BlackBerry
Intelligent Security. Everywhere.

事例

コーザッド地域医療システムが、BlackBerry の支援により、ランサムウェア攻撃を阻止

著者の注記：BlackBerry は、2019 年 2 月 21 日に Cylance の買収を完了し、現在、CylancePROTECT® ソリューションを BlackBerry®Protect という新たなブランド名で販売しています。この導入事例では、Cylance の組織と、そのブランドの製品およびサービスはすべて、BlackBerry のブランド名で示しています。

2018 年 12 月の回想シーン：コーザッド地域医療システム（Cozad Community Health System ： CCHS）の IT 部長 Jamion Aden 氏が、深夜に、デスクトップ管理者の Dustin Holbein 氏からの緊急連絡で目を覚まします。コーザッド地域病院の緊急治療室（ER）のスタッフから、より高度な治療をするために患者を別の施設に転送する必要があるが、必要な書類をプリントアウトできないために患者を送れない、という報告があったとのことです。スタッフは早急の支援を要請しています。Holbein 氏は、この時点ですでに、印刷の問題は ER だけで起きているのではないと判断していました。院内のネットワークに接続されたすべてのプリンターがオフラインになっていました。また、Holbein 氏は、ER のファイルサーバーとプリントサーバーで、奇妙な拡張子を持つ見慣れないファイルが動作していることにも気づいていました。

コーザッド地域医療システム（Cozad Community Health System ： CCHS）

業種：

医療

場所：

アメリカ合衆国

製品：

BlackBerry® Protect

展開：

300 台のエンドポイント

Web サイト：

https://cozadhealthcare.com

CozadCommunity
HEALTH SYSTEM

Aden 氏はすぐに、これらのファイルはマルウェアだと認識します。Aden 氏のチームは、感染したサーバーをただちにシャットダウンするとともに、これらのサーバーとそのサブネットを CCHS 企業ネットワークから分離するためのファイアウォールルールを展開します。この措置によって、マルウェアの複製と拡散が阻止されます。

とっさの判断と果断な行動によって、CCHS は、患者の治療に支障を来たし、患者データを損ない、復旧と修復に何万ドルものコストを強要する Ryuk ランサムウェア攻撃を回避することができました。

「ラッキーでした」と、Aden 氏は当時を振り返って述べています。「もっと悪い結果になっていたかもしれません。データを何も失うことなく、すばやく復旧することができました。しかし、この攻撃は、私たちが有効だと信じてきたエンドポイント防御策が、思ったほど有効ではない可能性があることを示す警鐘となりました」氏の懸念は事実に基づいていました。

「ログをチェックして、既存のアンチウイルスが最新のシグネチャファイルを実行していることを確認しました」と、Aden 氏は言います。「Ryuk は 4 か月前に正式に特定されていましたが [1]、アンチウイルスベンダーはこの検知を可能にするハッシュや証明書をまだリリースしていなかったため、防御をすり抜けてしまったんです。もはやシグネチャベースのツールには頼れないのは明らかでした」

「BlackBerry Protect の導入を、最初から最後まで 1 週間足らずで完了できました」

- Jamion Aden 氏
（コーザッド地域医療システム、情報テクノロジー部長）

米ネブラスカ州中部地域の包括的な医療ソリューション

CCHS には 5 つの施設があります。コーザッド地域物理治療院（Cozad Community Physical Therapy）、コーザッド地域病院クリニック（Cozad Community Hospital Clinic）、コーザッド地域メディカルクリニック（Cozad Community Medical Clinic）、セントラルプレーンズホームの医療とホスピス（Central Plains Home Health & Hospice）、メドーラークポイント介護施設（Meadowlark Pointe Assisted Living）です。「私たちは、ネブラスカ州ドーソン郡の地域に包括的な医療ソリューションを提供できることを誇りに思っています」と、Aden 氏は言います。該当地域には、コーザッド市、オーバートン市、ジョンソンレイク市、レキシントン市が含まれ、ドーソン郡のおよそ 2 万 3,500 人の人口の約半数がこれらの市に住んでいます。[2]

IT 部長の Aden 氏は、CCHS のコンピューティングおよびネットワーキングインフラストラクチャの責任者です。「Dustin のほかに、電子医療記録（EHR）システムを管理する情報科学担当者が 1 人おり、また点滴ポンプやバイタルサイン機器など、ネットワークに接続された医療機器のメンテナンスをサードパーティ企業数社に支援してもらっています」と、氏は言います。「しかし、最終的に、『丁寧で、誠実で、思いやりがあり、助けになる』高品質のケアを提供するために必要なコンピューティングリソースに、200 人の従業員が常にアクセスできるようにすることは、Dustin と私の役目です」

CCHS のエンドポイント防御策をアップグレードするという新年の決意の成就

ランサムウェア攻撃を阻止してからわずか 2 か月後の 2019 年 2 月、Aden 氏はより効果的なエンドポイントセキュリティソリューションを探し始めました。

「およそ 1 か月かかって、必要なものは何かがわかりました」と、Aden 氏は言います。「ゼロデイ脅威を阻止できるのは人工知能（AI）ベースの製品しかないことがわかったため、BlackBerry や他の次世代製品のプロバイダーと会い、各社の AI テクノロジーを評価しました。また、私たちのチームが小規模であることを踏まえて、管理しやすいソリューションを選択する必要もありました」

評価を終えた Aden 氏は、CCHS の新たなエンドポイントセキュリティソリューションとして、BlackBerry® Protect を選択しました。 Aden 氏は次のように語っています。「BlackBerry の AI テクノロジーに感銘を受けました。BlackBerry Protect は、送り込んだすべてのマルウェア亜種を阻止したのです。

また、直感的に操作できる管理コンソールや、容易な導入プロセスも気に入りましたし、スクリプトベースの攻撃、ファイルレス攻撃、悪意のあるデバイスベースの攻撃を阻止するための追加のセキュリティ対策もよいと思いました」

3 月に、CCHS は正式に顧客として契約しました。数週間後、BlackBerry Protect の展開が開始されました。

「導入を私たち自身で問題なく行えました」と、Aden 氏は言います。「BlackBerry Protect エージェントの展開後、数日かけて、環境のスキャンと、5 つの施設に適用する新しいグループポリシーの定義を行いました。その後、たった 1 日で、300 のエンドポイントすべてにポリシーを送信することができました。各エンドポイントは、再起動するとすぐに保護された状態になりました。BlackBerry Protect の導入を、最初から最後まで 1 週間足らずで完了できました」

新たなグループポリシーでは、最新のランサムウェアの脅威アクターが使用する戦術や手法に対する BlackBerry Protect の防御機能がフル活用されます。たとえば、ランサムウェアのグループは、しばしば、PowerShell などの正規のシステムサービスを乗っ取ることによって、攻撃者が管理するコマンドアンドコントロール（C2）サーバーへのバックドア接続を確立しようとします。Aden 氏は次のように語っています。「これを未然に阻止するために、システム管理者以外は PowerShell コマンドを実行できないようにする BlackBerry Protect のスクリプト制御ポリシーを作成しました。悪意のある Web ページや武器化したドキュメントが従業員のマシンで PowerShell スクリプトを実行しようとすると、BlackBerry Protect によってこの実行が自動的に阻止されます」

Aden 氏はまた、BlackBerry Protect を活用して CCHS ソフトウェア制限ポリシーを適用しています。「私たちのシステム構成はめったに変わることがないため、ほとんどのマシンで BlackBerry Protect のアプリケーション制御ポリシーを有効化しました」と、Aden 氏は言います。「その結果、従業員が不正なアプリケーションをインストールすることによって、システムが攻撃にさらされたり、パフォーマンスの問題が発生したりすることを、もう心配しなくてもよくなりました」

「BlackBerry の AI テクノロジーに感銘を受けました。BlackBerry Protect は、送り込んだすべてのマルウェア亜種を阻止したのです。また、直感的に操作できる管理コンソールや、容易な導入プロセスも気に入りましたし、スクリプトベースの攻撃、ファイルレス攻撃、悪意のあるデバイスベースの攻撃を阻止するための追加のセキュリティ対策もよいと思いました」

- Jamion Aden 氏
（コーザッド地域医療システム、情報テクノロジー部長）

データの盗難対策としては、BlackBerry Protect のデバイス使用制御機能がシステム全体で活用されています。「ウイルスに感染した USB ドライブを持ち込んでシステムを感染させたり、プライバシールールに違反して患者データをダウンロードしたり盗んだりするチャンスを与えてしまうようなリスクを冒すわけにはいきません」と、Aden 氏は言います。「現在、USB メモリは、私たちの直接的な監視下以外では使用できないようになっています」

BlackBerry Protect は、エンドポイント管理の合理化においても Aden 氏の期待を上回る成果を挙げています。「以前は、シグネチャの更新ファイルのインストールと監査に、毎日 2 時間くらい費やしていました。現在では、1 日 5 分ほど時間を取って、BlackBerry Protect のコンソールで脅威の痕跡はないかチェックするだけで、継続的な予防状況を確認することができます」

現在の課題

2 年前の 12 月の深夜に Holbein 氏が Aden 氏に連絡をしたときから、状況は大きく変化しました。ドーソン郡で、レキシントン市を中心として COVID-19 の広範囲の流行の初期兆候が見られる中 [3]、CCHS の医療提供者たちは、パンデミックとの戦いの最前線で 2020 年のホリデーシーズンを過ごしました。「この危機の中で、医療提供者やサポートスタッフが示した勇気と献身に心を打たれました」と、Aden 氏は言います。「彼ら全員に感謝しています」

氏はまた、パンデミックの発生以降、CCHS のような医療機関は、民族国家やサイバー犯罪組織の脅威グループの主要な標的となっていることを認識しています。「サイバーセキュリティ・インフラストラクチャセキュリティ庁が最近発表した警告 [4] は、これを明確に示しています」と、Aden 氏は言います。「ありがたいことに、私たちには、BlackBerry Protect がシステムとデータのセキュリティを静かに守ってくれているという安心感があります」

Aden 氏は、効果的なサイバー防御策だけでは堅牢なセキュリティ体制の保証はできないことを認識しています。「セキュリティ文化を確立する必要があり、そのためには、経営幹部の後援とサポートが必要です」と、Aden 氏は言います。「幸いなことに、CCHS の経営陣は、医療提供者として私たちが直面しているセキュリティの課題を完全に理解し認識しています。経営陣から信頼されていることを誇りに思っています」

詳細については、BlackBerry.com/Spark をご覧ください。また、Twitter アカウント @BlackBerrySpark をフォローしてください。

著者の注記：Ryuk は、悪名高いロシアのサイバー犯罪組織 [5] に関連する、悪質で捕捉が困難なランサムウェアの一種であり、Ryuk により、2018 年 2 月から 2019 年 10 月の間にビットコインによる 6,100 万ドル以上の支払いが被害者に強要されました。[6]Ryuk は、英国の国家サイバーセキュリティセンター（NCSC）による 2019 年 6 月の勧告でも世界的な脅威として挙げられています。[7]Ryuk やその他の高度なランサムウェアの詳細については、BlackBerry Threat Bulletin: Ransomware 2020- State of Play （BlackBerry 脅威速報：ランサムウェア 2020 - 現状）をご覧ください。

> 「以前は、シグネチャの更新ファイルのインストールと監査に、毎日 2 時間くらい費やしていました。現在では、1 日 5 分ほど時間を取って、BlackBerry Protect のコンソールで脅威の痕跡はないかチェックするだけで、継続的な予防状況を確認することができます」
>
> - Jamion Aden 氏
> *（コーザッド地域医療システム、情報テクノロジー部長）*

1. CISA Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector
2. United States Census Bureau QuickFacts
3. Lexington urban area shows early signs of a widespread COVID-19 outbreak
4. Alert (AA20-302A): Ransomware Activity Targeting the Healthcare and Public Health Sector
5. Ransomware victims are paying out millions a month. One particular version has cost them the most
6. RSA Presentation: Feds Fighting Ransomware: How the FBI Investigates and How You Can Help
7. Ryuk ransomware targeting organisations globally

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、1 億 9,500 万台の自動車をはじめ、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.