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

2023 年 8 月版

調査期間：2023 年 3 月 1 日 ～ 5 月 31 日

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」は、2023 年 1 月の季刊第 1 号の公開直後から、サイバーセキュリティ業界の重要リファレンスガイドとして揺るぎない地位を確立しています。CISO、セキュリティ管理者、その他の意思決定者を含む世界中のサイバーセキュリティの専門家が、自社の業界や自社プラットフォームに影響を及ぼす最新のサイバーセキュリティの脅威と課題について、本レポートから最新情報を入手しています。

この最新号では、政府機関 / 公的機関における課題、医療業界が抱える脆弱性、金融機関に潜むリスク、重要インフラを守ることの重要性について、BlackBerry がグローバルに展開する BlackBerry Threat Research and Intelligence チームが検証します。さらに、地政学的な観点から分析と見解を提示するセクションを新たに追加し、新たな背景情報をお知らせするとともに、入手されたデータを戦略的に読み解いています。なお、本レポートの調査期間は 2023 年 3 月から 2023 年 5 月までとなります。

本レポートの主な重要情報は以下のとおりです。

- **数字で見る 90 日間の動向：**BlackBerry® Cybersecurity ソリューションは、2023 年 3 月から 2023 年 5 月にかけて **150 万件を超える攻撃**を阻止しています。脅威アクターは平均で **1 分間に約 11.5 回**の攻撃を展開しており、これらの脅威には **1 分あたり約 1.7 件**の新しいマルウェアサンプルが含まれています。つまり、1 分あたりの新しいサンプルの平均数は、前回の調査期間で記録された約 1.5 件から **13% 増加**しています。これは、シグネチャとハッシュを基盤とするレガシーソリューションを中心とした防御用コントロールを回避するための攻撃者の手段が、ますます多様化していることを意味します。
- **最も狙われた業界：**最も多く標的とされた業界は、医療業界そして金融サービス業界でした。貴重なデータと重要なサービスが共存している医療業界は、サイバー犯罪者にとって狙いがいのあるターゲットです。医療機関に直接攻撃を仕掛けるランサムウェア

本レポートは、CISO、セキュリティ管理者、その他の意思決定者を含む

全世界の

サイバーセキュリティ専門家に活用されています。

グループの登場や、インフォスティーラと呼ばれる情報窃取型マルウェアの急増は、こうした理由が背景にあります。本レポートでは、患者データを保護し、必要不可欠な医療サービスを間断なく提供し続けることの重要性をあらためて振り返ります。

- **リモートアクセスによるサイバーリスクの増大：**経済を左右する重要な役割を担い、大量の機密データを運用する金融機関は、常に脅威にさらされています。本レポートでは、コモディティマルウェアの増加、ランサムウェア攻撃、デジタルバンキングサービスやモバイルバンキングサービスを狙うモバイルバンキング型マルウェアの増加など、金融業界が直面している課題を掘り下げます。

- **特定の国に固有のサイバー攻撃：**2023 年第 2 四半期は APT28 と Lazarus Group の非常に活発な活動が確認されました。これらはそれぞれロシアと北朝鮮に関連する国家支援型の脅威アクターであり、米国、ヨーロッパ、韓国を主なターゲットに長く攻撃を仕掛け続けています。攻撃対象は政府機関、軍事組織、企業、金融機関と幅広く、国家の安全保障と経済的安定に深刻な脅威をもたらしています。これらの脅威グループの攻撃は防御が難しいのが特徴です。これは、脅威グループが絶えず手法を変化させ、現状に適応させているためです。

- **総括と今後の展望：**最後に結論を提示するとともに、2023 年の残りの月間に向けたサイバー脅威予測を示します。

「MITRE 手法」と「適用された防御策と緩和措置」のセクションでは、脅威グループが使用した上位 20 件の手法をまとめ、前回の四半期レポートとの傾向を比較することで、実情を踏まえた実践的なサイバー脅威インテリジェンスを提供しています。たとえば、最も頻繁に使用された上位 5 つの戦術は、「探索」と「防御回避」のカテゴリに該当していたことが確認されました。これらの戦術に関連するとして報告された手法は、「パープルチーム演習」に取り入れたり、実践的な脅威モデル演習を行う際の TTP（戦術、手法、手順）の優先度設定に役立てたりすることができます。

さらに BlackBerry Threat Research and Intelligence チームは、MITRE D3FEND ™ に基づいて、今回の調査期間で使用されたすべての手法に対応するすべての防御策をリストにまとめました。 MITRE D3FEND は BlackBerry の公開 GitHub リポジトリから利用できます。今回の調査期間では、Cylance® AI を基盤とする BlackBerry Cybersecurity ソリューションが 224,851 件のユニークサンプルを阻止しました。本レポートでは、これらのユニークサンプルが示した悪意ある振る舞いの検知に最も効果的だった Sigma ルールをリストアップしています。本レポートの目標は、読者の皆様が実際に運用している脅威ハンティングや脅威検知の機能に、本レポートが提示する知見を応用していただくことです。

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。今回の 2023 年 8 月版に記載された詳細かつ実用的なデータすべてを、皆様のお役に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

国別の攻撃と業界別の攻撃

国別のサイバー攻撃

サイバー攻撃を最も多く受けた上位 5 か国

図 1 は、BlackBerry Cybersecurity ソリューションが未然に防御したサイバー攻撃の数と、使用された悪意あるユニークサンプルの数が最も多かった上位 5 か国を示しています。前回の調査期間と同様、BlackBerry が未然に防御した攻撃が最も多かったのは米国でした。前回以降はアジア太平洋（APAC）地域で増加したことで、韓国と日本が上位 3 か国に入り、ニュージーランドと香港が初めて上位 10 か国にランクインしています。最上位は依然として米国ですが、BlackBerry では、新しいサンプルが観測された国の多様性に特に注目しています。

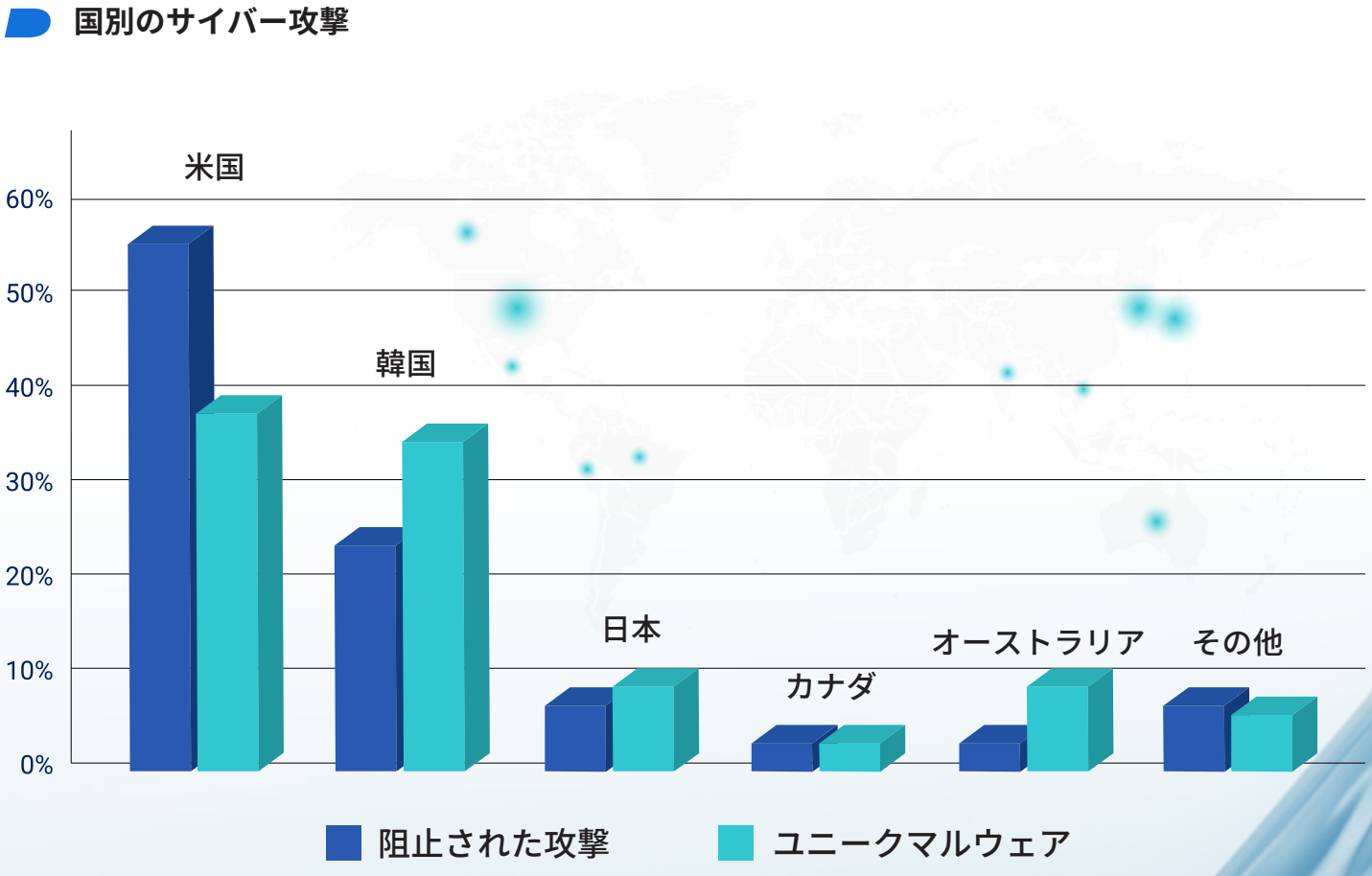

図 1：サイバー攻撃の標的にされた BlackBerry クライアント数と、BlackBerry 保護デバイスに対するそれらの攻撃で使用された悪意あるユニークサンプルの数が最も多かった上位 5 か国。

業界別の攻撃

BlackBerry のテレメトリによると、今回の調査期間中に BlackBerry Cybersecurity ソリューションが保護したサイバー攻撃の分布が最も多い上位の業界は以下のとおりです。

- 金融
- 医療サービス・医療設備（病院、クリニック、医療機器）
- 政府機関 / 公的機関
- 重要インフラ

今回の調査期間中に攻撃を受けた一連の業界は、前回のレポートに比べて多様性が増しています。図 2 は、上位 3 つの業界におけるサイバー攻撃の分布を示しています。この図から、阻止された攻撃の場合と、阻止された固有のハッシュの場合のそれぞれで、1 位から 3 位の業界の順位が反比例の関係になっていることも分かります。

業界別の阻止されたサイバー攻撃

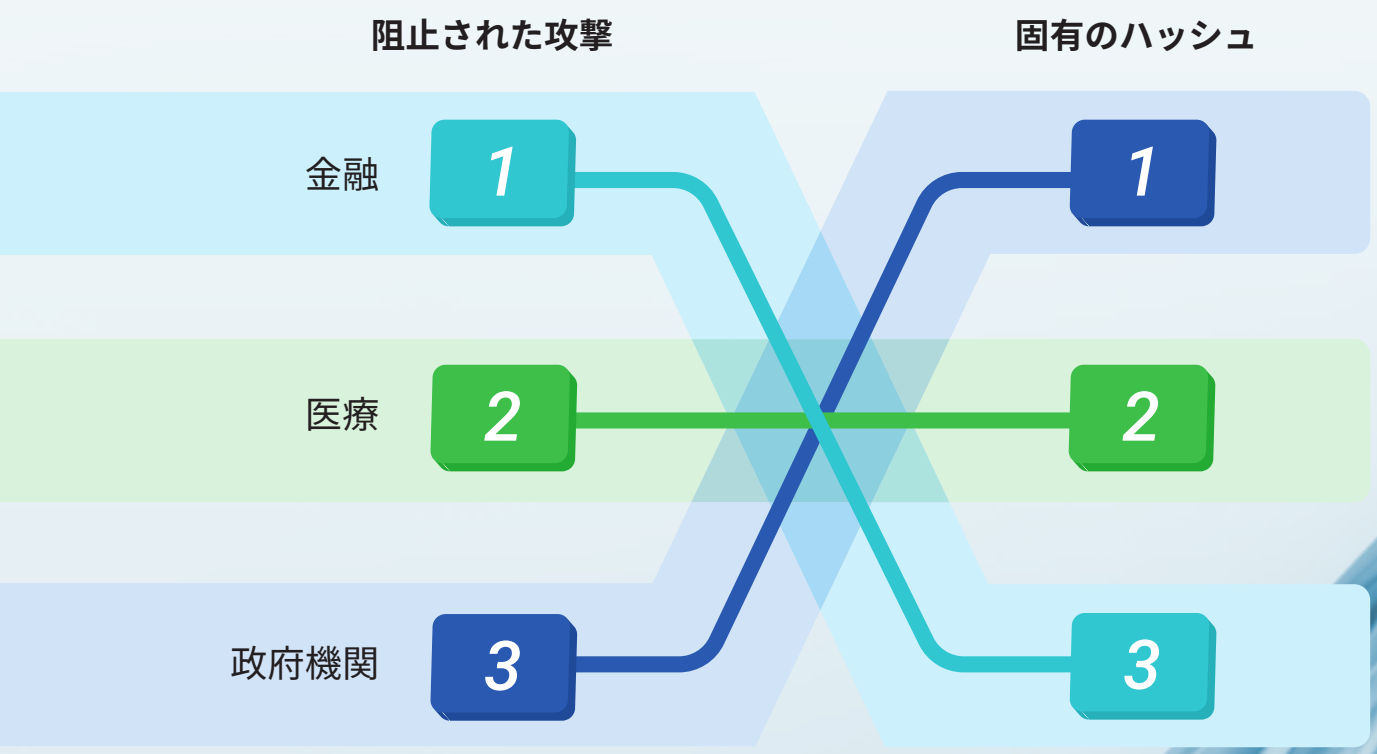

図 2：今回の調査期間中、阻止されたサイバー攻撃および阻止されたユニークサンプル（サンプルの種類）の分布が最も多かった 3 つの業界。

政府機関 / 公的機関

地政学的な優位性の獲得、金銭、業務の混乱などを動機とする脅威アクターにとって、政府機関は魅力的なターゲットです。こうした脅威アクターには、民間の一般人、小規模グループ、（APT 戦術に習熟した）国家支援型の APT グループなどが考えられるため、政府機関は幅広い脅威に対応できる防御能力が求められます。

今回の調査期間中 BlackBerry Cybersecurity ソリューションは、前回の調査期間と比較して 40% 近くの増加となる、政府機関 / 公的機関を標的とする 55,000 件を超える個別の攻撃を阻止しました。

BlackBerry Cybersecurity ソリューションが阻止した政府機関に対する攻撃が最も多かったのは北米と APAC 地域で、APAC 地域で最も多くの攻撃に狙われたのはオーストラリア、韓国、日本でした。

政府機関で最も多い脅威

前回の調査期間中 BlackBerry Threat Research and Intelligence チームは、RedLine、Emotet、RaccoonStealer（RecordBreaker）など、政府機関をターゲットとする安価で入手しやすいコモディティマルウェアファミリーを複数記録しました。同様に、政府機関を狙うコモディティマルウェアローダーには PrivateLoader や SmokeLoader などがありました。

今回の調査期間では DCRat（別名：Dark Crystal RAT）が記録されました。2019 年から頻繁に観測されるようになった DCRat は、脅威アクターによる被害者デバイスの制御を実現した後に、侵入対象の環境への便利なアクセスポイントとして機能します。

政府機関を取り巻く脅威の全体像の検証

今回の調査期間で何と言っても大きな話題となったのは、北米の市政府や州政府のシステムを標的にし、侵入することに成功したランサムウェアグループのニュースです。

たとえば 3 月には、ランサムウェア集団 LockBit がカリフォルニア州オークランド市[1] に攻撃を仕掛けました。このグループは RaaS（Ransomware-as-a-Service）を利用し、通常は複数の戦術と手法を駆使してネットワークに侵入します。侵入して重要情報や機密情報を特定して抜き出した後は、これらのデータを担保に二重恐喝の手口で被害者により多くの身代金を要求し、強制的に支払わせます。今回の調査期間中ではさらに、脅威グループ BlackByte が、以前テキサス州ダラス市とジョージア州オーガスタ市を襲った Royal と呼ばれるランサムウェアの攻撃者であると主張しました。

類似の RaaS に Clop ランサムウェアグループ（別名：Cl0P または CLOP）があります。これはマネージドファイル転送（MFT）アプリケーション GoAnywhere に存在する、

BlackBerry Cybersecurity ソリューションが

阻止

した政府機関に対する攻撃が最も多かったのは北米と APAC 地域で、APAC 地域で最も多くの攻撃に狙われたのはオーストラリア、韓国、日本でした。

パッチ適用済み CVE-2023-0669[2] の脆弱性を悪用するもので、この脆弱性が開示された後、Clop は、今回の調査期間で発生したカナダのトロント市[3] への攻撃を含むいくつかの攻撃について、自らが実行者だと主張しました。Clop グループは、デバイスを暗号化し、35,000 人を超える市民のメタデータを抜き出したのが自分たちだと主張しています。

ポーランドも攻撃に見舞われました。ロイター通信によると[4]、ポーランド税務局では 3 月にロシアのサイバー攻撃と疑われる事象が発生し、外部との通信が遮断されました。ポーランドの情報セキュリティ長官によれば[5]、この攻撃を仕掛けたのはロシアとつながりのあるグループ NoName で、攻撃の仕組みは現在の水準に比べるとシンプルだったということです。

5 月にはハクティビストグループ Mysterious Team による、セネガル[6] の政府サイトと財務省サイトをターゲットとする分散型サービス妨害（DDoS）攻撃が発生しています。

医療

医療業界は、脅威アクターの攻撃に最も絶え間なくさらされている業界の 1 つです。人命に関わるサービスを届け、長期間オフラインにすることができない医療システムやインフラを抱えている医療機関は、サービス再開と引き換えに身代金を一刻も早く支払わせようとするランサムウェアグループの格好の標的となっています。FBI インターネット犯罪苦情センター（IC3）の最新レポートによると、米国の重要インフラを運営する業界のうち、2022 年にランサムウェアグループに最も狙われたのは医療 / 公衆衛生業界でした。攻撃の数は公式に報告されただけでも 210 件に達しています[7]。

医療業界がターゲットになる理由はそれだけではありません。個人の名前、住所、生年月日、社会保障番号などの個人情報（PII）や、その多くが機密性の高い健康記録など、システムに格納されているデータの価値が高いことも原因の 1 つです。PII は、武器化して個人情報窃盗などの犯罪に利用する[8]、ダークウェブのマーケットフォーラムで販売する、脅迫や身代金の担保として悪用するなど、数多くの用途があります。

米国保健福祉省の市民権局が公開しているセキュリティ侵害ポータルによると[9]、今回の調査期間中に発生した米国医療機関を狙った「ハッキング /IT インシデント」事象は 146 件に達していました。

医療業界で最も多い脅威

調査期間中、BlackBerry Cybersecurity ソリューションは 13,433 件のユニークなマルウェアバイナリを検知して阻止し、医療業界全体では 109,922 件を超える個別の攻撃を未然に防御しました。

最も頻繁だった攻撃はコモディティマルウェアによるもので、RedLine に代表されるインフォスティーラが中心でした。また、感染したホスト上で偵察し、データを窃取して、追加のペイロードを配信する Amadey（同名のボットネットにリンクされたボット）も頻繁に観測されました。

さらに、Emotet、IcedID、SmokeLoader などのマルウェアファミリーで医療業界に攻撃を仕掛ける脅威アクターも数多く確認されています。これらの攻撃の共通点は、悪意あるペイロードを追加で配信できる情報窃取型マルウェアを採用していることです。

BlackBerry Cybersecurity ソリューションは 13,433 件のユニークなマルウェアバイナリを

検知

して阻止し、医療業界全体では 109,922 件を超える個別の攻撃を未然に防御しました。

医療業界を取り巻く脅威の全体像の検証

今回の調査期間では、医療業界全体を対象とする大規模かつ注意すべきサイバー攻撃がいくつか発生しています。3 月上旬、スペインの病院 Clínic de Barcelona[10] が、サイバー犯罪組織 RansomHouse によると考えられるランサムウェア攻撃の被害者[11] となりました。病院インフラストラクチャ内部の仮想マシンをターゲットとするこの攻撃は、医療サービス計画に大混乱をもたらしました。そのわずか 1 週間ほど後にはスペインの大手医薬品サプライヤー Alliance Healthcare が攻撃の標的となり、同社の Web サイト、請求システム、注文処理機能が完全に停止[12] する被害を受けました。

同じく 3 月には、インドで最大規模、世界でも第 4 位の規模を誇るムンバイ拠点の製薬メーカー Sun Pharmaceuticals が、ALPHV/BlackCat ランサムウェアのオペレーターによる攻撃を受けています[13]。攻撃直後には、同じランサムウェアオペレーターが、奪取した同社のデータをリークサイトに流出させています。このランサムウェアオペレーターグループは、ほぼ同時期にペンシルベニア州を拠点とする Lehigh Valley Health Network にも攻撃を仕掛け、女性の乳がん患者の写真を公開すると脅迫しています[14]。この脅迫行為は、サイバー犯罪業界の卑劣さの最低レベルを更新するものとして全世界から避難を受けました。

今回の調査期間では、国家支援型の脅威アクターも医療業界をターゲットに活動していた疑いがあります。たとえば 5 月には、北朝鮮を拠点とするハッカーがソウル大学病院に侵入して機密医療データを盗難したことが、韓国の警察当局によって発表されています。このセキュリティ侵害は 2021 年半ばに発生したもので、その後 2 年間の調査を経て今回の発表に至ったということです。メディアの複数の情報筋は、この攻撃は Kimsuky APT による犯行だと断定しています[15]。

これらの多種多様な攻撃は、どのような種類の脅威アクターにとっても医療業界が魅力的な標的であることを示しています。数多くの医療機関が、機密データを格納し、人命に関わるサービスを提供していることを考えると、医療業界に対する攻撃は今後も増え続けると見られます。

数多くの医療機関が、機密データを格納し、人命に関わるサービスを提供していることを考えると、医療業界に対する攻撃は

今後も増え続けると見られます。

金融

金融業界もサイバー犯罪者が頻繁に攻撃を仕掛けている業界の 1 つです。攻撃の目的は、多額の身代金、破壊的成果（政府による罰金の可能性、裁判費用、脅威緩和のための費用、被害者の評判失墜など）、さらにはダークウェブフォーラムで売買できる機密財務データなど多岐にわたります。奪取された財務データの多くは次の脅威アクターによって購入され、武器化され、新たな悪意ある目的の達成に利用されます。

今回の調査期間中、BlackBerry Cybersecurity ソリューションは金融機関を狙う 17,000 件を超える攻撃を阻止しました。全体のうち 15,000 件近くが米国の金融機関をターゲットとしており、それ以外の攻撃は南米とアジアの国々で検知され、阻止されています。

金融業界で最も多い脅威

今回の調査期間における BlackBerry のテレメトリからは、RedLine に代表されるコモディティマルウェアが引き続き利用される傾向が観測されています。RedLine は、保存された認証情報、クレジットカード情報、さらに最新バージョンでは暗号通貨などの情報を奪取できるマルウェアですが、バックドアマルウェア SmokeLoader やオープンソースフレームワーク MimiKatz を使用した攻撃も BlackBerry により観測されています。

金融業界に対する脅威としては、ロシア語圏のハッキングフォーラムで販売されているボットネット Amadey もあります。Amadey は、攻撃者による命令を待機しながら、ターゲットとなった被害者の情報をコマンドアンドコントロール（C2）に送り返します。Amadey の主な機能は、侵害されたマシンに悪意あるペイロードをロードすることです。

金融業界を取り巻く脅威の全体像の検証

今回の調査期間中、金融業界は特に銀行を中心に多くの攻撃を受けました。金融機関で多く観測されたもう 1 つの脅威に、CryptoMix ランサムウェアファミリーの亜種である Clop ランサムウェアがあります。このマルウェアの背後にいるグループは、GoAnywhere MFT ソフトウェアで発見された最新の脆弱性を悪用していることも確認されています。GoAnywhere MFT ソフトウェアに被害をもたらした認証前コマンドインジェクションの脆弱性は、最近のバンキングプラットフォーム Hatch Bank[17] で発生したセキュリティ侵害で CVE-2023-0669[16] として記録されたものです。

BlackBerry Cybersecurity ソリューションは、金融機関を狙う

17,000 件

を超える攻撃を阻止しました。

今回の調査期間が始まって間もなく、Lockbit 3.0 の背後にいる RaaS グループが、インドの非銀行金融会社 Fullerton India[18] を狙った攻撃を仕掛けました。この攻撃を仕掛けたグループは、600 GB を超えるデータを奪取してダークウェブのリークサイトで共有したと主張しています。

オーストラリアでは、ローン大手 Latitude Financial Services[19] に加え、Commonwealth Bank of Australia のインドネシア部門[20] をターゲットとするサイバー攻撃が 2023 年初頭に発生しています。

さらに金融業界では新たな Android マルウェアの被害も発生しています。これは「Chameleon」と呼ばれる Android 型トロイの木馬で [21]、PKO Bank Polski の電子バンキングサービスアプリケーションに成りすまし、騙された利用者に被害をもたらすものです。さらに、更新版をリリースした Xenomorph Android マルウェアグループは、全世界の 400 以上の銀行 [22] から認証情報を奪取したと言われています。

重要インフラ

あらゆる人々が等しく必要とする公共サービスを届けるには、信頼性に優れた重要インフラが欠かせません。つまり、攻撃を仕掛けようとする敵性国家などのグループにとって、重要インフラは効果の大きいターゲットになります。前回のレポートでも指摘したとおり、ウクライナのエネルギー業界は、背後にロシアの支援があると考えられるグループによって物理とデジタルの両面から攻撃されています。悪意ある攻撃者、政府機関、重要インフラ運営者による、運用技術（OT）に潜むセキュリティ脆弱性への注目がますます高まる中、インフラのセキュリティに最優先で取り組むことが求められています。

今回の調査期間中 BlackBerry のテレメトリに最も多く記録されたのは、米国のインフラに対する攻撃でした。それに続くのはインド、日本、エクアドルで、BlackBerry Cybersecurity ソリューション全体では、重要インフラをターゲットとする 25,000 件以上の攻撃を今回の調査期間中に阻止しています。

最も狙われた重要インフラ

外部脅威の影響を緩和する目的で、多くの重要インフラはそれ以外のすべてのシステムから隔離されています。しかし、IT エコシステムと OT エコシステムのいずれにおいてもデジタル化が進み、モノのインターネット（IoT）との連携も加速するばかりです。こうした状況が思いもよらないリスクになる可能性は否定できません。新しい技術を採用した場合、そこには高度なサイバー脅威が間違いなく引き寄せられています。こうしたサイバー犯罪者は、インフラに損害を与えることだけでなく、データやシステムへの不正アクセスをも狙っています。

インフラに対する脅威としてはコモディティ型マルウェアも蔓延し続けており、BlackBerry でも Vidar インフォスティーラというコモディティマルウェアを検知しています。

重要インフラを取り巻く脅威の全体像の検証

今回の調査期間中に発生した重要インフラに対する攻撃で最も広く報じられたものの 1 つに、中国が支援しているとされる脅威アクター Volt Typhoon の米国をターゲットとした攻撃があります。Microsoft の調査によると [23] Volt Typhoon の重要な目的はスパイ活動であり、Living off the Land（LotL）[24] 手法を利用してネットワーク機器に不正侵入し、検知されない状態を維持しながらネットワークトラフィックを流出させることができます。

4 月には、X_Trader サプライチェーン攻撃 [25] を主導したと考えられている北朝鮮拠点のグループと、米国とヨーロッパの重要インフラで発生したセキュリティ侵害との関連性が明らかになりました。こうした地政学的緊張の高まりに刺激され、欧米諸国の重要インフラを狙う脅威に対する一般市民の意識も高まっています。たとえば英国国家サイバーセキュリティセンター（NCSC）は、ロシアのウクライナ侵攻を支持する国家とつながりのある脅威アクターの活動が活発化しているとして、警戒を呼びかけるアラート [26] を発令しています。

BlackBerry Cybersecurity ソリューションは、重要インフラをターゲットとする 25,000 件以上の攻撃を阻止しています。

地政学的な分析と見解

現在のセキュリティは、デジタル地政学を切り離して考えることはできません。一部の国家では、国力の誇示、敵対する国家の混乱、地政学的目標の達成といった目的のために、悪意あるサイバー活動を頻繁に利用するようになっています。これはまさに、カナダのサイバーセキュリティセンターが発表した「National Cyber Threat Assessment for 2023-24」[27] において、サイバー脅威活動が「国家が紛争のしきい値を超すことなく事象を有利に進めるための重要な手段となっている」と指摘されているとおりです。こうしたサイバー攻撃の背後にある動機は、知的財産の奪取、サイバースパイ活動、重要インフラの妨害、デジタル情報操作キャンペーンによる政府に対する国民の信頼度低下など多岐にわたります（米国「National Cybersecurity Strategy」[28] を参照）。現在ますます進んでいる IT インフラストラクチャと OT インフラストラクチャのオンライン化と歩調を合わせるように、経済的、社会的、地政学的、軍事的目的を達成する手段として、サイバー活動はこれからも利用され続けるでしょう。

今回の調査期間中の BlackBerry の記録によれば、BlackBerry Cybersecurity ソリューションが阻止した公的機関に対するサイバー攻撃の数は、約 40% 増加しています。重要インフラ分野は、国家支援型のサイバー脅威アクターの戦略上重要なターゲットとなっています。これは、政府による公共サービスの提供が滞ることは悪影響が特に大きく、国民の信頼を損なうからです。こうした事情を背景に、Five Eyes（オーストラリア、カナダ、ニュージーランド、英国、米国で構成される国家間情報共有の枠組み）の加盟政府では継続的な評価活動を実施し、国家支援型のサイバー脅威アクターが「重要インフラに対する偵察活動をほぼ確実に実施して」おり、その目的が「産業用 OT ネットワークへの事前配置」および「国民の健康と安全を脅かす権力と能力があることを誇示し、威嚇するためのメッセージの配信」であることを突き止めています（「The Cyber Threat to Canada's Oil and Gas Sector」[29]、Canadian Center for Cyber Security、2023 年。CISA の「Cybersecurity Alerts & Advisories」[30] も参照）。

サイバー攻撃の深刻化を受け、インシデントの調査、対応、復旧を目的とした各国政府間の協力はますます強化されています。たとえば 2022 年にコスタリカ [31]、アルバニア [32]、モンテネグロ [33] の重要インフラに対するサイバー攻撃が発生した際、対応に追われる各国政府に対して、米国その他の同盟国がいち早く支援活動を開始しています。さらに最近では、カナダのバンクーバーに約 30 を超える国の政府代表が集結し、サイバー脅威に対応し、サイバー空間における責任ある国家活動を維持するための、幅広い国際間協力の必要性を再確認しています（「Nations urged to be responsible in cyber space after meeting in Vancouver」[34] を参照）。

ウクライナにおける戦闘が長期化する中、地政学とサイバー攻撃の関連性はますます明白なものになっています。オーストラリア、カナダ、ニュージーランド、英国、米国は、重要インフラを狙うサイバー活動の可能性を警告する複数のサイバー勧告を共同で発表しています[35]。ここで指摘されている活動の主体は、ロシアのウクライナ侵攻を支持する非国家の犯罪ハクティビストグループで、「ロシア国家が支援している」場合と「ロシアとつながりがある」場合の両方が想定されています。今回の調査期間中 BlackBerry は、ウクライナ難民に医療支援を行っている EU の在外公館や米国の医療機関をターゲットとした、ロシアとの関連が疑われる脅威アクターによる攻撃を記録しています。BlackBerry では、現在の地政学的危機がこのまま拡大していけば、この傾向はさらに続くと予想しています。

阻止された脅威の合計数

BlackBerry Cybersecurity ソリューションは、2023 年 3 月から 5 月にかけて 1,528,488 件のサイバー攻撃を阻止しました。この期間中に脅威アクターが BlackBerry のお客様に展開したマルウェアサンプルは 1 日平均 16,614 件に達しています。これは 1 分間に平均 11.5 件のマルウェアサンプルが展開されている計算になります。

これらのサンプルに含まれていた新しいユニークなマルウェアサンプルは 224,851 件でした。つまり新しいサンプルの展開ペースは 1 日あたり平均約 2,444 件、1 分あたり約 1.7 件で、前回の調査期間におけるユニークサンプルの平均数である 1 分あたり 1.5 件から 13% の増加となりました。

以下のグラフは、Cylance AI を基盤とする BlackBerry Cybersecurity ソリューションが今回の調査期間で未然に防御したサイバー攻撃の推移を示しています。

未然に防御された攻撃の推移

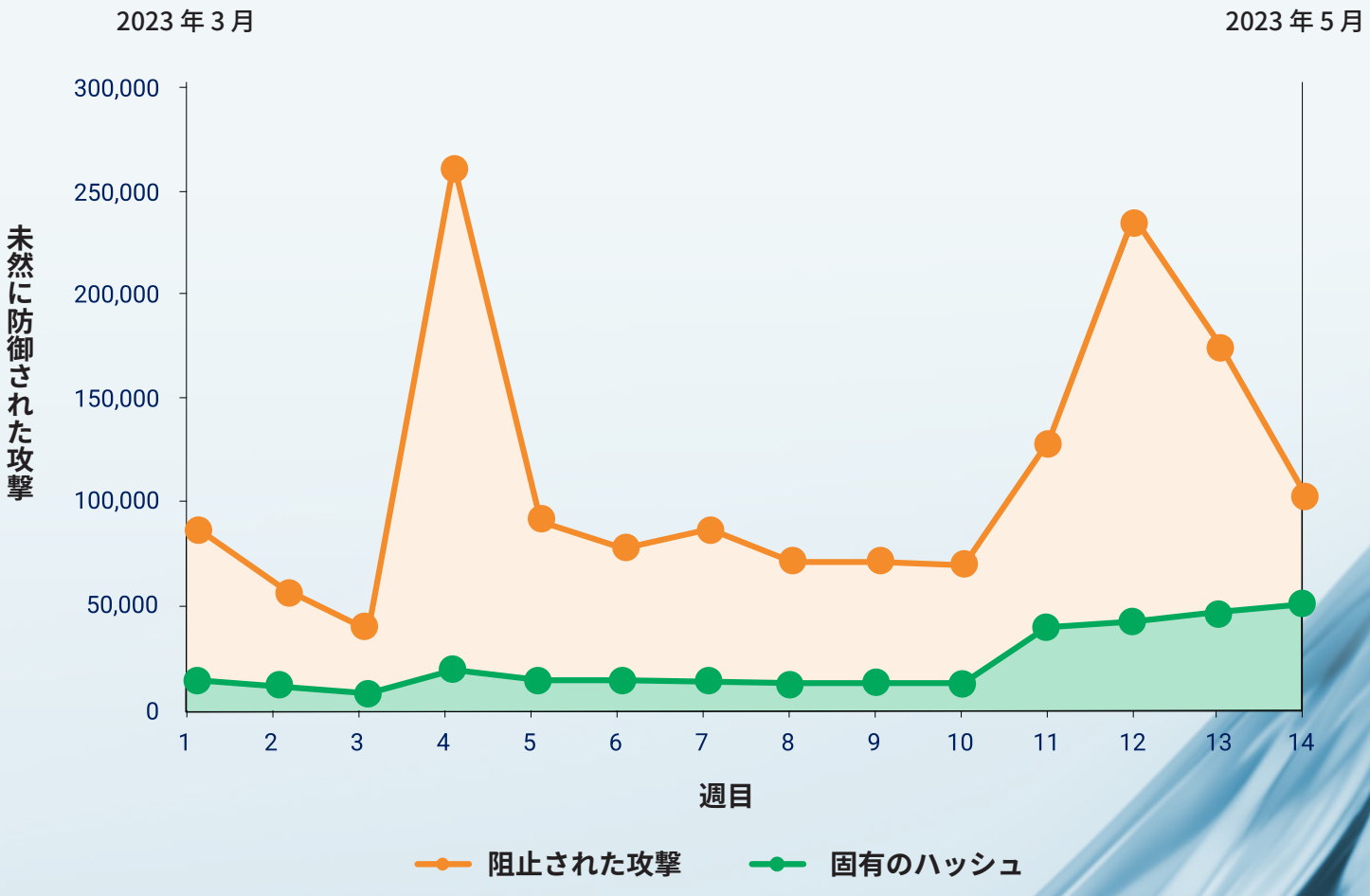

図 3：今回の調査期間中に BlackBerry が未然に防御した攻撃の推移。

脅威アクターとツール

今回の調査期間中、Cylance AI を基盤とする BlackBerry Cybersecurity ソリューションは、以下の高度な脅威アクターやツールからお客様を防御しました。

脅威アクター

APT28

Sofacy/Fancy Bear としても知られる APT28 は、高度な技術と豊富な資金を持つサイバースパイグループです。一般的には、西側諸国とその同盟国に攻撃を仕掛けることを目的に、ロシア政府の意向を受けて活動していると考えられています[36]。少なくとも 2007 年から活動しており、政府機関、軍、防衛関連企業、エネルギー企業など幅広い業界を標的としています。Operation Pawn Storm や Operation Sofacy などの持続的標的型攻撃（APT）キャンペーンへの関与も疑われています。

2015 年 11 月、APT28 は Zebrocy と呼ばれる武器を使い始めました。Zebrocy には 3 つの主要コンポーネントがあります。実行中のプロセスを発見し、悪意あるファイルをシステムにダウンロードするダウンローダとドロッパー、システム内に永続性を確立してデータを流出させるバックドアです。

Lazarus Group

Lazarus Group[37] は、北朝鮮偵察総局の諜報機関の指示で活動する、北朝鮮の国家支援型サイバー脅威グループだと考えられており、Labyrinth Chollima、Hidden Cobra、Guardians of Peace、Zinc、Nickel Academy などの別名があります。Lazarus Group は少なくとも 2009 年から活動が観測されており、2014 年 11 月、Operation Blockbuster と名付けられたキャンペーンの一環で Sony Pictures Entertainment に破壊的ワイパー型攻撃を仕掛けたのが同グループだと言われています[38]。

同グループによるシステム情報の収集、コマンドの実行、追加のペイロードのダウンロードには、Manuscrypt[39] と名付けられたカスタムのリモートアクセス型トロイの木馬（RAT）が使用されていました。

ツール

AdFind

AdFind は、Active Directory（AD）から情報を収集するオープンソースのコマンドラインツールです。「探索」段階で使用され、被害者の AD データを収集します。

Mimikatz

Mimikatz は、侵入テスト（ペンテスト）向けのオープンソースのフレームワークおよびツールで、さまざまな機能でネットワークセキュリティテストとシステムハードニングを支援します。Mimikatz によってパスワードや認証情報などの機密情報を抽出できるだけでなく、セキュリティ専門家向けのその他さまざまな機能を活用することで、Windows® ベースコンピューターにおける特権の昇格などの脆弱性を特定できます。強力な機能を数多く備えている Mimikatz は、脅威アクターによる悪意ある目標の達成によく利用されます。

Cobalt Strike

Cobalt Strike®[40] は、標的型攻撃の実行や、高度な脅威アクターによるポストエクスプロイト活動のエミュレートが可能な、攻撃者エミュレーションのための商用プラットフォームです。セキュリティ専門家の多くが、ネットワークやコンピューターシステムのセキュリティを評価およびテストするためのペンテストに Cobalt Strike を使用しています。

Cobalt Strike Beacon は軽量のファイルレスエージェントで、被害者のデバイス上に展開され、ファイル転送、キーロギング、権限昇格、ポートスキャンなどの機能を提供します。通常これらの機能は、セキュリティ専門家による脅威のエミュレーションやサイバー防御のテストに使用されますが、脅威アクターによって悪用されるケースも後を絶ちません。

Extreme RAT

Extreme RAT（別名：XTRAT、Xtreme Rat）は、リモートアクセス型トロイの木馬ツールです。ファイルのアップロードとダウンロード、レジストリ管理、シェルコマンドの実行、スクリーンショットのキャプチャ、実行中のプロセスやサービスの操作、デバイスのマイクまたは Web カメラ経由の録音などの機能を備えています。Extreme RAT は、イスラエル政府[41] とシリア政府[42] を狙った 2012 年および 2015 年の攻撃を始め、さまざまな脅威アクターによる攻撃で使用されました。

最も蔓延しているマルウェアファミリー

Windows

ドロッパー / ダウンローダ

Emotet

Emotet はこの 10 年間で進化を遂げています。最初はスタンドアロンのバンキング型トロイの木馬として登場しましたが、現在は、Epoch1、Epoch2、Epoch3 と呼ばれる 3 つのボットネットの背後で稼働する MaaS（Malware-as-a-Service）となっています。これらのボットネットは、TrickBot、IcedID、Bumblebee Loader など、別の各種コモディティマルウェアの配信メカニズムとして機能します。また、悪意ある Cobalt Strike Beacon がこれらのボットネットから展開されることもよく知られています。

過去には、悪名高い Ryuk ランサムウェアグループが TrickBot と組み合わせて Emotet を利用し、被害者の環境へのアクセスを効率化していました。Emotet は、主にスパムメールと感染済み Microsoft® Office ドキュメントを感染経路として使用します。警察当局による停止措置キャンペーンをくぐり抜け、何度かの自主潜伏を経た Emotet は、最新の脅威環境の中で今も生き残っています。

PrivateLoader

2022 年に初めて脅威環境に登場した PrivateLoader は、インストール報酬型サービスに接続されています。トロイの木馬化された「クラック版」（改変版）のソフトウェアを主な感染経路として使用する PrivateLoader は、多数のキャンペーンで使用され、RedLine、Remcos、njRAT、SmokeLoader、その他さまざまなコモディティマルウェアの配信に関わっています。誰からも望まれていない PrivateLoader ですが、BlackBerry のテレメトリを見る限り、残念ながら今後定番化する可能性が高いと思われます。

SmokeLoader

SmokeLoader は脅威環境でたびたび登場する定番の脅威で、2011 年の出現以来進化を続けながら現在に至っています。2014 年までは主にロシアの脅威アクターが、ランサムウェア、インフォスティーラ、クリプトマイナー、バンキング型トロイの木馬などさまざまなマルウェアをロードする目的で SmokeLoader を利用していました。SmokeLoader は通常、スパムメール、武器化されたドキュ

誰からも望まれていない
PRIVATELOADER
ですが、BlackBerry のテレメトリを見る限り、残念ながら今後定番化する可能性が高いと思われます。

メント、スピアフィッシング攻撃を介して配布されます。被害者のホストにインストールされた SmokeLoader は、再起動後にも消去されないための永続化メカニズムを作成し、DLL インジェクションを実行して正規プロセス内部での隠匿を図り、ホストの列挙を実行し、追加のファイルまたはマルウェアをダウンロード / ロードします。SmokeLoader には、コードの難読化などのアンチサンドボックス手法や耐解析手法も含まれています。

前回の調査期間では、ウクライナの組織を狙った攻撃で SmokeLoader が 2 回使用されたことが観測されています。この実行チェーンは、アーカイブ、おとりドキュメント、JavaScript ローダー、PowerShell（SmokeLoader ペイロードの配信用）が含まれていました。

インフォスティーラ

RedLine

RedLine は、Windows システムをターゲットとするよく知られた .NET ベースのインフォスティーラです。BlackBerry のテレメトリによれば、今回の調査期間で最も広く観測されたマルウェアファミリーの 1 つが RedLine でした。広範に蔓延している RedLine マルウェアファミリーは、グローバル脅威インテリジェンスレポートの 2023 年 4 月版でも取り上げられています。

RedLine は比較的安価なインフォスティーラで、ブラウザーに保存されたパスワード、社会保障番号、クレジットカード情報などの個人情報を、感染したシステムから抜き取ろうとします。さらに RedLine は、被害者のデバイスにインストールされているアプリケーション（セキュリティソフトウェアを含む）のリストを収集し、攻撃者に送信することができます。攻撃者はこのリストを参考に、それ以降の攻撃を計画できます。コマンド実行も可能な RedLine は、多くの場合マルチステージ型実行チェーンの 1 コンポーネントとして機能します。

RedLine はアンダーグラウンドフォーラムを通して広範に配布されています。スタンドアロン製品として、あるいは MaaS サブスクリプションパッケージに組み込まれて販売されており、本レポートの執筆時点では約 100 ～ 150 ドルで購入できます。

RedLine が現在のような需要と攻撃能力を獲得した要因は、その汎用性の高さにあります。RedLine はさまざまな方法で配信できるだけでなく、別のマルウェアの 2 段階目あるいは 3 段階目のペイロードとして展開することで、被害者のシステムの損害をさらに拡大する役割を担うこともできます。たとえば直近の数か月では、トロイの木馬化され、フィッシングメールに添付された Microsoft® OneNote ファイルを介して RedLine が配布されたケースが確認されています。

RaccoonStealer/RecordBreaker

RaccoonStealer は、ブラウザーの Cookie、パスワード、Web ブラウザーの自動入力データ、暗号通貨ウォレットデータを奪取するインフォスティーラで、ダークウェブフォーラムその他同種のプラットフォームで MaaS として販売されていることが報告されています。

RaccoonStealer の背後にいるグループは、2022 年半ばにおける運営の一時停止による空白期間を経て、RaccoonStealer 2.0 または RecordBreaker と呼ばれる RaccoonStealer の新バージョンを発表しました。現在闇市場で MaaS として配布されているこの更新版は、同グループの主張によれば、インフラストラクチャを更新し、情報窃取能力を強化し、完全にゼロから開発し直したとのことです。

Vidar

Vidar は、アンダーグラウンドフォーラムで公然と配布されている、頻繁な使用が観測されているコモディティマルウェアの 1 つです。Vidar は Arkei インフォスティーラのフォークと報じられており、標準的なファイルだけでなく、銀行情報、ブラウザーの認証情報、暗号通貨ウォレットを奪取することができます。実行された Vidar は、重要なシステム情報に加えて、ハードウェア、実行中のプロセス、ソフトウェアに関するデータを収集し、脅威アクターに送り返します。

Vidar は 2018 年の初リリース以来何度も更新を重ねていますが、全般的な機能、防御回避能力、全体的な複雑性も更新のたびに高められています。このような進化が、Vidar が脅威アクターの人気を集める理由となっています。また、Vidar を 2 段階目のペイロードとしてドロップする別のマルウェアファミリーも観測されています。

IcedID

BokBot と呼ばれることも多いバンキング型トロイの木馬です。2017 年に初めて発見されて以来数多くの進化を重ね、脅威環境で頻繁に観測される存在に成長しています。IcedID はモジュール型の特性を備えており、中核には高度なバンキング型トロイの木馬の機能があります。

頻繁に更新され、そのたびに回避能力と攻撃能力を高めている IcedID は、2023 年においても引き続き最も有力な脅威の 1 つです。さらに IcedID は、ランサムウェアや Cobalt Strike による侵害を含む、第 2 段階のマルウェアの追加ペイロードのドロッパーとしても数多く利用されています。

リモートアクセス型トロイの木馬

Agent Tesla

Agent Tesla は .NET でコンパイルされた RAT であり、脅威環境においては少なくとも 2014 年から蔓延しているインフォスティーラです。Agent Tesla は RAT のあらゆる特性を備えています。つまり多種多様なデータ（広く一般に普及しているアプリケーションのキーストローク、スクリーンショット、認証情報を含む）を盗み出して流出させることができます。

Agent Tesla の感染経路はスパムメールや武器化された Microsoft® Word ドキュメントなど複数存在し、Microsoft® Office の脆弱性を悪用して拡散する場合や、コンパイルされた HTML ファイルを介して拡散する場合もあります。前回の調査期間では、全世界の脅威環境の中で最も活発な RAT の 1 つが Agent Tesla でした。

ランサムウェア

BlackCat/ALPHV

BlackCat または ALPHV/Noberus は、2021 年に初めて存在が確認された、Rust プログラミング言語で記述されたランサムウェアファミリーです。Windows ベースと Linux ベースの両方のオペレーティングシステムをターゲットにすることができ、RaaS として販売されています。

ALPHV は、数多くの有名な企業をターゲットに被害者を増やした強力なランサムウェアです。ALPHV ランサムウェアは、ホストに感染し、回避能力を発揮して、復旧機能と報告機能のブロックを試みた後に、最終的なランサムウェアペイロードを実行します。

ALPHV が特に悪名高いのは、機密データを盗み出した後に二重恐喝の手法を使うことが理由です。暗号化済みファイルへのアクセスを回復するための身代金と、ファイルを機密のままにしておくためのさらなる身代金を支払うよう被害者に圧力をかけるのです。

ある FBI 勧告は[43]、BlackCat/ALPHV が DarkSide や BlackMatter といった以前のグループに関連している可能性を指摘しています。

これほどの人気を誇る Android は、脅威アクターにとっても魅力的な

ターゲット

であり、Android を取り巻く脅威環境はかつてないほど深刻化しています。

モバイル

Android

Android™ は、2008 年の最初のリリース以来 30 億人を超える携帯端末のアクティブユーザーが選ぶ[44]、世界市場の約 71% を占めるモバイルプラットフォームに成長しています[45]。これほどの人気を誇る Android は、残念なことに脅威アクターにとっても魅力的なターゲットであり、Android を取り巻く脅威環境はかつてないほど深刻化しています。今回の調査期間中に BlackBerry が最も頻繁に観測した Android の脅威のいくつかを紹介します。

SpyNote

SpyNote[46]（別名：SpyMax）は、被害者に対するスパイ行為のために使用されるマルウェアファミリーです。SpyNote は、モバイルデバイスから認証情報やクレジットカード情報などの機密情報を抽出できるだけでなく、ユーザーの位置情報の監視、デバイスのカメラへのアクセス、SMS テキストメッセージの傍受（脅威アクターによる 2 要素認証の回避に利用）、電話通話の監視と録音、デバイスの遠隔操作を行うことが可能です。

SpyNote は進化し続けており、SpyNote.C と呼ばれる最新バージョンは、偽アプリによって配信される SpyNote 初の亜種となりました。これらの偽アプリは、大手金融機関の正規アプリや、その他広く使用されているモバイルアプリケーションを装っています。2022 年 10 月のソースコード流出を受け、SpyNote のサンプルはモバイルを取り巻く脅威環境で大幅に増加しています[47]。

SpinOk

2023 年 5 月下旬に初めて記録された SpinOk は、マーケティングアプリのソフトウェア開発キット（SDK）を偽装した、スパイウェア機能を備えた悪意あるソフトウェアコンポーネントです。前回の調査期間では、SpinOK が数十ものアプリケーション[48]に意図せず埋め込まれるという SDK サプライチェーン攻撃が発生しています[49]。

埋め込まれた SpinOK は、ミニゲームのように見える広告を表示し、ユーザーにアプリを開き続けさせます。これにより、脅威アクターによるデバイスの中身の特定、リモートサーバーへのデータ流出、さらには脅威解析の妨害が可能になります[50]。

SMSThief

SMSThief は、デバイスのバックグラウンドで実行しながら、被害者の SMS テキストメッセージを傍受、転送、コピーできます。SMSThief の亜種は少なくとも過去 10 年間は使用されています。また SMSThief には、多額の課金が発生するプレミアムナンバーにユーザーのデバイスからテキストメッセージを送信し、被害者にプレミアムナンバー詐欺を仕掛ける能力もあります[51]。

Linux

Linux® は、ユーザーシステムではなくエンタープライズサーバー（オンプレミスとクラウドベースの両方）や IoT デバイスを中心に使用されています。最も一般的な感染経路は、パスワードのブルートフォースによる Secure Shell（SSH）アクセスの奪取や、一般公開されているサービスの脆弱性の悪用です。今回の調査期間に観測された攻撃は前回の調査期間と同様で、DDoS 攻撃、クリプトマイナー、特に VMWare ESXi サーバーを狙ったランサムウェアなどです。

Linux は脅威アクターのターゲットとして常に狙われているため、組織にはリスク軽減措置を講じる必要があります。特に優先すべきなのはセキュリティパッチを適用することです。パッチを適用することで、リモートエクスプロイトや、高度な攻撃でよく使われるローカル権限昇格（LPE）の脆弱性から Linux 環境を保護できます。リモートエクスプロイトにはバックドアなどの高度なマルウェアが含まれます。Linux 環境を狙う脅威の多くは強度の低いパスワードのブルートフォースによってアクセスを奪取しているため、効果的な脆弱性管理プログラムを導入することに加えて、強力な認証情報を要求することを推奨します。

分散型サービス妨害

今回の調査期間中、Linux システムに対する脅威で最も多く観測されたのが、マルウェアベースの DDoS 攻撃でした。展開された数が最も多かったマルウェアの亜種は、少なくとも 2016 年から活動が確認されている Mirai でした。Mirai のソースコードはアンダーグラウンドフォーラムに公開されているため、攻撃から特定のグループを突き止めることは簡単ではありません。Mirai の主なターゲットは、最新のセキュリティアップデートが適用されていない IoT デバイスです。

Gafygt[52] は、2014 年から活動が確認されている、Mirai に似たコードベースを使用する Linux ベースのボットネットです。通常は IoT ルーターなどのデバイスをターゲットとしています。XorDDos[53] は、前回の調査期間では、DDoS 攻撃で使用された最も高度なマルウェアであると同時に、最も一般的でないマルウェアでもありました。XorDDoS は、主に SSH へのアクセスのブルートフォースによって拡散します。また、システム管理者からその存在を隠匿できるルートキットを XorDDoS に含めることもできます。

クリプトマイナー

今回の調査期間中の Linux サーバーに対する脅威で 2 番目に多かったのはクリプトマイナーでした。クリプトマイナーとは、被害者のシステムリソースを使用して暗号通貨（主に Monero）を採掘する脅威アクターです。最も一般的なクリプトマイナーは、オープンソースのクロスプラットフォームソフトウェア XMRig ですが、今回の調査期間では Prometei ボットネット[54] の利用が急増したことが明らかになりました。Prometei は少なくとも 2020 年に活動が確認され、Windows 版も提供されているクリプトマイナーで、ドメイン生成アルゴリズムを使用してボットネットの停止を困難にする高度な機能を備えています。Prometei は全世界をターゲットに被害者を増やしていましたが、唯一ロシアのホストは狙われませんでした。設計当初の Prometei は、ロシア、ウクライナ、ベラルーシ、カザフスタンの CIS 諸国をターゲットから外していたと言われていますが、その後のエディションの変遷を見るともはや当初の方針は守られておらず、現在はロシアに属するデバイス以外の全デバ

イスを感染ターゲットとして設計されているようです。この動きは、ロシアの侵攻に対抗してウクライナ支持に回った国々を攻撃する方法を、親ロシア派のハクティビストが模索しているかのようです。

ランサムウェア

ランサムウェア攻撃の大部分は Windows がターゲットですが、有力な脅威グループの大部分はマルウェアの Linux 版を開発しており、それらの多くが VMWare ESXi をターゲットにしています。こうした動きは、Lockbit、Black Basta、BlackCat/ALPHV、Babuk、Royal、Hive など、複数の有力なグループに見られます。Linux バージョンを備えた新登場のランサムウェアには、Trigona[55] や Money Message[56] などがあります。

BlackBerry では、これからの新たなランサムウェアグループの多くは、Linux 版の亜種を開発したうえで活動を開始すると予測しています。つまり Linux システムがランサムウェア攻撃のターゲットになる確率は今後ますます高まると思われます。

macOS

macOS は Windows に比べて安全だと考えられていますが、実際は以前から高度な脅威アクターに狙われ続けています。詳しくは、「macOS: Tracking High Profile Targeted Attacks, Threat Actors & TTPs」[57] という題名の、RSA 2023 における BlackBerry のプレゼンテーションを視聴してください。

macOS 向けマルウェアの多くは、アドウェアの表示や Web ブラウザー検索のハイジャックなどを実行しますが、今回の調査期間を通して、クロスプラットフォームプログラミング言語を使用して macOS 自体を狙うマルウェアを開発する脅威アクターが増加していることが分かりました。たとえば BlackBerry が観測した Atomic macOS（AMOS）と呼ばれるインフォスティーラの新種は、クロスプラットフォームプログラミング言語 GoLang（別名：Go）を基盤に作成されていました。

アドウェアとブラウザーハイジャック

多くの人はアドウェアを単に迷惑なアプリケーション程度に考えていますが、バックドアなどの有害なコンポーネントをダウンロードしてインストールできるのがアドウェアです。今回の調査期間における BlackBerry のテレメトリによると、AdLoad と Pirrit が引き続き最も広く展開されているアドウェアでした。また、これらよりも古い Genieo が再び活発化していることも分かりました。Genieo は、検索バーの結果をリダイレクトし、悪意が疑われるアドウェアにユーザーを誘導するアドウェアです。アドウェアをプログラミングすることで、Web 検索を行っているユーザーを悪意ある Web サイトに誘導し、被害者のデバイスにマルウェアをダウンロードするよう促すことができます。こうした悪意あるサイトは、複製によって正規サイトと同じ外観になっている可能性もあります。たとえば最近では、脅威グループ RomCom が、正規のエンタープライズアプリケーションをホスティングしているサイトを複製し、さらにタイポスクワッティングを使用することで、実際の Web サイトのものに似た URL を作成しています。こうした偽サイトの訪問者は、一般的なソフトウェアのトロイの木馬化されたバージョンを知らないうちにダウンロードし、このソフトウェアがマシンのバックドアを脅威アクターに提供することで、情報流出へとつながっています。

Atomic macOS（AMOS）Stealer

Atomic macOS（AMOS）は、macOS をターゲットとする新種のインフォスティーラプログラムで、今回の調査期間中に出現し[58]、実際に展開されている例が観測されています。クラウドベースの人気メッセージングアプリ Telegram から購入できる AMOS は、キーチェーン、ブラウザー、暗号ウォレットからユーザー認証情報を収集し、デスクトップやドキュメントなど特定のユーザーディレクトリからファイルを流出させます。Windows プラットフォームの場合、奪取した認証情報を初期アクセスブローカー（IAB）で使用すれば、ネットワークを侵害してランサムウェアを展開することができます。現時点でこのような振る舞いは AMOS で観測されていませんが、今後発生する可能性はあります。

BlackBerry では、これからの新たなランサムウェアグループの多くは、Linux 版の亜種を開発したうえで活動を開始すると予測しています。つまり Linux システムがランサムウェア攻撃のターゲットになる確率は今後ますます高まると思われます。

最注目の攻撃事例

SideWinder がサーバーサイドポリモーフィズムを利用してパキスタン政府高官を攻撃、現在のターゲットはトルコに

BlackBerry Threat Research and Intelligence チームが 5 月上旬に公開した調査結果から、インドが発生源と見られる APT グループ SideWinder[59] によるキャンペーンの存在が明らかになりました。このキャンペーンは、パキスタン政府の人物を狙い、フィッシングメールと武器化されたドキュメントを使用する複雑な実行チェーンによって配信され、CVE-2017-0199[60] 脆弱性を悪用したリモートテンプレートインジェクションを実行するものでした。SideWinder は独自のサーバーサイド [61] ポリモーフィズムを使用してシグネチャベースの検知メカニズムの回避を試み、成功した場合、このエクスプロイトから 2 段階目のペイロードが配信されます。

このキャンペーンは 2022 年 12 月に初めて実行され、2023 年 3 月には BlackBerry Threat Research and Intelligence チームが、トルコをターゲットとした追加の SideWinder キャンペーンの証拠を発見しました。この追加キャンペーンが展開された時期は、この地域の地政学的な事象、具体的にはカシミールをめぐるインドとパキスタンの紛争で、トルコがパキスタンを正式に支援する動きと重なっていました [62]。

3CX がサプライチェーン攻撃の被害に。初期インプラントとネットワークの解析から、2022 年秋の時点で攻撃が開始されていた模様

2023 年 3 月末、ビジネスコミュニケーションサプライヤー 3CX は、大規模なセキュリティ侵害の発生を発表しました [63]。このセキュリティ侵害により、同社の VOIP ソフトウェア 3CXDesktopApp のトロイの木馬化されたバージョンが、世界中で配布されるという事態に至っているとのことです。

3CXDesktopApp は、通話、ビデオ通話、ライブチャットに幅広く使用されている音声 / ビデオ会議製品です。同社の Web サイトによると、3CX の顧客企業は約 60 万社、デイリーユーザーは 190 か国に 1,200 万人以上存在します [64]。

3CX によるセキュリティ侵害の発表 [65] は攻撃の翌日のことでした。インシデント発生後の情報更新で 3CX は [66]、この攻撃では Taxhaul（別名：TxRLoader）マルウェアが Coldcat ダウンローダとともに展開されており、攻撃自体は北朝鮮と関わりのある脅威アクター UNC4736 の関与によるものと指摘しています。

この Taxhaul は、最初に悪意あるインストーラによって配信されていました。このインストーラが依存関係ファイルを侵害することで、トロイの木馬化されたファイルへの署名が成功し、3CX の正規ファイルを偽装することに成功していたと見られます。

BlackBerry のテレメトリ、初期サンプルの解析、関係するネットワークインフラストラクチャの解析から、この攻撃は 2022 年の夏から秋の初め頃にかけて開始されていたことが判明しています。この攻撃は、オーストラリア、米国、英国の医療業界、製薬業界、IT 業界、金融業界に幅広く影響を及ぼしました。

NOBELIUM、ポーランド大使の訪米にタイミングを合わせ、ウクライナ支援の EU 各国政府をターゲットとする攻撃を展開

3 月上旬、BlackBerry の研究者は、ヨーロッパの政府機関をターゲットとするキャンペーンを観測しました。この攻撃は、ロシアの対外諜報機関 SVR との関連が判明している、NOBELIUM（APT29）として知られるロシアの国家支援型脅威アクターによるものです。

もうひとつのルアーは、情報交換や安全なデータ転送のために EU 各国で採用されている正規システム LegisWrite と eTrustEx を悪用するもので、いずれのルアーも EnvyScout という悪意ある HTML ファイルをダウンロードするよう被害者を誘導する設計になっていました [67]。

この手法では、HTML スマグリング技術を駆使して悪意あるコンポーネント（多くの場合 ISO ファイルまたは IMG ファイル）を被害者のマシンに追加配信し、機密情報の窃取を試みます。攻撃のルアーがポーランド大使の訪米に合わせた内容になっていることから、NOBELIUM が地政学的事象を利用して被害者を誘導し、感染の成功確率の向上を図っていることが分かります。

Google Ads を悪用するキャンペーンと、スペイン国税庁に偽装する大規模スピアフィッシングキャンペーン

2023 年 4 月上旬、BlackBerry Threat Research and Intelligence チームは、それぞれ意図や目的が異なる、タイポスクワッティング [68] を利用した 2 つの悪意あるキャンペーンを数か月にわたり追跡調査した結果を発表しました。

1 つ目のキャンペーンは Google Ads プラットフォームを悪用したマルバタイジング [69] キャンペーンで、少なくとも数か月前から活動していたことがわかっています。このキャンペーンの脅威アクターは、Libre Office、AnyDesk、TeamViewer、Brave などの人気ソフトウェアの偽バージョンやトロイの木馬化されたバージョンによって Vidar や IcedID などのコモディティインフォスティーラを配信していました。さらに正規の Web サイトを複製し、タイポスクワッティングによって正規 Web サイトの URL を偽装したドメイン名を割り当てることで、警戒心を持たない被害者を欺いていました。

2 つ目は、スペインの国税庁を偽装した大規模な標的型スピアフィッシングキャンペーンです。このキャンペーンの目的は、テクノロジー、建設、エネルギー、農業、コンサルティング、政府、自動車、医療、金融といった主要業界の被害者からメール認証情報を盗み出すことでした。

脅威アクターが集中的に悪用する PaperCut RCE 脆弱性

2023 年 3 月、PaperCut NG/MF バージョン 8.0 以降におけるリモートコード実行（RCE）の脆弱性が発表されました [70]。PaperCut は印刷管理ソフトウェアの開発企業で、その製品は世界中で使用されています。この RCE 脆弱性は CVE-2023-27350 として記録されており [71]、現在ではパッチも提供されています。ただし一般的な概念実証（POC）用に公開されている点と、検知が難しい点から、同ソフトウェアのパッチ未適用バージョンを実行するシステムに侵入しようとする脅威アクターにとって、理想的な感染経路となっています。

Bl00dy ランサムウェアのオペレーターによる教育機関を狙った攻撃では、この脆弱性が利用されています [72]。また、Clop や LockBit を利用するグループもこの脆弱性を有するサーバーを狙っていることが確認されています [73]。さらに 5 月上旬の Microsoft の発表によれば [74]、Mango Sandstorm や Mint Sandstorm などイランが国家として支援する複数の APT グループが、この脆弱性を積極的に悪用していることが観測されています。

法執行機関がロシアのスパイマルウェアの活動基盤を解体

米司法省は 5 月上旬、悪名高い脅威アクター Turla が使用していたインフラストラクチャが解体され、ロシアのサイバースパイ性能が大打撃を受けたと発表しました [75]。ロシア連邦保安庁（FSB）とのつながりを背景に持つ Turla は、Snake と呼ばれる高度なインフォスティーラを駆使して、北大西洋条約機構（NATO）や国連に加盟している国々の機密文書を奪取していました。Snake のインフラストラクチャに含まれるボットネットは NATO 加盟国を含む少なくとも 50 か国の感染済みシステムで発見されており、実に 20 年以上にわたって悪用が続いていたと考えられます。

この発見を受けた FBI は、Perseus（妖怪を退治するギリシャ神話の勇者）という、その役割にふさわしい名前を持つユーティリティを開発しました。Perseus を使用すれば、感染済みシステムに損害を与えることなく Snake マルウェアを無効化できます。

新たな脅威グループ「Rhysida」がチリ軍を攻撃

2023 年 5 月下旬、Rhysida と呼ばれる新たな脅威グループが、チリ軍（Ejercito de Chile）にランサムウェア攻撃を仕掛けたことが発表されました [76]。攻撃の詳細は完全には明らかにされていないものの、このランサムウェア攻撃に関与した疑いで陸軍伍長が逮捕されています [77]。

BlackBerry Threat Research and Intelligence チームが発見した侵入の痕跡（IOC）によれば、この時点で Rhysida は開発の初期段階にあると見られます。また、サンプル解析によると、Rhysida は PowerShell から .exe ファイルを実行していました。このポータブル実行可能ファイル（PE）は、レジストリキーを介したユーザーデスクトップの壁紙の変更、XOR および AES アルゴリズムを使用したファイルの暗号化、暗号化済みファイルへの Rhysida 拡張子の追加（システムの稼働停止をもたらす OS フォルダの暗号化を避ける）を試みます。また、エクスプローラーに対するプロセスインジェクションも観測されています。

これらが完了した後は、「CriticalBreachDetected.pdf」と名付けられた脅迫状が配置されます。脅迫状には、TOR ポータルから Rhysida に連絡する方法が記載されています。Rhysida は身代金をビットコイン（BTC）で支払うよう要求しており、被害者が支払いに同意した場合、身分証明書の提出と、Rhysida との連絡窓口を追加でフォームに記入することが求められます。

この発見を受けた

FBI

は、感染済みシステムに損害を与えることなく Snake マルウェアを無効化するという役割にふさわしい、Perseus という名前のユーティリティを開発しました。

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。BlackBerry が観測した、脅威アクターが採用していた上位 20 件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数が前回のレポートに比べて増えていることを意味しています。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。

MITRE 手法の全リストは、Threat Research and Intelligence の GitHub で一般公開されています。

手法名	手法 ID	戦術	前回レポートの順位	変化
1- システム情報の探索	T1082	探索	1	=
2- 仮想化 / サンドボックスの回避	T1497	防御回避	3	↑
3- セキュリティソフトウェアの探索	T1518.001	探索	4	↑
4- プロセスインジェクション	T1055	防御回避	2	↓
5- マスカレーディング	T1036	防御回避	5	=
6- リモートシステムの探索	T1018	探索	6	=
7- 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	7	=
8- ファイルとディレクトリの探索	T1083	探索	8	=
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	9	=
10- プロセスの探索	T1057	探索	10	=
11- 入力キャプチャ	T1056	収集	13	↑
12-DLL サイドローディング	T1574.002	永続化	12	↓
13- ソフトウェアパッキング	T1027.002	防御回避	14	↑
14- コマンドとスクリプトインタープリター	T1059	実行	12	↓
15- レジストリ Run キー / スタートアップフォルダ	T1547.001	永続化	19	↑
16- 暗号化されたチャネル	T1573	コマンドアンドコントロール	17	↑
17- ツールの無効化または変更	T1562.001	防御回避	15	↓
18-Rundll32	T1218.011	防御回避	16	↓
19- 難読化されたファイルまたは情報	T1027	防御回避	18	↓
20- アプリケーションウィンドウの探索	T1010	探索	20	=

上位 5 つの手法は前回の調査期間と変わらず、順位のみ変化していました。「仮想化 / サンドボックスの回避」が 3 位から 2 位に移動し、「セキュリティソフトウェアの探索」が 4 位から 3 位に移動しています。同時に「プロセスインジェクション」手法は前回のレポートから 2 つ順位を下げています。

BlackBerry Threat Research and Intelligence チームは、MITRE D3FEND に基づいて、今回の調査期間で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。

適用された防御策と緩和措置

検知手法

BlackBerry Threat Research and Intelligence チームは、今回の調査期間中に BlackBerry Cybersecurity ソリューションが阻止した 224,851 件のユニークサンプルから、脅威関連の振る舞いを検知した 386 件のパブリック Sigma ルールを特定しました。図 4 は、悪意ある振る舞いの大部分を検知した Sigma ルールの上位 10 件を示しています。

悪意ある振る舞いを検知した Sigma ルールの上位 10 件

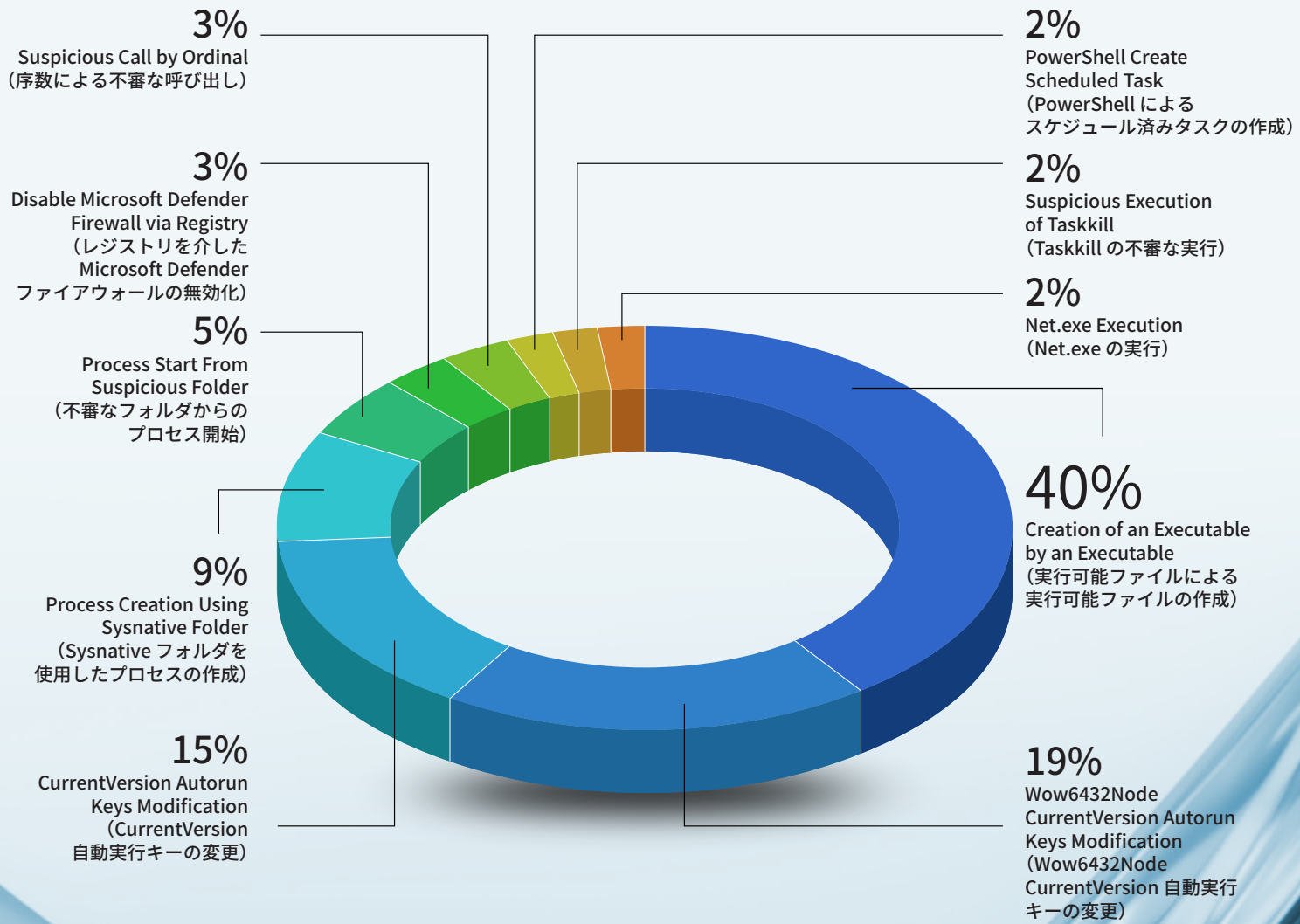

図 4：今回の調査期間中に疑わしい振る舞いを検知した Sigma ルールの上位 10 件。

Sigma ルール	説明	MITRE ATT&CK 手法	MITRE ATT&CK 戦術	前回レポートの順位	変化
1-Creation of an Executable by an Executable（実行可能ファイルによる実行可能ファイルの作成）	別の実行可能ファイルによる実行可能ファイルの作成を検知する	機能の開発：マルウェア - T1587.001	リソース開発	1	=
2-Wow6432Node CurrentVersion Autorun Keys Modification（Wow6432Node CurrentVersion 自動実行キーの変更）	レジストリ内の自動開始拡張ポイント（ASEP）の変更を検知する	起動時とログオン時の Autostart の実行：レジストリ Run キー / スタートアップフォルダ - T1547.001	永続化	2	=
3-CurrentVersion Autorun Keys Modification（CurrentVersion 自動実行キーの変更）	レジストリ内の自動開始拡張ポイント（ASEP）の変更を検知する	起動時とログオン時の Autostart の実行：レジストリ Run キー / スタートアップフォルダ - T1547.001	永続化	6	↑
4-Process Creation Using Sysnative FolderProcess Creation Using Sysnative Folder（Sysnative フォルダを使用したプロセスの作成）	Sysnative フォルダ（Cobalt Strike による生成に多く使用される）を使用するプロセス作成イベントを検知する	プロセスインジェクション - T1055	防御回避	3	↓
5-Process Start From Suspicious Folder（不審なフォルダからのプロセス開始）	一時フォルダ（複数の場合あり）など、ほとんど使用されないフォルダや一般的でないフォルダからのプロセス開始を検知する	ユーザーによる実行 - T1204	実行	5	=
6-Disable Microsoft Defender Firewall via Registry（レジストリを介した Microsoft Defender ファイアウォールの無効化）	ネットワークの利用に制約を課すコントロールを回避する目的で、攻撃者がシステムのファイアウォールの無効化や改変を行う場合がある	防御策の妨害：システムファイアウォールの無効化または変更 - T1562.004	防御回避	7	↑
7-Suspicious Call by Ordinal（序数による不審な呼び出し）	rundll32.dll エクスポート内での序数を使用した DLL の不審な呼び出しを検知する	システムバイナリプロキシ実行：Rundll32 - T1218.011	防御回避	9	↑
8-PowerShell Create Scheduled Task（PowerShell によるスケジュール済みタスクの作成）	攻撃者が Windows タスクスケジューラを悪用して、悪意あるコードの初期実行または反復実行のタスクをスケジュール設定する場合がある	スケジュール済みタスク / ジョブ：スケジュール済みタスク - T1053.005	永続化	8	=
9-Suspicious Execution of Taskkill（Taskkill の不審な実行）	Exchange や SQL Server などのサービスのデータストアに「データ破壊」や「影響拡大のためのデータの暗号化」を実行する目的で、攻撃者がサービスやプロセスを停止させる場合がある	サービス停止 - T1489	影響	該当なし	↑
10-Net.exe Execution（Net.exe の実行）	Windows ユーティリティ Net.exe の実行を検知する（疑わしいものと無害なものの両方）	複数の手法： 許可グループの探索 – T1069 アカウントの探索 – T1087 システムサービスの探索 – T1007	探索	該当なし	↑

Sigma ルール：Net.exe Execution（Net.exe の実行）

「Sysmon イベント ID 1 プロセス作成」に関連しています。この Sigma ルールは、特定のコマンドラインを含む実行を特定します。BlackBerry が観測した注目すべき振る舞いの例を以下に示します。

\AppData\Local\ の親プロセスが以下を実行：

> C:\\Windows\\system32\\net.exe view

\AppData\Local\ の親プロセスが以下を実行：

> net stop “TeamViewer”

親プロセス C:\Windows\SysWOW64\cmd.exe が以下を実行：

> net user

\AppData\Local\ の親プロセスが以下を実行：

> net group “Domain Admins” /domain

Sigma ルール：Suspicious Execution of Taskkill（Taskkill の不審な実行）

「Sysmon イベント ID 1 プロセス作成」にも関連しているこの Sigma ルールの目的は、システム内の「kill」プロセスに関連する振る舞いを特定することです。

> taskkill /F /IM chrome.exe /T

> taskkill /f /t /im <FILENAME>.exe

> taskkill /im google* /f /t

観測された振る舞いの大部分に、これはプロセスが強制終了されることを意味する /F フラグが含まれています。/T フラグは、子プロセスも終了させられることを意味します。最後は、終了させるプロセスのイメージ名を /IM パラメーターで指定しています。ワイルドカード（*）も使用できます。

Sigma ルール：Process Start From Suspicious Folder（不審なフォルダからのプロセス開始）

この Sigma ルールは、OS 内の一般的でないフォルダから開始されるプロセスを示しています。以下は一般的なフォルダの例です。

> C:\Users\<USER>\AppData\Local\Temp

> C:\Windows\Temp

この Sigma ルールに合致する一般的でないフォルダには、以下のようなものがあります。

> C:\Users\Public\Libraries（RomCom その他の脅威アクターが使用）

> C:\Users\Public

> C:\Users\<USER>\AppData\Local\Temp\~[a-zA-Z]+\.tmp\（「~[a-zA-Z]+\.tmp」は正規表現）

Sigma と MITRE の関係性

Sigma は、ログイベントとログパターンを記述できる、テキストベースのオープンなシグネチャフォーマットです。一般に、Sigma ルールは MITRE 手法にマッピングできます。また、複数の MITRE 手法を単一の Sigma ルールにマッピングすることもできます。今回の調査期間では、386 件の Sigma ルールが、220,000 万件を超える新規かつユニークなマルウェアサンプルの悪意ある振る舞いを検知しました。

これらの Sigma ルールを逆に MITRE 手法にマッピングしても、今回の調査期間における「MITRE 手法」との直接的な相関関係は確認できません。

Sigma ルールで観測された MITRE 手法の上位 5 件を以下に示します。

手法	Sigma ルールの数
起動時とログオン時の Autostart の実行：レジストリ Run キー / スタートアップフォルダ - T1547.001	14
防御策の妨害：ツールの無効化または変更 - T1562.001	11
コマンドとスクリプトインタープリター：PowerShell – T1059.001	10
コマンドとスクリプトインタープリター - T1059	9
スケジュール済みタスク / ジョブ：スケジュール済みタスク – T1053.005	9

悪意ある振る舞いを検知した 386 件の Sigma ルールに関連する MITRE の戦術を確認することで、侵入時の検知ターゲットの位置が明らかになります。実際「防衛回避」は最も頻繁に使用された戦術の 1 つであり、このことは「MITRE 手法」セクションでも確認できます。

Sigma ルールで観測された戦術

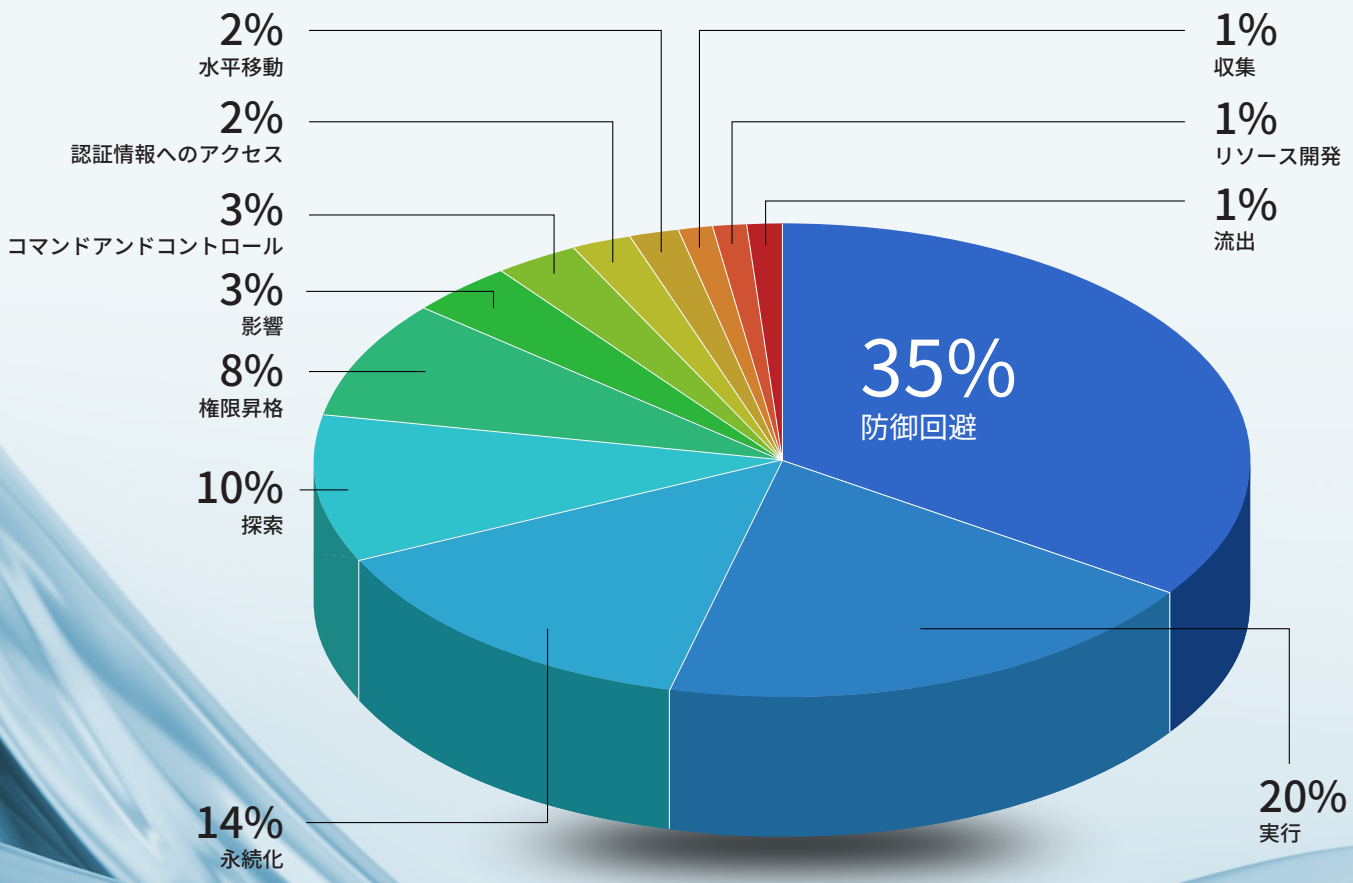

図 5：今回の調査期間中に Sigma ルールで観測された MITRE 戦術。

結論

BlackBerry のお客様を狙った悪意あるユニークサンプルは 13% 増加しています。これは、コンパイル時にツールを多様化させることに脅威アクターが意識的に取り組んでいることを示しています。このプロセスでは、類似したサンプルに対して異なるハッシュが生成されます。これにより、従来のセキュリティオペレーションセンター（SOC）が採用しているようなシンプルなフィードやフィルターを回避することができます。

BlackBerry のお客様をターゲットとする脅威アクターのうち、今回の調査期間で最も活発な動きが確認されたのは APT28 と Lazarus Group の 2 つです。いずれも国家支援型と考えられており、APT28 はロシア、Lazarus は北朝鮮とつながっていると見られます。この 2 つのグループは、特に米国、ヨーロッパ、韓国を中心とする西側諸国の政府機関、軍事組織、企業、金融機関などを狙って、これまでも長い間攻撃を展開してきました。いずれのグループも、国家の安全保障と経済的繁栄に深刻な脅威をもたらしています。また、防御を困難にする手法を両グループとも常に進化させているため、防御する組織側は、これらの脅威アクターの最新の TTP を把握し、それらを「パープルチーム演習」に取り入れて、防御戦略を強化し防御策を講じる必要があります。

今回の調査期間中、最もターゲットになった業界は医療業界と金融業界でした。金融と医療のいずれの業界でも、最も多く観測されたエクスプロイトは、認証情報を盗み、盗んだ情報を販売するインフォスティーラでした。一方で、ウクライナの救済活動に関係している病院や金融機関への攻撃も顕著でした。たとえば RomCom などのサイバー脅威グループが攻撃を仕掛けたのは、ウクライナ難民への人道支援に取り組んでいる米国拠点の医療機関でした。

ランサムウェアは、金融機関と医療機関の両方にとって現在も脅威となっています。今回と前回の調査期間における BlackBerry のテレメトリによれば、これら 2 つの業界は今後も集中して狙われる可能性が高いと見られます。

今回の調査期間で得られたサンプルを検証する中で、最も頻繁に使用された戦術は「探索」と「防御回避」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。サイバーセキュリティチームは、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

- 5 月下旬、ソフトウェア企業 Progress Software は、同社の MOVEit Transfer[78] 製品の脆弱性について顧客に通知しました。この脆弱性（CVE-2023-34362[79]）が SQL インジェクション経由で悪用されれば、権限の昇格やシステム侵害を招く可能性があります。この脆弱性は、パッチ未適用の数多くのシステムでこれまで悪用された例が観測されています。特に Clop というランサムウェアグループは、この脆弱性を利用して数百の組織に侵入したと言われています[80]。BlackBerry では、この脆弱性が解消されていないすべてのシステムにパッチが適用されるまで、脅威アクターによる脆弱性の悪用は止まらないと予測しています[81]。

- 最近の調査[82]によると、世界のモバイルバンキング市場の規模は 2026 年には 18 億 2,000 万ドルに達すると予測されています。さらにネオバンク[83]の台頭といった流れもあることから、デジタルバンキングやモバイルバンキングサービスの利用は今後 10 年にわたり増加し続けると思われます。ただし残念ながら、この成長が達成される頃には、モバイルバンキング型マルウェアも増加しているはずです。約 450 種類の金融アプリケーションをターゲットとした新たな Android ボットネットが登場する[85]など、この予測を裏付けるような事象もこの数か月の間にいくつか発生しています[84]。

- フィッシングキャンペーンの検知回避能力は、現在進行形で高度化を続けています。直近の数か月では、悪意あるコンテンツを配信する際にプロキシとして機能する Web ドメインの新規登録が増加しています。プロキシやジオフェンシングを利用して被害者になるターゲットの国や地域を絞り込むことで、不正 Web サイトの早期発見はますます困難になります。そして、この種のフィッシングキャンペーンは今後も増加すると思われます。つまり、フィッシング攻撃者が情報の奪取を開始してから攻撃が検出されるまでの時間が、今まで以上に長くなる可能性があります。

- ChatGPT などの生成 AI は、潜在的なサイバーセキュリティの問題をもたらしています。ChatGPT を使って生成された新しいマルウェアはすでに登場しています。たとえば HYAS Labs の研究者は、ChatGPT の基盤技術である大規模言語モデル（LLM）を悪用して BlackMamba[86] を概念実証として作成することに成功しています。BlackMamba は、その場その場でコードを自動的に変更することで検知を回避するポリモーフィックキーロガーです。それ以外にも、ChatGPT に対する全世界的な関心を悪用してマルウェアのインストールに一般ユーザーを誘導する脅威アクターも確認されています。たとえば Facebook Business アカウントから情報を収集する Quick access to ChatGPT[87] という悪意あるブラウザー拡張機能は、1 日に約 2,000 人ものユーザーにインストールされています。BlackBerry では、ChatGPT を利用する革新的な脅威は、2023 年の間にハイペースで増えていくと見ています。

BlackBerry がいかに組織の安全を確保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。

法的免責条項

「2023 年 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、知識の提供のみを目的としています。BlackBerry は、本レポート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。本レポートで示されている解析は、BlackBerry の調査アナリストが入手可能な情報について現時点で把握している内容を反映しており、追加情報について知るところと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誤用を一切容認しません。

謝辞

「2023 年 BlackBerry グローバル脅威インテリジェンスレポート」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。

Dmitry Bestuzhev

Geoff O'Rourke

Dean Given

Maristela Ames

Natalia Ciapponi

Jacob Faires

Jose Luis Sanchez

Pedro Drimel

Patryk Matysik

巻末注

1 https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-now-also-claims-city-of-oakland-breach/
2 https://nvd.nist.gov/vuln/detail/CVE-2023-0669
3 https://www.cybersecurity-insiders.com/details-of-a-failed-clop-ransomware-attack-on-city-of-toronto-canada/
4 https://www.reuters.com/world/europe/poland-says-russian-hackers-attacked-tax-website-2023-03-01/
5 https://www.thefirstnews.com/article/cyber-attacks-have-become-commonplace-says-govt-official-36902
6 https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/
7 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
8 https://www.fraudsmart.ie/personal/fraud-scams/phone-fraud/identity-theft/
9 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
10 https://www.clinicbarcelona.org/en/news/computer-attack-on-the-frcb-idibaps
11 https://www.bleepingcomputer.com/news/security/hospital-cl-nic-de-barcelona-severely-impacted-by-ransomware-attack/
12 https://www.scmagazine.com/news/incident-response/cyberattack-hits-spanish-pharmaceutical-company-alliance-healthcare
13 https://www.cpomagazine.com/cyber-security/fourth-largest-generic-drugs-manufacturer-sun-pharmaceuticals-hit-by-ransomware-attack/
14 https://twitter.com/vxunderground/status/1632464810863390721
15 https://www.bleepingcomputer.com/news/security/north-korean-hackers-breached-major-hospital-in-seoul-to-steal-data/
17 https://nvd.nist.gov/vuln/detail/CVE-2023-0669
16 https://www.bleepingcomputer.com/news/security/hatch-bank-discloses-data-breach-after-goanywhere-mft-hack/
18 https://www.timesnownews.com/technology-science/lockbit-3-0-ransomware-targets-fullerton-india-demand-a-staggering-2400-crores-ransom-in-just-5-days-article-99721253
19 https://www.bleepingcomputer.com/news/security/latitude-financial-data-breach-now-impacts-14-million-customers/
20 https://www.reuters.com/technology/commonwealth-bank-australias-indonesian-arm-hit-by-cyber-attack-2023-03-08/
21 https://www.bleepingcomputer.com/news/security/new-chameleon-android-malware-mimics-bank-govt-and-crypto-apps/
22 https://www.bleepingcomputer.com/news/security/xenomorph-android-malware-now-steals-data-from-400-banks/
23 https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
24 https://darktrace.com/blog/living-off-the-land-how-hackers-blend-into-your-environment
25 https://techcrunch.com/2023/04/20/3cx-supply-chain-xtrader-mandiant/
26 https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups
27 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024
28 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
29 https://www.cyber.gc.ca/sites/default/files/cyber-threat-oil-gas-e.pdf
30 https://www.cisa.gov/news-events/cybersecurity-advisories?page=0
31 https://www.reuters.com/world/americas/costa-ricas-alvarado-says-cyberattacks-seek-destabilize-country-government-2022-04-21/
32 https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a#:~:text=In%20September%202022%2C%20Iranian%20cyber,ties%20between%20Albania%20and%20Iran.
33 https://apnews.com/article/russia-ukraine-nato-technology-hacking-religion-5c2bd851027b56a77eaf9385b7d5d741
34 https://www.itworldcanada.com/article/nations-urged-to-be-responsible-in-cyberspace-after-meeting-in-vancouver/541968
35 https://www.cyber.gc.ca/en/alerts-advisories/understanding-ransomware-threat-actors-lockbit-joint-cybersecurity-advisory
36 https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed
37 https://attack.mitre.org/groups/G0032/
38 https://www.usna.edu/CyberCenter/_files/documents/Operation-Blockbuster-Report.pdf
39 https://www.cisa.gov/news-events/analysis-reports/ar20-133a
40 https://attack.mitre.org/software/S0154/
41 https://cyware.com/news/xtreme-rat-a-deep-insight-into-the-remote-access-trojans-high-profile-attacks-14dea04b
42 https://archive.f-secure.com/weblog/archives/00002356.html
43 https://www.cisa.gov/news-events/alerts/2022/04/22/fbi-releases-iocs-associated-blackcatalphv-ransomware
44 https://www.theverge.com/2021/5/18/22440813/android-devices-active-number-smartphones-google-2021
45 https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/
46 https://cyware.com/news/spynote-infections-on-the-rise-after-source-code-leak-c5d36dce
47 https://www.threatfabric.com/blogs/spynote-rat-targeting-financial-institutions
48 https://github.com/DoctorWebLtd/malware-iocs/blob/master/Android.Spy.SpinOk/README.adoc
49 https://www.cloudsek.com/threatintelligence/supply-chain-attack-infiltrates-android-apps-with-malicious-sdk
50 https://news.drweb.com/show/?i=14705&lng=en
51 https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/mobile-premium-services
52 https://threatpost.com/gafgyt-botnet-ddos-mirai/165424/
53 https://www.bleepingcomputer.com/news/security/microsoft-detects-massive-surge-in-linux-xorddos-malware-activity/
54 https://blog.talosintelligence.com/prometei-botnet-improves/
55 https://unit42.paloaltonetworks.com/trigona-ransomware-update/
56 https://blog.cyble.com/2023/04/06/demystifying-money-message-ransomware/
57 https://www.rsaconference.com/library/presentation/usa/2023/macOS
58 https://blog.cyble.com/2023/04/26/threat-actor-selling-new-atomic-macos-amos-stealer-on-telegram/
59 https://attack.mitre.org/groups/G0121/
60 https://nvd.nist.gov/vuln/detail/cve-2017-0199
61 https://nakedsecurity.sophos.com/2012/07/31/server-side-polymorphism-malware/
62 https://moderndiplomacy.eu/2023/03/26/breaking-diplomatic-norms-indian-response-to-oic-turkish-support-for-kashmir-issue/
63 https://www.3cx.com/blog/news/desktopapp-security-alert/
64 https://www.3cx.com/
65 https://www.3cx.com/blog/news/desktopapp-security-alert/
66 https://www.3cx.com/blog/news/mandiant-initial-results/
67 https://attack.mitre.org/software/S0634/
68 https://support.microsoft.com/en-us/topic/what-is-typosquatting-54a18872-8459-4d47-b3e3-d84d9a362eb0
69 https://www.cisecurity.org/insights/blog/malvertising
70 https://www.papercut.com/blog/news/rce-security-exploit-in-papercut-servers/
71 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27350
72 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a
73 https://www.bleepingcomputer.com/news/security/microsoft-clop-and-lockbit-ransomware-behind-papercut-server-hacks/
74 https://twitter.com/MsftSecIntel/status/1654610012457648129
75 https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled
76 https://www.cronup.com/ejercito-de-chile-es-atacado-por-la-nueva-banda-de-ransomware-rhysida/
77 https://izoologic.com/2023/06/19/rhysida-ransomware-exposes-stolen-data-from-the-chilean-army/
78 https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
79 https://nvd.nist.gov/vuln/detail/CVE-2023-34362
80 https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/
81 https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
82 https://www.alliedmarketresearch.com/mobile-banking-market
83 https://www.bankrate.com/banking/what-is-a-neobank/
84 https://www.cleafy.com/cleafy-labs/nexus-a-new-android-botnet#3
85 https://blog.cyble.com/2022/12/20/godfather-malware-returns-targeting-banking-users/86 https://www.darkreading.com/endpoint/ai-blackmamba-keylogging-edr-security
87 https://www.darkreading.com/application-security/chatgpt-browser-extension-hijacks-facebook-business-accounts

BlackBerry | Cybersecurity

BlackBerry について：BlackBerry（NYSE：BB、TSX：BB）は、インテリジェントなセキュリティソフトウェアとサービスを世界中の企業と政府機関に提供しています。BlackBerry のソリューションは、2 億 3,500 万台の車両を含む 5 億以上のエンドポイントを保護しています。BlackBerry はカナダのオンタリオ州ウォータールーに本拠を置き、AI と機械学習を活用してサイバーセキュリティ、安全、データプライバシーソリューションの分野に革新的なソリューションを提供しています。また、エンドポイントセキュリティ、エンドポイント管理、暗号化、組み込みシステムの分野におけるトップクラスの企業です。BlackBerry のビジョンは明確です。つながる未来に信頼性あるセキュリティを確保することです。

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

©2023 BlackBerry Limited.BLACKBERRY、EMBLEM、Design、CYLANCE などの商標（ただし、これらに限定されない）は、BlackBerry Limited、BlackBerry Limited の子会社、BlackBerry Limited の関連会社などの商標または登録商標です。これらはライセンスに基づいて使用されるものとし、このような商標に対する独占的権利が明確に留保されています。その他すべての商標は各社の所有物です。BlackBerry は、いかなるサードパーティの製品またはサービスに対しても責任を負いません。
BlackBerry Limited の書面による明示的な許可なく、本書の一部または全部を改変、複製、転送、または複写することを禁じます。