BlackBerry
Intelligent Security. Everywhere.

ホワイトペーパー

ランサムウェアは予防可能

はじめに

ランサムウェアは、コンピューターに感染してファイルを暗号化し、システムとデータにアクセスできないようにするマルウェアの一種です。ほとんどの場合、ファイルを回復するには、バックアップコピーから復旧するか、ランサムウェアの攻撃者から復号キーを購入するほかにありません。身代金（ランサム）要求への回答が遅れると、身代金を吊り上げられたり、復号キーを削除されたりして、ファイルを回復できなくなることもあります。

警察は身代金の要求に応じないことを勧めていますが、実際には身代金を支払う企業が多く存在します。その背景には、事業が妨害される度合い、顧客や株主に降りかかる可能性のある影響、復旧とクリーンアップに要するコストとの兼ね合いなどがあるほか、感染が露見した場合に当局から課される処罰の重さや、企業のブランドと評判の失墜の程度なども勘案されています。

現在、ランサムウェアは国家の支援を受けた攻撃者とサイバー犯罪組織の双方にとって主要なビジネスと化しており、マルウェアに関連したセキュリティインデントの 27%[1] を占めます。憂慮すべき統計データを以下に挙げます。

- 2021 年末までには、事業者に対するランサムウェア攻撃が 11 秒に 1 件発生するようになると予測されています。[2] さらに、40 秒に 1 件の割合でこうした攻撃が成功すると見られています。[3]
- 2020 年のサイバー脅威対策レポート[4] に回答した組織の 62% がランサムウェアの被害に遭ったと回答しています。このうち 58% の企業が身代金を支払うことを選択しました。この比率は前年から 13% 増加しています。

サイバー兵器としてのランサムウェア

BlackBerry Cylance 2020 年版脅威レポートで、ランサムウェア攻撃を仕掛ける攻撃者の手法に見られるいくつかの重要な傾向について BlackBerry の Research and Intelligence Unit が報告しています。顕著な傾向として、特定の標的を狙い撃ちする攻撃にランサムウェアが使用されていることがあります。こうした攻撃には、odinokibi、Ryuk、Zeppelin[5] などのランサムウェア群が使用されています。

この傾向が幅広い注目を集めたきっかけは、2017 年に発生した WannaCry の大流行です。[6] その後、一時的に流行は収まりましたが、現在再びランサムウェアの感染が急拡大しています。従来のランサムウェア攻撃は、個人ユーザーや中小企業を狙った金銭目的のサイバー犯罪でした。しかし、BlackBerry の Research and Intelligence Unit は、大企業、公共機関、政府機関が攻撃の対象となるケースが最近になって大幅に増加していることに注目しています。

特に巧妙な事例では、攻撃者はターゲットを慎重に選択した後、綿密な偵察によって最善の侵入経路を探します。ターゲットの環境にアクセスできるようになった攻撃者は、まず情報を盗み取るマルウェアを送り込み、機密情報を盗み出したうえで、ファイルを暗号化します。[7] 被害を受けた企業が復号ツールの購入を拒否すれば、攻撃者は盗んだ機密情報を公開すると脅して、金銭を奪おうとします。機密情報には顧客の個人情報が含まれていることが多いので、データのプライバシーが侵害されることになります。BlackBerry® のセキュリティ製品やサービスが検知または対応した攻撃の約 10% がこの戦術を利用していました。[8] 最近の事例として、Maze ランサムウェアグループが挙げられます。[9]

1 Verizon 2020 年度データ漏洩/侵害調査報告書
2 Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021（世界のランサムウェア被害は 2021 年までに 200 億米ドルに達するとの予測）
3 What It Means To Have A Culture Of Cybersecurity（サイバーセキュリティ文化が存在することが意味するもの）
4 2020 Cyberthreat Defense Report（2020 年版サイバー脅威対策レポート）
5 BlackBerry 2020 年版脅威レポート
6 WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017（WannaCry、Petya、NotPetya：2017 年のランサムウェア大流行の状況）
7 Another ransomware strain is now stealing data before encrypting it（データを盗んでから暗号化する新種のランサムウェアの登場）
8 脅威の掲示板：ランサムウェア 2020 - 現状
9 Ransomware Gangs Now Outing Victim Businesses That Don’t Pay Up（身代金要求に応じない被害企業の秘密を暴露するランサムウェアグループ）

現在でも最も多く見られる攻撃経路はフィッシングです。しかし、攻撃者が使用する TTP（Tactics, Techniques, and Procedures：戦術、技術、手順）の中には、悪意あるリンクをクリックしたり、マルウェアが仕込まれたドキュメントを開いたりしなくても感染を可能とするものが存在します。たとえば、サポート対象外になったソフトウェアを使用している VPN に侵入した攻撃者の事例がいくつかあることを、BlackBerry® Security Services のインシデント対応チームが確認しています。また、Cobalt Strike のようなファイルレス攻撃を採用する攻撃者もいます。これは、実行中のプロセスに悪意あるコードを注入することで、脆弱なシステムを乗っ取る攻撃です。こうしたメモリベースの攻撃の意図は、従来のウイルス対策製品を無力にすることにあります。つまり、エンドポイント保護をファイルのシグネチャマッチングとヒューリスティクス技術に依存する製品が狙われています。

侵入に成功した攻撃者には、コマンド & コントロール（C2）サーバーに接続するバックドアのインストールやシステムレジストリを書き換えることによる永続性の確保のほか、ネットワークの偵察、資格情報の窃盗、ラテラルムーブメントを補助するツールのロードなどの操作が可能になります。有価値のターゲットをすべて特定して盗み出した後で、ランサムウェアをインストールし、暗号化を開始します。

特定のターゲットを狙ったランサムウェア攻撃は、既知のマルウェア群を繰り返し使用する傾向があります。こうしたマルウェアの多くは、闇フォーラムで販売されているものや、サービスとしてのランサムウェア（RaaS）のベンダーから購入するものです。ほとんど場合、このようなランサムウェアの目的は金銭です。一方で、ランサムウェア攻撃の中にはプロセスやサービスを妨害することを意図したものもあります。この場合、重要なデータを破壊したり、正常に動作しない決済サービスや暗号化ルーチンを使用したりすることで、ファイルの復号や身代金の支払いを不可能にします。

巧妙なランサムウェア攻撃の分析

2018 年 8 月[10] に発見された Ryuk はランサムウェアの変種であり、悪名高いロシアのサイバー犯罪グループの関与が指摘されています。FBI（米国連邦捜査局）によると[11]、2018 年 2 月から 2019 年 10 月までの間に 6,100 万ドル相当のビットコインを被害者から脅し取っています。[12]

また、Ryuk は 2019 年 7 月の英国国家サイバーセキュリティセンター（NCSC）の勧告で、国際的脅威に指定されています。[13] この勧告では、犯罪グループがアクセスに成功した後、多くの場合、数日から数か月をかけて偵察したうえで Ryuk を解き放ち、活動状態にすることが指摘されています。一方で、上記よりも早いタイミングで Ryuk による攻撃が進行した事例も存在します。注目された事例として、最近発生したユニバーサルヘルスサービス（UHS）に対する攻撃があります。UHS は Fortune 500 に名を連ねる、医療とヘルスケアサービスを提供する企業で、1 年に約 350 万人の患者を扱っています。

攻撃を最初に報じたのは Bleeping Computer[14] で、2020 年 9 月 28 日のことです。最初の感染から 5 時間で、カリフォルニア、フロリダ、テキサス、アリゾナ、ワシントン D.C. など米国全土に存在する数百の UHS のヘルスケア施設でコンピューターシステムと電話システムが使用できなくなりました。その結果、UHS の従業員は患者の予約を延期することを迫られました。また、緊急処置室の患者を代替施設に移送することを余儀なくされたケースもあります。[15]

[10] CISA Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector（CISA アラート（AA20-302A）ヘルスケアと公衆衛生分野を狙ったランサムウェアの活動）
[11] Ransomware victims are paying out millions a month. One particular version has cost them the most（ランサムウェアの被害は 1 か月に数百万ドル。特定の亜種による被害が大多数）
[12] RSA Presentation: Feds Fighting Ransomware: How the FBI Investigates and How You Can Help（RSA プレゼンテーション：ランサムウェアに挑む FBI その調査方法と一般ユーザーができること）
[13] Ryuk ransomware targeting organisations globally（世界中の組織を狙う Ryuk ランサムウェア）
[14] UHS hospitals hit by reported country-wide Ryuk ransomware attack（全国的な感染が報告されている Ryuk ランサムウェア攻撃によって UHS の病院に被害が発生）
[15] A Ransomware Attack Has Struck a Major US Hospital Chain（ランサムウェア攻撃によって米国の大規模な病院チェーンに被害が発生）

攻撃終息後に、DFIR Report のアナリストによって次のようなキルチェーンが推測[16] されています。

1. 最初の感染の原因となったのはフィッシング攻撃です。この攻撃による被害を受けたコンピューターがマルウェア BazarLoader に感染しました。Bazar は TrickBot グループ[17] が開発したトロイの木馬型マルウェアであり、証明書に署名するコードとさまざまな難読化技術を利用して検知を回避しようとします。[18]

2. インストールされたこのマルウェアは、攻撃者の C2 サーバーに接続するバックドアを作成し、Nltest[19] をはじめとする正規の Windows ユーティリティを使用して UHS のネットワークのマッピングを開始します。Nltest は、Microsoft Windows Server のコマンドラインツールで、ドメインサーバーのリストを作成する機能があります。

3. UHS のプライマリドメインサーバーの場所を突き止めた攻撃者は、権限の昇格を可能にする脆弱性である Zerologon を悪用して管理者権限を取得します。この脆弱性は、いくつかの Microsoft Windows Server OS で発見されており、共通脆弱性評価システム（Common Vulnerability Scoring System : CVSS）では重大（スコア 10.0）に分類されています。[20]

4. 次に、Ryuk グループは Server Message Block（SMB）によるファイル転送と Window Management Instrumentation（WMI）による実行機能を使用して Cobalt Strike ツールキットを展開します。これにより、セカンダリドメインコントローラの場所を突き止め、そこに侵入できるようになります。そのドメインコントローラから、PowerShell Active Directory スクリプトを利用してドメインの検出を継続します。

5. こうしてドメインサーバーとターゲットのデータストアを特定した攻撃者は、同じ方法でセカンダリドメインサーバーの管理者権限を取得します。

6. 偵察とターゲット設定を完了した攻撃者は、RDP を使用して Ryuk の実行ファイルをプライマリ DNS サーバー、ネットワークストレージデバイス、従業員の PC に送り込みます。最後の手順として、Ryuk ランサムウェアを実行します。

[16] Ryuk in 5 Hours（Ryuk 感染から 5 時間の動き）
[17] BazarBackdoor: TrickBot gang's new stealthy network-hacking malware（BazarBackdoor : TrickBot グループの新たなネットワークハッキングマルウェア）
[18] Front Door" into BazarBackdoor: Stealthy Cybercrime Weapon（ステルスサイバー犯罪兵器 BazarBackdoor に開いているフロントドア）
[19] Microsoft command line reference（Microsoft コマンドラインリファレンス）
[20] NIST National Vulnerability Database CVE-2020-1472 Detail（NIST 脆弱性情報データベース CVE-2020-1472 の詳細）

セキュリティ意識の高い企業がすべきこと

まずは、賢明でセキュリティ意識の高い組織がすべきでないことから取り上げます。それは、すでに過剰に複雑で管理不能になっている可能性があるセキュリティインフラストラクチャに、新しいセキュリティレイヤーを追加することです。セキュリティコントロールの数が多すぎると、組織のサイバーレジリエンスが強化されるどころか低下して、意図しない結果になりかねません。IBM Security の報告[21] によると、調査対象となった組織の約 30% が 50 以上のセキュリティツールを導入していました。少数のセキュリティツールを導入している同業者と比べると、こうした組織では攻撃を検知する能力が 8% 低く、インシデント対応（IR）能力が 7% 低いという結果が出ています。

その原因として、まずアラート対応疲れがあります。また、エンドポイントなどのネットワークデバイスで生成される膨大な量の監視データとイベントデータも原因になっています。このようなデータを分析担当者がしらみつぶしに調べ、ルーチンの活動で発生する無作為のノイズに潜む脅威の兆候を見つけ出すことなど不可能です。

したがって、ビジネスとセキュリティを主導する部門が組織のサイバーリスクの大きさとリスク耐性を十分に把握するまで、新たなセキュリティ対策を導入するべきではありません。

計画と分析からの着手

多くの場合、BlackBerry のエキスパートは、まずセキュリティ侵害診断（CA）業務をお客様にお勧めします。これにより、リスク要因の特定と、今後のセキュリティのアップグレードを検討するためのベースラインの設定が容易になります。セキュリティ侵害診断では、脅威ハンティングと攻撃対象領域削減という 2 つの分野を扱うべきです。重点的に取り組む点は以下のとおりです。

- データの外部流出とデータ利用の妨害
- コマンド & コントロール攻撃
- ユーザーアカウントの異常な挙動
- マルウェアとその永続化メカニズム
- 設定に脆弱性があるネットワーク、ホスト、アプリケーション

セキュリティ侵害診断の所見と推奨事項をレビューする際には、お客様の組織でセキュリティとビジネスを主導している部門の参加が推奨されます。

- **脅威ハンティングによる所見**：過去または現在のセキュリティ侵害が検知された場合、その内容や範囲と環境に対する影響を詳しく確認します。
- **攻撃対象領域の削減による所見**：企業の総合的なセキュリティ体制を改善するための戦術的および戦略的な推奨事項を確認します。それと同時に、攻撃対象領域を削減できる余地を、リスクを優先的な要素として評価します。たとえば、セキュリティ侵害診断では、重大な脆弱性（Zerologon など）があるシステムを要注意として指定し、段階を追った改善指示を実施します。

[21] サイバー・レジリエンス・レポート（2020 年版）

IBM の調査[22] によると、今日の組織の「大多数」は重大なセキュリティインシデントに効果的に対応する備えができていません。また、2020 年に IBM が実施した調査[23] では、悪意のある攻撃によって発生したデータ侵害を企業が特定し、封じ込めるまでに平均で 315 日を要していることが判明しています。こうした対応時間を短縮することが、事業のレジリエンス強化に必要不可欠です。これは損益にも影響します。インシデントを 200 日未満で解決した組織は、解決に時間を要した組織と比べて平均で 112 億ドルのコストを節減することに成功しています。[24]

こうした問題に取り組むにあたり、BlackBerry は、お客様に自社のセキュリティ対策チームの能力を明確に評価することをお勧めしています。具体的には、セキュリティ侵害を特定し、それを封じ込めて根絶し、侵害から復旧する能力を確認します。調査プロセスで取り上げる項目は、担当者からの聴き取り、セキュリティポリシーに潜むギャップの分析、お客様に応じたインシデント対応（IR）演習を通じたセキュリティ対策チームの能力評価です。こうした調査結果を基に、業界のベストプラクティスと規制基準に適合するようにインシデント対応計画を再考する必要があります。

こうした分析は重要ですが、実戦さながらの現実的な攻撃シナリオによってセキュリティ対策チームの能力をテストすることも欠かせません。たとえば、BlackBerry Security Services は侵害のシミュレーションと攻撃者のシミュレーションの両方を提供することで、お客様の多様な要望に応えます。セキュリティ対策能力の実践演習、セキュリティ上の仮定の検証、セキュリティ体制に潜むギャップの特定を目指す組織には侵害シミュレーションが最適です。自社の業界に頻繁に攻撃を仕掛けている現実の攻撃者グループの攻撃を検知し、対処する経験を積んでおくことを目指す組織には、攻撃者シミュレーションが最適です。

BlackBerry Security Services の構成に関する詳細は、弊社のウェブサイトをご覧ください。

BlackBerry Protect によるランサムウェアインシデントの予防

攻撃者は悪意のあるスクリプトでシステムの脆弱性を突いたり、マルウェアを利用したりして、ランサムウェアをインストールしようとします。ランサムウェアインシデントの発生を予防する最も効果的な方法は、このようなインストールを阻止することです。BlackBerry® Protect はエンドポイント保護プラットフォーム（EPP）ソリューションであり、洗練された人工知能（AI）技術と機械学習（ML）技術を利用して、こうした手口を阻止します。

BlackBerry のアジャイルな統合エージェントによってエンドポイントに展開された BlackBerry Protect は、ファイルを実行しても安全かどうかを数ミリ秒で判定します。安全であれば、ファイルを実行できます。安全でなければ、ファイルの実行は阻止されます。そのファイルは隔離され、BlackBerry® Cyber Suite の管理コンソールにアラートとその発生の経緯に関するデータが表示されます。このファイル検知プロセスはエンドポイント単位で実行され、そこで使用されるシステムリソースは最小限に抑えられています。リモートデータベースの参照、継続的なアップデート、クラウドへの接続などは不要です。BlackBerry Protect の AI モデルはオープンネットワーク環境と分離されたネットワーク環境の両方で、マルウェアとランサムウェアを検知し、その実行を阻止します。

[22] IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them（IBM 調査結果：整備したサイバーセキュリティ対応計画をテストしている組織は全体の半数未満）
[23] IBM Security：2020 年「情報漏えいのコストに関する調査」レポート
[24] IBM Security：2020 年「情報漏えいのコストに関する調査」レポート

BlackBerry Protect は、悪意あるファイルの実行を防止するだけでなく、攻撃者が悪意あるコードをシステムメモリに注入して実行することも阻止できます。これは、実行中の 32 ビットおよび 64 ビットのプロセスをすべて監視し、脆弱性を利用した多くの攻撃に伴う挙動を発見することで実現しています。メモリ侵害を検知した BlackBerry Protect は、その侵害によって発生する関数呼び出しを阻止し、その関数が実行される前に適切な是正措置を実行できるようにします。この是正措置として、違反警告を無視して実行を許可するものから、該当のプロセスを全面的に停止するものまであります。このような各種機能によって、攻撃者が Bazar などのマルウェアを利用して正規のシステムサービスを乗っ取り、目的を達成することを阻止します。

また、BlackBerry Protect は、UHS に対する攻撃で使用されたような悪意ある PowerShell、Active Scripts、Microsoft Office のマクロスクリプトの実行も防止できます。通常、スクリプト制御ポリシーは、管理者がさまざまな条件を指定できるように警告モードに初期設定されています。その条件として、どのスクリプトを制御対象とするか、誰がスクリプトを使用するか、スクリプトの実行を許可するか、許可する場合はどのような条件で実行できるようにするかなどがあります。こうした調査が完了すると、遮断モードを使用できるようになります。このモードでは、特定のフォルダーにインストールしたスクリプトと、例外ルールに従って明示的に指定したスクリプトを除き、どのスクリプトも実行できません。

侵害された大容量記憶装置を通じて、ネットワーク上にランサムウェアが導入されることもあります。BlackBerry Protect のデバイス管理ポリシーを利用すると、許可されていないソフトウェアがインストールされること、データが外部に持ち出されること、不注意で感染したデバイスの接続によって業務システムが危険にさらされることを防止できます。これにより、感染リスクを最小限に抑えることが可能です。BlackBerry Protect のデバイス管理ポリシーは、大容量記憶装置を対象としています。マウスやキーボードなどの周辺機器は影響を受けません。

BlackBerry Protect のアプリケーション制御機能を利用すると、攻撃者によるマルウェアのインストールや、OS、ファームウェア、プロトコルスタック、周辺アプリケーションの改変を阻止できます。これにより、組織が保有する固定機能デバイスを、感染とは無縁の状態に維持できます。

BlackBerry Optics によるランサムウェアの脅威ハンティング、修正、復旧

ランサムウェア攻撃の阻止に BlackBerry Protect が有効でありながら、BlackBerry® Optics のようなエンドポイント検知/対応（EDR）ソリューションが必要なのでしょうか。

第一に、BlackBerry Protect は、マルウェアの実行防止に 99% 以上の効力[25] を発揮しますが、100%ではありません。言うまでもなく、これは小さくても重要な差です。そのため、防御の第一線を突破したランサムウェア攻撃を封じ込め、その状態を容易に調査できるようなシステムを配置することは実に賢明な選択です。

第二に、脅威の性質は変化し続けています。Verizon は「2020 年度データ漏洩/侵害調査報告書」[26] で、攻撃者が使用した戦術を分析したところ、「データの漏洩と侵害にマルウェアが占める割合は、過去 5 年間、一貫して着実に減少している」との結論を出しています。また、「攻撃の 45% がハッキング、データ漏洩/侵害の 22% が日常のエラー、22% がソーシャルエンジニアリング攻撃、17% がマルウェア関連」であるとしています。

[25] NSS Labs Advanced Endpoint Protection Cylance Security Value Map（NSS Labs：先進的なエンドポイント保護製品：Cylance Security Value Map、2018 年 4 月）
[26] 2020 年度データ漏洩/侵害調査報告書

だからといって、攻撃手段としてのマルウェアが消滅しつつあるわけではありません。攻撃者が Portable Executable 形式の実行可能ファイルを必要としない TTP を、少なくともキルチェーンの初期段階で利用するようになっているにすぎません。

BlackBerry Optics は、BlackBerry Protect の脅威防御能力を拡張した EDR ソリューションであり、真の AI によるインシデント防御、根本原因分析、スマートな脅威ハンティング、自動検知と自動対応の機能を提供します。BlackBerry Optics は、他の EDR 製品とは異なり、オンプレミス設備への高額な投資や、クラウドへの継続的なデータストリーミングを必要とする対症療法的なアプローチは不要です。その代わり、BlackBerry Optics はエンドポイントに検知/対応ロジックを適用して、インシデント対応までの遅延時間を解消します。迅速な対応をとることができれば軽微なセキュリティイベントで終わる現象であっても、このような遅延時間があるがために、制御不能で重大なセキュリティインシデントに発展することがあります。

BlackBerry Optics は、ランサムウェアの脅威を検知するため、コンテキスト分析エンジン（CAE）を備えています。CAE はエンドポイントのイベントをほぼリアルタイムに監視することで、悪意ある活動や疑わしい活動を特定します。CAE には BlackBerry 監修の実装済み検知ロジックのセットが付属します。このロジックにより、多種多様なインシデント対応を開始できます。このロジックには、BlackBerry のインシデント対応チームが実際に調査して解決した現実の攻撃に由来するルールや、BlackBerry の脅威調査担当者が解析して記録した攻撃に由来するルールが組み込まれています。たとえば、BlackBerry の Threat Research Unit が BlackBerry Optics 向けに作成したカスタムルールを適用すると、Ryuk マルウェアの変種が使用する手口を追跡し、被害を軽減できます。[27]

検知ルールは必要ですが、ルールによってあらゆる攻撃の挙動をモデル化することはできません。そのため、BlackBerry Optics には、BlackBerry の Data Science チームが開発した機械学習による脅威検知モジュールが組み込まれています。このモジュールは、絶えずエンドポイントの挙動を分析することで、きわめて巧妙なランサムウェア攻撃グループが使用するゼロデイ攻撃、APT、Living off the Land（自給自足/環境寄生型）攻撃などを検知できます。

CAE ルールまたは機械学習によって脅威を検知した BlackBerry Optics は、オンデマンド対応と自動化対応の両方を開始します。このような対応として、フォレンジックデータの収集やシステムのオフライン化をはじめとして、ランサムウェアの感染拡大を調査し、解決するうえで必要な各種の機能があります。

インシデントが検知された場合、それを徹底的に調査し、キルチェーンのすべての段階を把握する必要があります。キルチェーンに対するこれらの知見を、その後の封じ込め作業や復旧作業に取り入れます。BlackBerry Optics には手動と自動両方のインシデント調査ツールが用意されているので、脅威ハンティングの分析と根本原因の分析を効率的に実施できます。

たとえば、セキュリティチームが InstaQuery （IQ）検索を使用してフォレンジック関連データを収集できるので、脅威ハンティングのプロセスが簡潔になります。IQ はあらゆるエンドポイントからデータを収集して結果を集計できる軽量なツールです。この集計した結果を、脅威の経緯がわかる形式と直感的な形式の両方で分析に持ち込むことできます。

[27] Ryuk Malware Optics Rules（Optics で Ryuk マルウェアを検知するためのルール）

最近、ある大企業がランサムウェアの被害に遭ったとき、BlackBerry のコンサルタントが IQ を使用して、その被害の調査とそこからの修正を支援しました。調査開始から数秒で、主要な IOC（ランサムウェアのファイル拡張子）が米国にのみ出現していることを担当チームが確認しました。これにより、依頼者と BlackBerry のチームは米国のみを対象に調査、修正、クリーンアップを進めればよいことを判断できました。この事実がわからないと、欧州、アジア、南太平洋にわたって依頼者の業務環境を診断することになり、時間を浪費することになったはずです。さらに、BlackBerry のコンサルタントは、ランサムウェアをただちに検知して速やかに隔離できようにするカスタムルールを作成して配布しました。これにより、今後の感染防止策の構築を支援しています。

ランサムウェアによるインシデントの予防に BlackBerry のアプローチを採用する利点

BlackBerry がランサムウェア対策として用意しているソフトウェアとサービスの各種ソリューションにより、次の利点が得られます。

- ランサムウェアの実行や、ランサムウェアが正規のシステムサービスを悪用して感染の足場を確保し、ネットワークに感染を広めることを防止できます。
- 検知、応答、修正の自動化ルーチンを導入して、事前対応型の脅威ハンティングと根本原因分析を支援することで、ランサムウェアによる被害を食い止めることができます。
- ランサムウェアによるインシデントに迅速に対応できます。ミッドティアプロバイダや大規模なコンサルティング会社によるセキュリティ侵害への対応では、その完了まで数週間も待たされることがあります。その間にも被害は拡大し、復旧とクリーンアップのコストは増大していきます。BlackBerry のランサムウェアエキスパートであれば、ご依頼にただちに対応し、業界最高クラスの一貫したサービスを提供します。
- 最高情報セキュリティ責任者（CISO）とセキュリティチームが必要とする指導とサポートをエキスパートから受けることで、お客様がさらされるリスクを最小限にすることができます。こうした指導とサポートによって、お客様のセキュリティ体制にある欠落箇所を特定して排除し、サイバー防御を強化できます。また、インシデント対応に向けた堅牢なプロセスを実装し、対症療法的なセキュリティ体制から予防優先のセキュリティ体制へ効率的に移行できます。

結び

実際のところ、ランサムウェアインシデントは予防可能だと、どこまで言い切れるでしょうか。それは、予防という概念をどのように捉えているかによって大きく異なります。ランサムウェア攻撃を遮断できる魔法のスイッチを入れることだと考えているとしたら、残念ながら失望することになります。しかしながら、BlackBerry では、ほとんどすべてのランサムウェア攻撃はキルチェーンが配信された段階で完全に阻止できると考えています。ただし、攻撃を無力にする実践的な手法を取ることが条件です。

その手法は、コンピューティングインフラストラクチャを徹底的に評価し、サイバーリスクを特定して各リスクに優先順位を割り当てることから始まります。広く知られた脆弱性があるシステムにはパッチを適用して、悪用されないようにする必要があります。システム構成の誤りにも同様に対処します。たとえば、BlueKeep 脆弱性[28] を防ぐために、RDP システムへの外部からのアクセスを禁止する必要があります。

基本的な遮断と捕捉の処理も無視するべきではありません。ソーシャルエンジニアリング攻撃に対抗するには、従業員に対する持続的なトレーニングが必要です。現代の基準を満たさないようなパスワードポリシーは、多要素認証や連続認証の技術を導入することで強化します。さらに、セキュリティ診断にも継続的に全力で取り組む必要があります。これは、新たな脅威やデジタルトランスフォーメーションプロジェクトによって組織が新種のサイバーリスクにどのようにさらされるかを見極めるためです。こうした構想には長期的な取り組みが必要ですが、結果的に長期的な利点が得られます。

一方で、すぐに取り入れることで中短期的な利点が得られる対策も存在します。BlackBerry Protect はランサムウェアだけでなく、ランサムウェア攻撃者が攻撃の最初の足場を築くために使用するファイルレス攻撃も検知して阻止できます。巧妙な攻撃を防ぐうえで人工知能と機械学習が大きな効果を発揮します。攻撃が何らかの手段で組織の防御をすり抜けたとしても、対応と修正の自動化ルーチンを BlackBerry Optics が素早く発動し、セキュリティ侵害が大規模なセキュリティインシデントに発展することを防止します。

したがって、ランサムウェアの予防は可能であり、実際に予防が機能しています。

ランサムウェアからの防御と修正のために BlackBerry が用意している各種ソリューションの詳細をこちらでご覧ください。また、緊急の支援が必要な場合は、03-5575-1511（代表番号）までお問い合わせください。

ランサムウェア防御に関する BlackBerry の詳しい見解や、BlackBerry のリソースの詳細については、弊社ウェブサイトをご覧ください。

[28] NIST Vulnerability Database CVE-2019-0708（NIST 脆弱性情報データベース CVE-2019-0708）

BlackBerry について

BlackBerry（NYSE : BB、TSX : BB）は、インテリジェントなセキュリティソフトウェアおよびサービスを世界中のエンタープライズと政府機関に提供しています。現在 BlackBerry がセキュリティ保護しているエンドポイントの数は 5 億台を上回り、そのうちの 1 億 7,500 万台は道路を走行する車両です。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。

BlackBerry
Intelligent Security. Everywhere.

MKTG 19-0108 | 210115