最新のマルウェア攻撃から医療機器を保護する方法

AI と機械学習が道を切り拓く新しいセキュリティ対策

BlackBerry®

医療技術：大きな脅威が潜む環境

過去 10 年間でサイバー犯罪の標的となることが最も多かった業界は医療機関（HDOs）であり、すべてのセキュリティ侵害のうち 24% を超える率を占めています（出典元：2017 年 1 月 Protenus Security Breach Barometer Report）。医療データベースには年間で 10 億を超えるアクセスがあり、サイバー犯罪者にとっては攻撃対象とできる領域が並外れて多い存在となっています。巨大な医療業界の一部である医療技術市場は、マルウェア、ランサムウェア、その他の攻撃ベクトルを利用したサイバー犯罪者によって深刻な攻撃にさらされています。米国には 6,000 を超える病院があり、各病院では、病床 1 つあたり 5 ～ 10 台の医療デバイスがネットワークに接続されています（輸液ポンプ、EKG、人工透析器など）。その他にも、ナースステーションの PC やモバイルタブレット、画像装置（CT スキャナー、MRI 装置など）をはじめとする、多数の IT デバイスが存在します。そのため、医療機器はサイバー犯罪者にとって大規模で魅力的な攻撃目標となっています。

さらに、医療機器には以前からの脆弱性が存在していて、マルウェアの恰好の標的となっています。

- 医療機器は既成の IT テクノロジーを利用しており、IT を悪用したマルウェアやハッキングの脅威を受けやすくなっています。
- 従来、医療機器では古いオペレーティングシステムが実行されており、セキュリティの脆弱性に関するパッチが適用されていないケースが往々にしてあります。
- 多くの医療機器はクローズな環境で動作しており、デバイスは断続的にのみネットワークに接続しています。そのため、デバイス（またはデバイスの脅威データベース）の更新が難しくなっています。

多くのエクスプロイトは医療機器のみを標的としています。たとえば、MedJack.1（実際に発見されたのは 2015 年）、MedJack.2（2016 年）、MedJack.3（2017 年）などがあります。MedJack.3 は特に厄介な、Microsoft Windows の比較的新しいバージョンに存在する脆弱性を悪用するものでした。これらの脆弱性は、血液ガス分析装置、MRI や CAT などの画像装置、X 線装置など、幅広い機器に存在することが判明しました。

Ponemon Institute の 2017 年の調査（Medical Device Security: An Industry Under Attack and Unprepared to Defend, Ponemon Institute、2017 年 5 月）によると、医療機器メーカーの 67%、および医療機関の 56% が、今後 12 ヶ月の間にいずれかの機器が攻撃にさらされると予測しています（図 1 を参照）。こうした懸念が生じるのも、医療機器メーカーの 31%、および医療機関の 40% が、デバイスに対する攻撃が実際にあったことを把握しているという事実があるからです。ですから、医療機器メーカーの 61%、および医療機関の 59% が、サイバー関連の主要な懸念事項として医療デバイスのハッキングを挙げているのです。ワイヤレスやモバイルの医療機器が使用されるようになったことで、脆弱性の存在に対する認識が高まっただけでなく、実際にそれらのデバイスの脆弱性が増えているのです。

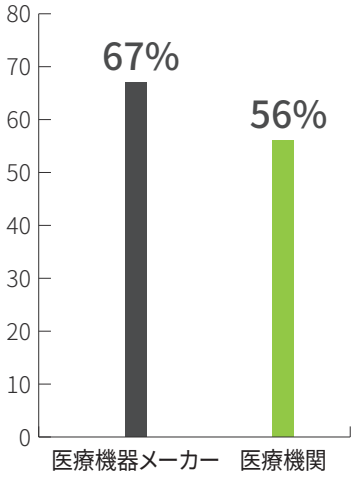


図 1：

「貴組織で製造または使用する医療デバイスが、今後 12 ヶ月の間に 1 つでも攻撃される可能性はどれくらいあると思いますか ?」という質問に対して「非常に高い」および「高い」と答えた組織の合計。

医療機器のセキュリティが侵害された場合、患者のケアや健康に計り知れない悪影響が及ぶ可能性があります。図 2（Medical Device Security: An Industry Under Attack and Unprepared to Defend, Ponemon Institute、2017 年 5 月）は、そうした影響に関する、医療機器のベンダーや医療機関による見通しを示しています。さらに考えなければいけないのは、この調査では医療機関におけるランサムウェアの影響が過小評価されている可能性があるということです。Verizon の 2018 年のデータ侵害調査レポートによると、ヘルスケア業界におけるマルウェア全体のうち 85% 以上がランサムウェアです。これらすべてのランサムウェアが医療機器を標的にしているわけではありませんが、医療機器はこうしたタイプのマルウェアの標的の 1 つであることが知られています。

医療機器のマルウェアに対する従来型アプローチの問題

医療機器には 2 つの制約があるため、マルウェアの検知と防止に従来型のアプローチを用いると悪影響が及ぶことになります。1 つ目の制約は、特にサーバーやデスクトップコンピューターなどの標準的な IT 機器と比較した場合、医療機器ではプロセッサ、メモリ、ストレージといったリソースに制約があることです。2 つ目は、これらのデバイスの多くがクローズドな環境で運用されていることです。こうした制約があることは、シグネチャベースの検知、サンドボックス、ヒューリスティクスなどの従来型のアプローチにおいて大きな影響を及ぼします。以降ではこれらの制約について詳しく見ていきます。

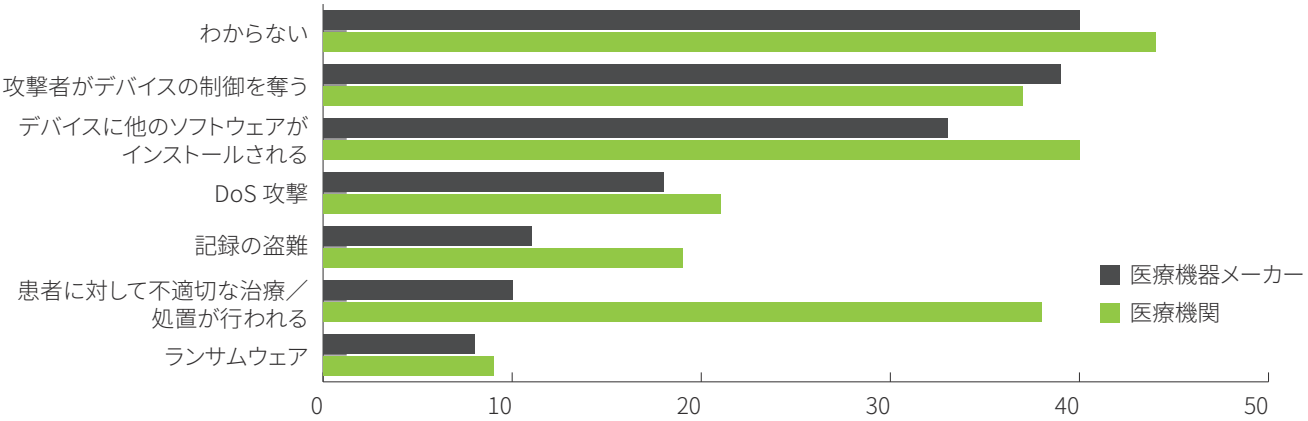
最新のコンピューティングデバイスには強力なコンピューティングリソースが搭載されています。企業向けのミドルレンジのノート PC には、通常、マルチコアプロセッサ、16GB 以上の RAM、500GB 以上のフラッシュストレージが標準的に搭載されています。しかし、ほとんどの医療機器にはこれよりもはるかに少ないコンピューティングリソースしか搭載されておらず、それらのリソースは主に、デバイスで提供される機能のみを実行するように設計されています。したがって、従来のアンチウイルスプログラムの場合、ノート PC の動作が 5 ～ 10% 低下しますが、そのようなプログラムを輸液ポンプや他の医療機器で実行すると、デバイスの性能は大きく損なわれてしまいます。従来のアンチウイルスプログラムではシグネチャ用に多くのストレージが必要になりますが、そのこともリソースに大きな影響を及ぼします。これらのリソースの需要によって生じる問題については、『Competitive System Resource Impact Testing』 のホワイトペーパーをご覧ください。

多くの医療機器がネットワーク接続の存在しないようなクローズド環境で動作する必要があることは、問題をより複雑にし、その克服を難しくしています。従来のアンチウイルスプログラムは定義ファイルと呼ばれるシグネチャデータベースに依存しており、新たな脅威に効果的に対処するためには、シグネチャデータベースを定期的に更新する必要があります。ネットワークに接続できないと、時間の経過に伴いこれらのプログラムの効果は大きく損なわれることになります。

こうした制約に加え、サンドボックスやヒューリスティクスなどのアプローチは、未知のファイルを実行して異常な動作がないか観察するという概念に依存しています。望ましくない状況が起きた場合、これらのアプローチでは、そうした状況に陥ってからそれを元に戻そうと試みるのです。医療機器の機能を考えた場合、さらに深刻なのは、このアプローチが医療機関の IT セキュリティだけでなく、患者の健康にも重大な危険を及ぼすことです。これらすべてのアプローチは、マルウェアやサイバー攻撃の手法の急激な進化に追いつくのに苦労しています。2014 年と 2015 年を比較すると、ソフトウェアの脆弱性の数は 34.6% も増えています（National Cybersecurity and Communications Integration Center、“Malware Trends”、2016 年 10 月）。

図 2：

マルウェアによって引き起こされる医療機器に対する脅威



AI と ML を使用して医療機器に対するサイバー脅威のリスクを軽減する

医療機関のインフラストラクチャにおいて医療機器が最も脆弱性の高いコンポーネントであるとしたら、臨床でのデバイスのパフォーマンスや機能に影響を及ぼすことなくセキュリティ侵害の可能性を低下させるにはどうすればいいでしょうか。マルウェアやサイバー犯罪とアンチマルウェアとの戦いで実際に効果をもたらす戦術として、人工知能（AI）と機械学習（ML）があります。Enterprise Strategy Group（ESG）の調査によると、29% の組織が AI ベースのサイバーセキュリティテクノロジーを活用してインシデント検知をより高めたいと考えており、27% の組織がこのテクノロジーを活用してインシデントへの対処をより迅速に行いたいと考えています（John Oltsik、プリンシパルアナリスト、ESG、“Artificial intelligence and cybersecurity: The real deal”、CSO、2018 年 1 月 25 日）。AI と ML によるマルウェア検知のアプローチは他のソリューションとは異なります。AI と ML に基づくアンチマルウェアソリューションでは、ファイル、ハイパーリンク、スクリプト、その他の脅威ベクトルのうち、良性のもの（クリーン）と悪性のもの（マルウェア）を何百万と分析することによって、脅威ベクトルのプロファイルを作成します。これにより、アンチマルウェアソフトウェアは、プログラムが更新されていなくても、学習サンプルに存在しない脅威（ゼロデイ脅威など）をも認識できるようになります。

CylancePROTECT®：医療機器のセキュリティ侵害を適切に防止

次世代の医療技術セキュリティソリューションが効果を発揮するためには、以下の特徴を備えている必要があります。

- 臨床における医療機器のパフォーマンスや可用性に影響を及ぼさず、干渉もしない
- クローズドネットワークでも自律的に実行可能
- 最新の OS とレガシー OS のいずれにおいても互換性があり、効果を発揮する
- 医療機器の CPU、メモリ、ネットワークのリソースでも対応できるシステム要件
- マルウェアの実行を確実に阻止できる

この目標を達成するため、サイランスは他とは違うアプローチを採用しています。サイランスのユニークなマルウェア防御機能の中核を成すのは、アルゴリズム科学と AI の力を活用した、画期的な機械学習プラットフォームです。ファイルごとに何十万もの特性をリアルタイムで解析・分類し、コア DNA レベルまで分解して、ファイルを実行しても安全であるかどうかを判断します。CylancePROTECT のアーキテクチャは小さなエージェントを利用します。このエージェントは、クラウドまたはシグネチャデータベースに依存することなく、数理モデルをホスト上で使用することによって、エンドポイント上の脅威を検知し、実行を阻止します。

CylancePROTECT は、オープンなネットワークと隔離されたネットワークのいずれであっても、脅威が実行される前にその脅威を食い止めます。継続的なシグネチャの更新やクラウドへの接続は必要ありません。さらに重要なのは、CylancePROTECT は、既知の脅威か、未知の難読化手法が使用されているかどうかにかわらず、ランサムウェアなどの脅威の実行を阻止することができます。このアプローチは、患者の健康、治療の有効性、およびデバイスの可用性に影響を及ぼしかねないデバイスのセキュリティ侵害の可能性を大幅に減らします。

サイランスの手法	従来型の製品の手法
• AI ベースの防御 • 実行前の防御 • 最小限の更新のみ必要 • すべての領域にわたる防御 • エアギャップネットワークでも動作	• サンドボックス処理 • マイクロ仮想化 • 人間による分類 • 頻繁な更新 • オンプレミスのインフラストラクチャが必要 • シグネチャ • 脅威が実行された後に動作 • ヒューリスティクス

CylancePROTECT を医療機器に導入する

以下をはじめとするさまざまな医療機器のエコシステムでは、さまざまな場所で CylancePROTECT を活用して、サイバー犯罪やマルウェア攻撃を防止することができます。

- 患者モニタリングシステム
- 輸液ポンプ
- X 線機器、コンピューター断層撮影（CAT）機器
- 磁気共鳴画像（MRI）機器
- 超音波画像機器
- 内視鏡画像システム
- 血液ガス分析装置

CylancePROTECT は 2 つの異なる方法で導入できます。あらかじめ工場で医療機器にインストールして出荷することも、或いは、すでに現場で使用されている医療機器に追加導入することも、いずれも可能です。工場でのインストールの場合、そのプロセスは簡単です。Linux のパッケージまたは Windows の実行可能ファイルとして CylancePROTECT をインストールします。ソフトウェアをインストールするときに、Linux のカーネルや Windows を変更する必要はありません。その後 CylancePROTECT はバックグラウンドで動作して、デバイス上のすべてのファイルと新たに読み込まれたファイルがマルウェアでないかどうかをチェックします。

すでに現場で使用されているシステムに Cylance PROTECT をインストールする場合には、Cylance のクラウドから直接インストールする、すべての医療機器に対してイメージを配布してインストールする、エアギャップ環境でリムーバブルメディア（USB ドライブなど）を使用して手動インストールする、という 3 つの選択肢があります。既存の製品に対する通常のオペレーティングシステムやソフトウェアの更新の一環として CylancePROTECT をインストールすることもできます。

まとめ：CylancePROTECT® は医療機器に対する真の保護を提供

医療機器の攻撃対象領域の大きさは、医療機関にとって大きなリスクです。しかし、従来型のアンチウイルスソリューションを医療機器で使用することには大きな問題があります。それらのデバイスでは定期的なアンチウイルスの更新が必要ですが、エアギャップ環境に置かれた場合はそれができないからです。また、医療機器ではコンピューティング／ストレージのリソースに制約がありますが、従来型のアンチウイルスソリューションではリソースの消費が大きく、デバイスの機能に悪影響を及ぼす可能性があります。

CylancePROTECT は、人工知能／機械学習（AI/ML）のアプローチを採用しており、従来製品のようなシグネチャデータベースの更新が不要です。したがって、クローズド環境にも導入できます。また、サイランスの AI/ML のアプローチによって、ゼロデイ脅威や未知のマルウェアなどの攻撃に対する CylancePROTECT の有効性は高まっています。CylancePROTECT は、医療機器の機能、性能に影響を及ぼすことなく、脅威の阻止を可能にします。

BlackBerryについて

BlackBerry はAI を活用することによって、予防ファーストで予測的なセキュリティ製品と特別なセキュリティサービスを提供しています。これらの製品やサービスは、エンドポイントセキュリティに対するアプローチを変革します。サイランスのセキュリティソリューションは、企業のすべての領域に対して予測的な脅威防御と可視性をもたらし、マルウェア、ランサムウェア、ファイルレスマルウェア、悪意のあるスクリプト、武器化したドキュメント、その他の攻撃ベクトルの脅威に対処します。AI（人工知能）に基づくマルウェア防御、アプリケーションとスクリプトの制御、メモリ保護に、エキスパートセキュリティサービスを組み合わせることによって、サイランスは医療機関のスタッフの作業負荷やコストを増加させることなく医療機器を保護します。

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 7,500 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/ja/jp にアクセスしてください。

BlackBerry
Intelligent Security. Everywhere.

© 2022 BlackBerry Limited. BLACKBERRY や EMBLEM Design などの商標（ただし、これらに限定されない）は、BlackBerry Limited の商標または登録商標です。また、このような商標に対する独占的権利が明確に留保されています。その他すべての商標は各社の所有物です。BlackBerry は、いかなるサードパーティの製品またはサービスに対しても責任を負いません。

MKTG20-0637 | 200921