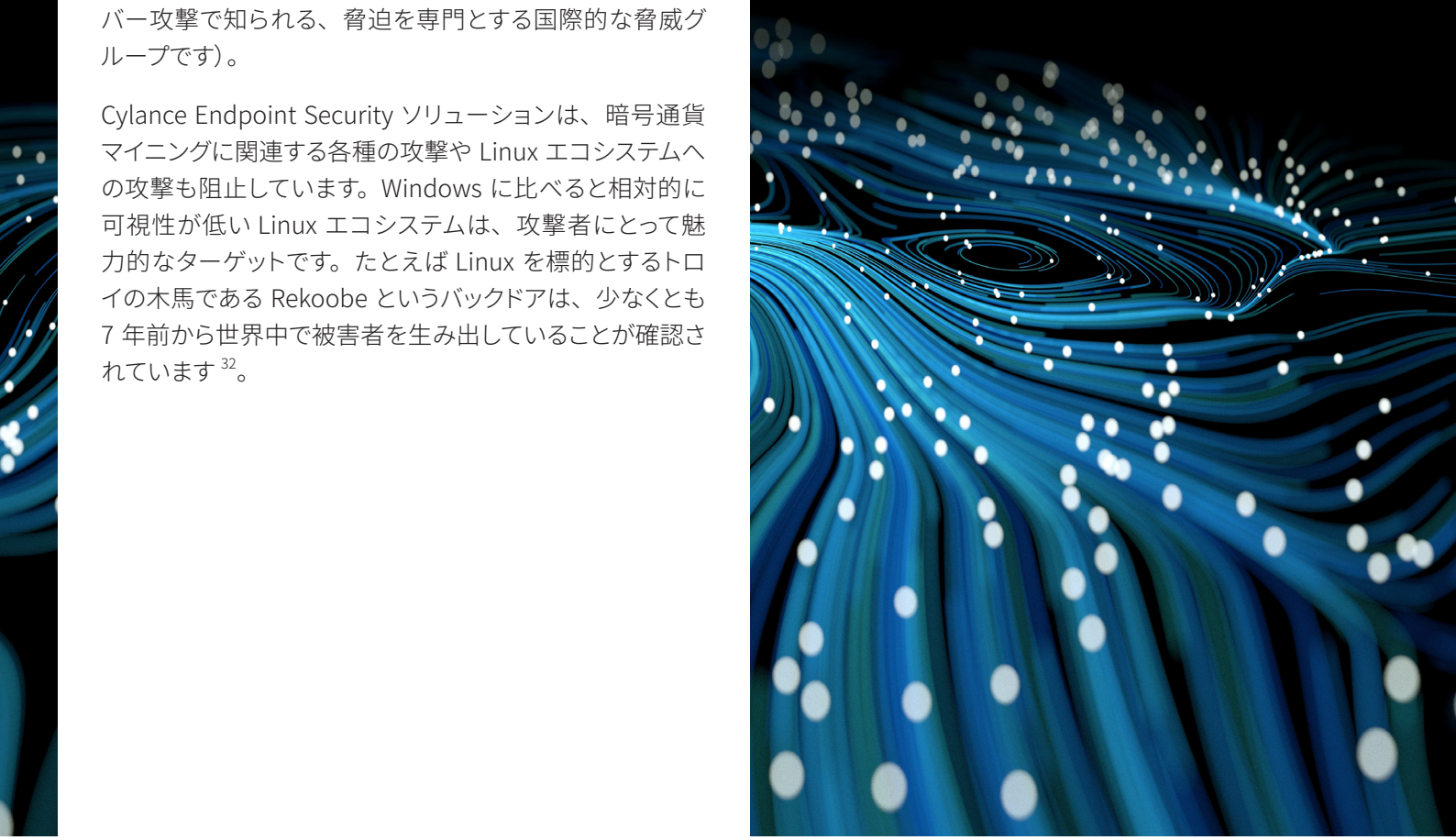
BlackBerry が阻止したその他の主な脅威には、Redline Stealer などの初期アクセスインフォスティーラがあります。初期アクセスツールに高い需要があるのはよく知られています。これは、被害者のネットワークへのアクセスを奪取した後に、そのアクセス権を販売できるためで、Lapsus$ グループなど数多くの脅威アクターが、インフォスティーラを利用して企業へのアクセスを取得しています（Lapsus$ グループは、企業や政府機関への数多くのサイバー攻撃で知られる、脅迫を専門とする国際的な脅威グループです）。

Cylance Endpoint Security ソリューションは、暗号通貨マイニングに関連する各種の攻撃や Linux エコシステムへの攻撃も阻止しています。Windows に比べると相対的に可視性が低い Linux エコシステムは、攻撃者にとって魅力的なターゲットです。たとえば Linux を標的とするトロイの木馬である Rekoobe というバックドアは、少なくとも 7 年前から世界中で被害者を生み出していることが確認されています [32]。

金融業界を標的に発動された マルウェアのユニークサンプル

9,721 件

を CYLANCE ENDPOINT SECURITY ソリューションが阻止しています。



最も活発な脅威アクター

BlackBerry が収集したテレメトリからは、数多くの脅威アクターの活動も明らかにされています。このセクションに記載されている攻撃者には、攻撃の具体的な種類や特定の業界に関する前述のセクションで紹介されたものがあります。

TA505

TA505 は、金銭を目的とするサイバー脅威環境に大きな影響を及ぼしている、活発で影響力のあるサイバー犯罪グループで、世界中の教育、金融、医療、接客、小売などの業界を標的にしています。

このグループは悪意あるメールを大量送信することで知られており、多種多様なマルウェアを駆使できる能力から、地下のマルウェアネットワークとの強いつながりが指摘されています。現在使用し続けている主な攻撃手段はランサムウェア Locky ですが、新たな種類のマルウェアを実験的に使用することも知られています。

TA505 のツールセットには、Cl0p ランサムウェア、FlawedAmmyy RAT（正規のツール Ammyy Admin の流出したソースコードを基盤とする）、さらには Dridex をはじめとするバンキング型トロイの木馬が含まれます。

ALPHV

ALPHV は現在急速に拡大している比較的新しいサイバー犯罪グループで、従来見られなかったような脅迫戦術と攻撃手法で注目を集めています。歴史は比較的短いながらサイバー犯罪コミュニティに対する影響力は大きく、今後も進化し続けながら活動を拡大していくと見られています[33]。

ALPHV は Rust を使用することが知られています。強力なプログラミング言語 Rust を使用することで、脅威アクターが 1 つのコードベースで各種のオペレーティングシステムに対応できるようになります。複数の LotL バイナリ、スクリプト、ライブラリ（LOLBin）を利用して目的を達成する点もこのグループの特徴です。

BlackCat RaaS は、ALPHV によるハッキングキャンペーンの最終段階に、特定のホスト内での横展開が完了し、探索していた情報の収集がすべて完了した後に利用されます。その後 ALPHV は金銭を要求する脅迫を開始します。これまでの例では、DDoS 攻撃の実行をちらつかせて身代金の支払いを迫ったこともあります。現在のマルウェアでは、データを抜き出すとともにデータを暗号化して身代金を要求する二重脅迫攻撃が流行していますが、ランサムウェア BlackCat を RaaS としてリリースした ALPHV も、この流れにあると言えます。

ALPHV グループが特定の業界や国をターゲットにしている兆候は見られません。ALPHV はその他の脅威アクターによる BlackCat ランサムウェアの使用を許可しているため、このマルウェアの存在が ALPHV による直接攻撃を意味するわけではありません。現在までに、BlackCat ランサムウェアによる攻撃は、米国、オーストラリア、日本、イタリア、インドネシア、インド、ドイツといった国々の、小売、金融、製造、政府、テクノロジー、教育、輸送などの業界で確認されています[34]。

APT32

APT32 は、ベトナムを拠点に少なくとも 2014 年から悪意あるサイバー活動を行ってきたと見られています。ベトナム、フィリピン、ラオス、カンボジアなどの東南アジア諸国を活動の中心とし、さまざまな民間産業、外国政府機関、その他反体制派やジャーナリストなどの個人を標的としています。被害者のシステムへのアクセスには戦略的な Web 侵害などの戦術が多用されています。APT32 の技術レベルは高く、防衛機関、ハイテク企業、医療機関、製造企業なども攻撃されたことがあります。

BlackBerry Threat Research & Intelligence チームが APT32 による複数の侵入事例を解析したところ、このグループが Ratsnif と呼ばれる RAT スイートを使用して新たなネットワーク攻撃能力を獲得していることがわかりました。また、ステガノグラフィ（機密ではない一般的なファイルやメッセージに機密データを隠す手法）を利用して、PNG 画像に悪意あるペイロードを埋め込んでいたことも確認されました。

APT29（DUKES）

APT29 は、豊富な資金と高度な組織体制を誇る Dukes とも呼ばれるグループです。少なくとも 2008 年以降、ロシア政府の意図を受けてサイバースパイ活動を行った疑いが指摘されています。このグループの標的は主に北米とヨーロッパの政府機関や非政府組織ですが、攻撃の範囲はアジア、アフリカ、中東の組織にも及んでいます。

このグループは、Cobalt Strike、Mimikatz、AdFind（Active Directory からの情報収集に利用できる無料のコマンドラインクエリーツール）などを多く使用しているほか、CloudDuke、CozyDuke、FatDuke といった一連のカスタムツールも開発しています。APT29 は、一部の製品が影響を受ける脆弱性を悪用して被害者のシステムにアクセスすることでも知られています。

MUSTANG PANDA

Mustang Panda は、サイバー諜報活動を行う脅威アクターとして特定されている、中国を拠点とする APT グループです。このグループの存在が初めて検知されたのは 2017 年ですが、2014 年から活動していた可能性があります[35]。Mustang Panda は、米国、ヨーロッパ、モンゴル、ミャンマー、パキスタン、ベトナムを含む世界各国で、政府機関、非営利団体、宗教団体、非政府組織（NGO）など幅広い組織を標的としてきました。

このグループが活動の遂行に多用しているのは China Chopper と PlugX です。PlugX はモジュール型の RAT で、構成によって HTTP と DNS の両方を使用してコマンドアンドコントロール（C2）活動を行えるようになります。China Chopper は Web サーバー上でホストされる悪意あるソフトウェアで、感染対象デバイスとリモート C2 サーバーの通信を必要とせずに、組織ネットワークへの不正アクセスを可能にします。

BlackBerry Threat Research & Intelligence チームが把握した最新の動向では、ロシアとウクライナの戦争に対する世界的な関心に乗じて、Mustang Panda がヨーロッパとアジア太平洋地域のターゲットを攻撃していました。

TA542

このサイバー犯罪者グループ TA542 は、マルウェア Emotet の作成に重要な役割を果たしたと見られています。2014 年半ばに初めて発見された Emotet は、バンキング型トロイの木馬 Bugat（別名 Feodo）と共通する特徴を持ち、C2 通信用の RSA 鍵交換機能とモジュール設計を追加することでさらに強化されたマルウェアです。通常 TA542 は、攻撃を短期間行った後に数か月間活動を休止し、マルウェアの新しいバージョンまたは亜種によって攻撃を再開します。これはサイバー犯罪グループの典型的な行動パターンとは異なります。TA542 のキャンペーンの標的は、教育、金融、小売、医療などの業界です。

MITRE 手法

BlackBerry Threat Research and Intelligence チームは、複数の MITRE 手法、イベント解析技術、テレメトリを活用して脅威を解析しています。以下の表は、今回の調査期間中に使用された MITRE 手法です。BlackBerry チームが使用した MITRE 手法の全リストは、MITRE ATT&CK® Navigator Layer で確認できます。

表 1：MITRE 手法と戦術

MITRE 手法	手法 ID	戦術
システム情報の探索	T1082	探索
プロセスインジェクション	T1055	防御回避
仮想化 / サンドボックスの回避	T1497	防御回避
リモートシステムの探索	T1018	探索
マスカレーディング	T1036	防御回避
アプリケーション層プロトコル	T1071	コマンドアンドコントロール
ソフトウェアパッキング	T1027.002	防御回避
セキュリティソフトウェアの探索	T1518.001	探索
プロセスの探索	T1057	探索
ツールの無効化または変更	T1562.001	防御回避
アプリケーションウィンドウの探索	T1010	探索
Windows Management Instrumentation	T1047	実行
クエリーレジストリ	T1012	探索
難読化されたファイルまたは情報	T1027	防御回避
レジストリの変更	T1112	防御回避
ファイルとディレクトリの探索	T1083	探索
暗号化されたチャネル	T1573	コマンドアンドコントロール
コマンドとスクリプトインタープリター	T1059	実行
Rundll32	T1218.011	防御回避
Regsvr32	T1218.010	防御回避

ここにリストされた手法の大部分は、防御回避と探索の戦術に関連するものです。通常これらの戦術や関連手法は、感染後に事後調査を行う中で発見されます。これらの手法を使用するには、これまでに特定された侵入に関する情報が必要です。以下に挙げるのは、最も一般的な 5 つの手法に関連する動作のサンプルです。

攻撃の兆候例

以下の表は、MITRE 手法に関連する動作のリストです。

表 2：攻撃の兆候例

手法	動作
システム情報の探索 - T1082	> wmic csproduct get UUID > query user > tasklist | findstr “dll” > systeminfo >> output > date /t
プロセスインジェクション - T1055	> dllhost.exe > rundll32.exe > explorer.exe > MSBuild.exe
仮想化 / サンドボックスの回避 - T1497	> timeout 5000 > Start-Sleep -s 100 > VMWare と VirtualBox のレジストリをチェック
リモートシステムの探索 - T1018	> net group /domain admins > nltest /domain_trusts /alltrusts > net view /all
マスカレーディング - T1036	> マルウェアのファイル名を正規なものと思わせるファイル名に変更 > バイナリに .jpg 拡張子を使用 > スケジュール済みタスクに win32times など正規の名前を使用

MITRE D3FEND を活用した対策

組織が自らの防御戦略を改善し、適切な可視化手法や検知手法が配備されているかどうかを判断するには、一般的な対策を理解することが有効です。対策は、OS イベント（システム内で発生するプロセスイベントなど）やファイルイベント（ファイルの作成、変更、削除など）に基づいて適用できます。

攻撃手法およびそれらに関連する対策の全リストは、BlackBerry の GitHub リポジトリで確認できます。選択する対策は、組織のニーズに最適で 100% 実装できるだけに絞り込むことをお勧めします。

特筆すべき攻撃

2022 年 9 月 1 日～ 11 月 30 日の期間中、BlackBerry Threat Research & Intelligence チームは、全世界中のサイバー脅威環境について追跡、発見、調査した成果を、最新情報として発表しています。世界の経済は新型コロナウイルスのパンデミックがもたらした影響から完全には回復しておらず、現在の東欧における地政学的な事象の先行きは見えず、東西関係も不透明な状態が続いています。こうした複数の要因は、政治目的か金銭目的かを問わず、脅威アクターの活動を支える絶好の機会となります。

直近の四半期では、国家支援による APT グループ、金銭を目的とするランサムウェアギャング、あらゆる規模、技術、動機を持つその他数多くの脅威アクターが、複数のキャンペーンを展開したことが確認されました。ここからは、直近の四半期を通して全世界で発生した攻撃のうち最も重要な攻撃と、BlackBerry が得た最も重要な知見を紹介します。

攻撃手法およびそれらに関連する対策の全リストは、BLACKBERRY の GITHUB リポジトリで確認できます。

DJVU：無害なプログラムに偽装するランサムウェア

DJVU ランサムウェアは、正規のサービスやアプリケーションを偽装するだけでなく、無害を装うためにおとりファイルがバンドルされていることもよくあります。悪名高い STOP ランサムウェアの進化版である DJVU は、2018 年の誕生以来、更新を何度も繰り返しています。このランサムウェアの暗号化ルーチンには、暗号化のためのストリーム暗号 Salsa20 が使用されています。DJVU は、耐解析とアンチサンドボックスのチェックを数多く実行して、自身が実際のシステム上で実行されていることを確認します。その後、

複数の種類のファイルを暗号化して、被害者によるファイル復元の手続きが記載された身代金要求文を生成します。脅威アクターによって暗号化前に実行するダウンローダ機能を追加したことで、このランサムウェアの攻撃力は最近ますます高まっています。

直近の四半期では、DJVU がインフォスティーラをダウンロードして展開する動作が確認されました。これは脅威アクターが被害者を犠牲にして利益を得るための新たな選択肢であり、Arkei の亜種である Vidar Stealer や Redline Stealer の背後にいるグループとの関連性が明らかに疑われます。

MUSTANG PANDA：正規のアプリを悪用してミャンマーで被害を拡大

BlackBerry では 10 月上旬、数か月にも及んだ Mustang Panda APT グループの追跡結果を発表しました。このグループは Bronze President、Red Delta、Honeymyte といった名前でも知られ、中国を拠点としていることが正式に発表されています。

BlackBerry による調査で発覚したのはミャンマーを標的としたキャンペーンです。このキャンペーンは、ミャンマーの有名な報道機関になりすまして行われたもので、政府機関の VPN ポータルを含む複数の組織が標的でした。このキャンペーンでの感染経路は、悪意ある添付ファイルによるフィッシング文書でした。騙されたユーザーがファイルを実行すると、システム上に攻撃者のための足場が確保されます。

実行チェーンは、DLL 検索順をハイジャックするための無害の正規ユーティリティに加え、悪意ある DLL ローダー、暗号化された DAT ペイロードなどの要素で構成されており、悪意ある DLL ローダーがサイドロードされると、PlugX ペイロードがメモリに読み込まれます。感染ベクトル、実行チェーン、PlugX の使用、全体的な TTP は、試行錯誤を繰り返した Mustang Panda のキャンペーン手法に準拠したものでした。

またたく間にファイルを暗号化する BIANLIAN ランサムウェア

BianLian は、Go 言語で記述された、非常に高速な動作を特徴とするランサムウェアです。Go 言語をはじめとする非主流の言語が悪意ある目的で利用される現在のような動きは、BlackBerry がこのホワイトペーパーで以前から予測していました。脅威アクターは、特にカスタムメイドのランサムウェアを中心に、こうした言語にマルウェア開発の潜在能力があることを認識しているのです。Go 言語が特に優れているのは並行処理のサポートです。複数の悪意ある機能を独立して同時実行することで、攻撃をさらに高速化できます。

BianLian は、幅広い業界を標的とする比較的新しい脅威アクターです。BianLian との関わりがある攻撃は 2022 年末時点でも継続的に発生しています。このマルウェアの背後にいるグループは純粋に金銭的な動機で活動していると考えられています。アクセスされたシステムやネットワークは徹底的に悪用されると考えられています。典型的な手法は、手動でシステムに侵入して初期アクセスを奪取した後、LOLBins を悪用してネットワークとシステムを探索し、情報収集が完了したらランサムウェアを展開し、金銭の獲得に移るという流れです。

ウクライナ軍を狙う著名なアプリを装う正体不明の脅威アクター ROMCOM

BlackBerry は 10 月、ウクライナの軍事機関を標的とする未知の RomCom RAT を発見しました。この脅威アクターは、人気のソフトウェア Advanced IP Scanner ソフトウェアの偽装バージョンを展開することで知られていましたが、その後は同じく人気のアプリケーションである PDF Filler へと偽装先を変えています。いずれのエクスプロイトも、この脅威アクターが独自に開発したと見られます。

RomCom RAT は、感染したデバイスを外部から制御することにより悪用します。BlackBerry が確認した最初の感染経路はメールでした。このメールにはリンクが埋め込まれており、接続先は Наказ _309.pdf（英語で Order_309.pdf の意味）というウクライナ語の偽文書となっていますが、このリンクによって後続段階のダウンローダがドロップされてしまいます。

今回の調査期間中、この脅威アクターが世界中の被害者を狙って新たな手法を積極的に開発していることが確認されています。

脅威アクター ROMCOM、有名ソフトウェアブランドを悪用してウクライナと英国を標的に

ウクライナに対する一連の攻撃に携わったグループが次に着手したのは、人気のソフトウェアブランドを悪用した新たな攻撃キャンペーンでした。このキャンペーンは、RomCom RAT に関する調査で特定されていたネットワークアーティファクトを解析する作業の中で、BlackBerry Threat Research & Intelligence チームが発見しました。

BlackBerry リサーチャーの発見によると、このキャンペーンで脅威アクターは SolarWinds Network Performance Monitor、オープンソースの KeePass パスワードマネージャー、PDF Reader Pro になりすましていました。このキャンペーンは、こうした正規の企業の名前を前面に出し、正規の Web サイトを模倣した偽の Web サイトを設計して、被害者による Remcos RAT マルウェアのダウンロードを誘導するものです。RomCom の脅威アクターはウクライナの被害者を標的とする新たなキャンペーンを積極的に展開し続けてきましたが、最新の一連の攻撃からは、ターゲットが全世界の英語圏に拡大しつつある可能性が示唆されます。

こうしたキャンペーンの大規模性は、MUSTANG PANDA グループが

豊富

なリソースと高い技術を備えていることを表しています。BLACKBERRY では、このグループの攻撃は今後も続くと考えています。

ARCRYPTER ランサムウェア、中南米から全世界へ活動範囲を拡大

2022 年を通して ARCrypter ランサムウェアファミリーの監視を続けていた BlackBerry Threat Investigation チームは、中南米の機関をターゲットとする未知の亜種を 8 月に発見し、ARCrypter と名付けました。10 月にはコロンビア国立食品・医薬品監視研究所（INVIMA）が一時的に閉鎖され、原因となったサイバー攻撃が報告されました[36]。

BlackBerry は、脅威ハンティングを通してこのランサムウェアに関連するサンプルを追加で特定しました。攻撃の時間的経過と身代金要求文での INVIMA の記載から判断し、INVIMA へのサイバー攻撃は ARCrypter ランサムウェアによるものという結論を高い確率で導き出しました。さらに追加調査を実施した結果、追加のマルウェアドロッパーとファイル暗号化機能という 2 つのファイルセットが発見されました。

MUSTANG PANDA、ロシアとウクライナの戦争に乗じてヨーロッパとアジア太平洋の標的を攻撃

Mustang Panda に対する監視を続けていた BlackBerry は 12 月、複数の国と大陸の組織を標的としたキャンペーンを発見しました。

このキャンペーンでは、最新の地政学的事象に関連したテーマのルアー（「Political Guidance for the New EU Approach Towards Russia.rar」というタイトルのファイルなど）が使用されていました。このルアーには、おとり文書と、ルアーの RAR ファイルと同じ規則で名付けられた LNK ファイルが格納されていました。さらに、DLL 検索順をハイジャックするための無害のユーティリティ、悪意ある DLL ローダー、DAT ペイロードなどの要素が含まれていました。これらはいずれもこのグループが過去使用したものと同様でした。

この実行チェーンの目標は、PlugX ペイロードをホストシステムのメモリに読み込ませ、侵害されたホストに対する完全なリモートアクセスを可能にすることです。

このキャンペーンの中核となる実行チェーンと TTP は以前にも確認されたものですが、今回の攻撃ではわずかな変更点が確認されました。たとえば実行フローに軽微な変更が加えられ、シェルコードの実行に EnumThreadWindows 関数ではなく EnumSystemCodePagesW 関数が使用されていました。こうしたわずかな変更に対処して保護の効果を最大限に高めるには、防御意識や防御対策を常に調整し続けることが必要です。

BlackBerry では、固有のドメイン SSL 証明書に基づいてさらに 15 個の IP アドレスを発見しました。それらのうち 5 つは Mustang Panda グループの C2 サーバーで、同じ攻撃チェーンと TTP を使用する同様のファイルセットを送信し、さらに多くの場所で被害者を生み出していることがわかりました。

こうしたキャンペーンの大規模性は、このグループが豊富なリソースと高い技術を備えていることを表しています。BlackBerry では、このグループの攻撃は今後も続くと考えています。

その他の攻撃

EMOTET

Emotet は、2022 年 11 月に再び浮上してきた、進化を続ける高度なマルウェアファミリーです。Heodo や Geodo としても知られ、犯罪グループ TA542 が関与する Emotet マルウェアは、2014 年に構想されて以来、強化され続けています [37]。

Emotet はメールで配布され、初期ステージャの多くはトロイの木馬化された Microsoft® Excel® ドキュメントです。このマルウェアは、セキュリティ警告ポップアップを無視して添付ファイルを開くよう被害者を誘導する手口を利用します。Emotet のターゲットは多岐にわたり、そのルアー文書が偽装するトピックもさまざまな言語と地域に対応させています。被害者が警告を無視して偽文書の実行を許可すると、マルウェアが意図するペイロードのダウンロードが試みられます。マルウェアがインストールされた後は、追加のマルウェアをドロップして展開するなど、さまざまな操作を実行できるようになります。

CRYWIPER

CryWiper は、12 月上旬に詳細が明らかになった新たなワイパー型マルウェアです。CryWiper の特徴的な点は、その設計や展開方法がロシア国内の機関（裁判所や市長室など）を狙うことに特化していることです [38]。

CryWiper の動作は、一見しただけでは典型的なランサムウェアと変わりません。つまり CryWiper は、システムのシャドーコピーを削除して感染ファイルの復元を不可能にし、感染ファイルを暗号化して .CRY 拡張子を付加して、身代金の支払い方法とファイル復元方法が記載された身代金要求文 README.txt をドロップします。ただし、CryWiper はランサムウェアではなくワイパーです。このため CryWiper の目標は、その他のワイパーと同様に、ターゲットシステム上のファイルを徹底的に破壊して、身代金が支払われるかどうかに関係なく、いかなる手段によっても復元できないようにすることです。

目的とする水準でファイルを破壊するため、CryWiper では Mersenne Vortex という疑似乱数生成器（PRNG）のアルゴリズムによってファイルの元の内容を上書きして破壊し、復元の可能性を完全になくします。

結論と見通し（2023 年第 1 四半期）

直近の四半期、あるいは 2022 年全体を通して言えるのは、サイバーセキュリティの重要なトレンドが複数明らかになり、そのトレンドは 2023 年以降も続く見込みだということです。政治的な動機を持つ脅威アクターは現在も増え続けています。それらがもたらす脅威には、フェイクニュースサイトによる誤報や偽情報の拡散、ジャーナリストや反体制派の行動や素行の追跡、政府や軍事組織に対する直接攻撃の試みなどが挙げられるでしょう。

全体として、脅威アクターによる使用が確認された数多くの手法の中には、新たに特定されたツールや技法もありましたが、既存ツールを改変して検知の回避を可能にしている例もありました。自動車業界、医療業界、金融業界に対する標的型攻撃は増加し続けており、こうした業界が抱える広大で脆弱な攻撃対象領域をいかに保護するかが、新たな喫緊の課題として浮かび上がっています。

マルウェアやサイバー攻撃から組織を防御するには、現在の業界を脅威アクターがどのような方法で狙おうとするか、脅威アクターが採用しているツール、考えられる脅威アクターの動機について、深く理解することが必要です。そのような詳細な情報があれば、現実的な状況と今後の予測を踏まえた実用的なサイバー脅威インテリジェンスを入手して、脅威が組織にもたらす影響を軽減できるはずです。

教訓 / 重要ポイント

- 金銭目的の脅威アクターだけでなく、経済的、地政学的、社会的な状況の影響によって個人や組織を被害に陥れようとする脅威アクターが増えています。防御する側は、経済や政治の発展がサイバーセキュリティに与えうる影響を、先を見越して考慮に入れることが必要です。
- 脅威アクターのマルウェア開発では、Go 言語 や Rust のような非主流あるいは異色のプログラミング言語が採用されるようになっています。脅威ハンターは、常に警戒を怠ることなく、新たなプログラミング言語の採用がどのような形で攻撃に反映されるかを理解する必要があります。たとえば Go 言語 はクロスプラットフォームコーディングに対応しているため、今後 Linux や macOS に対する攻撃が増える可能性があります。
- 2022 年は、初期アクセスツールの利用が拡大したことや、マルウェアを独自開発できる技術力を持たないグループでもランサムウェアをマネージドサービスとして利用できるようになったことが、インシデントの規模を広げる結果をもたらしました。これを受け、国民支援の脅威アクターによるランサムウェアの利用がますます拡大しています。
- 2022 年の自動車業界は、多種多様なサイバー攻撃による深刻な被害に見舞われました。大規模メーカーや業界サプライヤーが次々と侵害され、製造ラインが数多く停止する事態が発生しました。こうした一連の攻撃は 2023 年も続くと予測されます。
- 正規のアプリを悪用して悪意あるペイロードを配信するサプライチェーン攻撃は、軽減あるいは予防することができます。その方法は、ゼロトラストポリシーを導入し、ネットワークやアプリケーションへのアクセスに対する継続的認証と継続的承認を必須にすることです。

2023 年第 1 四半期の見通し

- ロシアによるウクライナ侵攻の現時点での主な特徴に、ウクライナの軍事インフラと市民インフラに対するサイバー攻撃が挙げられます。このような標的型サイバー攻撃のパターンが、戦闘が続くことでさらに繰り返される可能性があります。
- 病院や医療機関を標的としたランサムウェア作戦が、ウクライナに支援や資金を提供している国々を中心に継続されることが予測されます。
- 重要インフラへのサイバー攻撃は引き続き発生する見込みです。攻撃の自動化に加えて、高度なディープフェイク攻撃の開発に、AI がますます活用される可能性があります。
- 2022 年 9 月、英国を拠点とする Revolut（人気のアプリを提供するフィンテック企業）への攻撃が発生し 5 万件以上の顧客記録が流出しました。ヨーロッパの金融機関を対象とした同様の攻撃は今後も継続する可能性があります。
- BlackBerry では、商業用モバイルスパイウェアによる攻撃が南北アメリカ大陸で爆発的に増加すると予測しています。また、ブラジルの複数の脅威アクターが、トロイの木馬による銀行への攻撃をデスクトップシステムからモバイルデバイスに拡大することで、南米での被害が引き続き発生する見込みです。たとえば 2022 年 12 月には、米国の Zelle に似た決済システム PIX を含む、ブラジルの銀行業界に特化した BrasDex マルウェアファミリー [39] の存在が明らかになりました。
- Linux システムに対する攻撃は、システムの仮想化、ランサムウェアのドロップ、ターゲットシステムへのバックドアのインストールなどを中心に、目立たない形で引き続き行われるでしょう。
- 脅威アクターは、標的とする組織をさらに可視化して、組織の弱体化や利益の奪取につなげようとしています。こうしたことから、クラウドインフラストラクチャへの標的型攻撃が今後あらゆる業界において増加すると思われます。

リソース

BlackBerry Threat Research & Intelligence の公開リソースを紹介します。

侵入の痕跡（IOC）

BlackBerry Threat Research & Intelligence チームでは、解析済みのキャンペーンに関連する侵入の痕跡（IoC）を、GitHub の公開リポジトリで開示しています。BlackBerry の脅威レポート、ブログ、ホワイトペーパーで言及されている IoC その他の実用的な情報（YARA ルールや Sigma ルールなど）は、BlackBerry Threat Research & Intelligence チームの公開 GitHub で確認できます。

公開ルール

BlackBerry Threat Research & Intelligence チームでは、本書で取り上げた脅威の大部分を特定するための YARA ルールを作成しています。BlackBerry の YARA ルールは、こちらで公開されています。

MITRE 手法

BlackBerry Threat Research and Intelligence チームは、MITRE による複数の手法、イベント解析技術、テレメトリを活用して脅威を解析しています。MITRE 手法の全リストは、BlackBerry チームが生成した MITRE ATT&CK Navigator Layer で確認できます。

MITRE D3FEND を活用した対策

攻撃手法およびそれらに関連する対策の全リストは、BlackBerry の GitHub リポジトリにあるブログとレポートのセクションで確認できます。

参照資料

1 https://www.uber.com/newsroom/security-update/

2 https://www.computerworld.com/article/3604601/macs-reach-23-share-in-us-enterprises-idc-confirms.html

3 https://www.developer.com/news/90-of-the-public-cloud-runs-on-linux/

4 https://sysdig.com/blog/malware-analysis-shellbot-sysdig/

5 https://threatpost.com/sysrv-k-botnet-targets-windows-linux/179646/

6 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22947

7 https://yoroi.company/research/outlaw-is-back-a-new-crypto-botnet-targets-european-organizations/

8 https://sandflysecurity.com/blog/log4j-kinsing-linux-malware-in-the-wild/

9 https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-44228

10 https://cyware.com/news/kinsing-operators-target-weblogic-servers-and-docker-apis-for-cryptomining-5ce39d4b

11 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14882

12 https://twitter.com/MsftSecIntel/status/1542281836742729733

13 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26134

14 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2725

15 https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009

16 https://www.reuters.com/business/autos-transportation/continental-investigates-cyberattack-after-report-says-data-up-sale-2022-11-15/

17 https://www.juniperresearch.com/press/in-vehicle-commerce-opportunities-exceed-775mn

18 https://www.lv.com/insurance/press/keyless-technology-drives-rise-in-theft-over-past-four-years

19 https://www.europol.europa.eu/media-press/newsroom/news/31-arrested-for-stealing-cars-hacking-keyless-tech

20 https://www.bbc.com/news/uk-england-39906534

21 https://resources.infosecinstitute.com/topic/biggest-data-breaches-of-2019-so-far/

22 https://attack.mitre.org/groups/G0050/

23 https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/

24 https://www.zdnet.com/article/europes-biggest-car-dealer-hit-with-ransomware-attack/

25 https://www.broshuis.com/news/ransomware-attack

26 https://www.reuters.com/business/autos-transportation/japans-bridgestone-reports-ransomware-attack-us-subsidiary-2022-03-18/

27 https://europe.autonews.com/automakers/toyota-suspend-output-japan-after-supplier-hit-cyberattack

28 https://www.nhtsa.gov/press-releases/nhtsa-updates-cybersecurity-best-practices-new-vehicles

29 https://www.bleepingcomputer.com/news/security/commonspirit-health-ransomware-attack-exposed-data-of-623-000-patients/

30 https://www.cisa.gov/emergency-directive-21-02

31 https://asec.ahnlab.com/en/27346/

32 https://malpedia.caad.fkie.fraunhofer.de/details/elf.rekoobe

33 https://www.computerweekly.com/news/252525240/ALPHV-BlackCat-ransomware-family-becoming-more-dangerous

34 https://www.securitymagazine.com/articles/97489-blackcat-alphv-ransomware-breaches-60-organizations

35 https://attack.mitre.org/groups/G0129/

36 https://twitter.com/invimacolombia/status/1577455552954712064?s=20&t=JYJsQ6PFhxBv3YHim_PQrw

37 https://malpedia.caad.fkie.fraunhofer.de/actor/mummy_spider

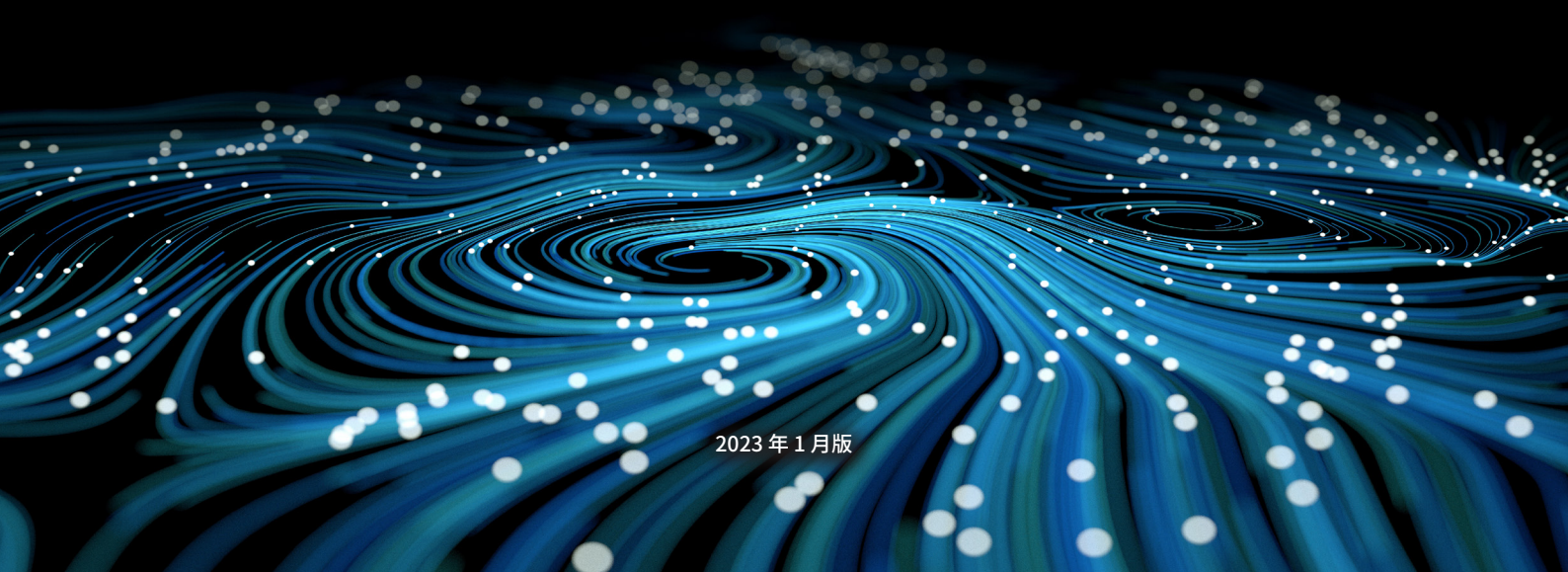
38 https://www.bleepingcomputer.com/news/security/new-crywiper-data-wiper-targets-russian-courts-mayor-s-offices/

39 https://thehackernews.com/2022/12/beware-cybercriminals-launch-new.html

BlackBerry | Cybersecurity

BlackBerry について：BlackBerry（NYSE: BB、TSX: BB）は、インテリジェントなセキュリティソフトウェアとサービスを世界中の企業と政府機関に提供しています。BlackBerry のソリューションは、2 億 1,500 万台の車両を含む 5 億以上のエンドポイントを保護しています。BlackBerry はカナダのオンタリオ州ウォータールーに本拠を置き、AI と機械学習を活用してサイバーセキュリティ、安全、データプライバシーソリューションの分野に革新的なソリューションを提供しています。また、エンドポイントセキュリティ、エンドポイント管理、暗号化、組み込みシステムの分野におけるトップクラスの企業です。BlackBerry のビジョンは明確です。つながる未来に信頼性あるセキュリティを確保することです。

*詳細については、**BlackBerry.com** にアクセスし、**@BlackBerryJPsec** を**フォローしてください。*



2023 年 1 月版