ソリューション概要

医療機関を狙うランサムウェアを阻止する

ランサムウェアは、非対称暗号で標的の情報を暗号化し、金銭を要求するマルウェアです。非対称暗号（公開鍵/秘密鍵）は、鍵のペアを使用してファイルの暗号化と復号を行う暗号化技術です。攻撃者は標的ごとに固有の鍵ペア（公開鍵/秘密鍵）を生成し、ファイルの復号に使用する秘密鍵をサーバーに格納します。攻撃者は身代金と引き換えに秘密鍵を渡すとしていますが、最近のランサムウェアを見ると、言葉どおり秘密鍵が渡されるとは限りません。秘密鍵がなければ、ファイルの復号はほぼ不可能です。

この数年間、セキュリティ担当者にとってランサムウェアは厄介な存在となっています。サイバー犯罪者にとって、ランサムウェアは簡単に金銭を稼げる便利な攻撃ツールになっています。攻撃の標的も変化しています。これまでは個人を狙っていましたが、より多くの身代金が期待できる企業にシフトしています。最近では、病院がランサムウェアの標的になっています。『McAfee Labs脅威レポート: 2016年9月』では、2016年の前半に発生した病院を狙ったランサムウェア攻撃について詳しく分析しています。それほど洗練されていないにもかかわらず、これらの攻撃が成功しているのはなぜでしょうか。また、病院には固有の問題が存在します。古いシステムやセキュリティに問題がある医療機器が使用され、治療に関する情報に迅速にアクセスしなければなりません。

ランサムウェアを阻止するポリシーと手順

ランサムウェアからシステムを保護するには、問題点と拡散方法をよく理解する必要があります。以下に、ランサムウェアによる被害を最小限に抑えるために、病院が行うべき手順とポリシーを示します。

- 攻撃発生時の行動計画を作成しておく。重要なデータのある場所と侵入経路の存在を確認しておく必要があります。緊急管理チームと協力して、業務継続と障害時復旧の訓練を行い、目標復旧地点と時間を検証する必要があります。これらの訓練により、通常のバックアップ テストでは表面化しない、見えない影響を確認することができます。緊急時の対応計画がないため、多くの病院が身代金を払う結果になっています。

intel Security

- 最新のパッチをシステムに常に適用する。ランサムウェアが悪用する脆弱性の多くはパッチの適用で解決できます。オペレーティング システム、Java、Adobe Reader、Flash、アプリケーションにパッチを適用し、最新の状態を維持しましょう。パッチ適用の手順を決め、パッチが正常にインストールされていることを確認してください。
- 古いシステムや医療機器にパッチが適用できない場合には、アプリケーション ホワイトリストを利用してリスクを回避しましょう。これにより、システムをロックし、未承認のプログラムの実行を阻止できます。ファイアウォールや侵入防止システムを使用して、これらのシステムとデバイスをネットワークの他の部分から分離しましょう。これらのシステムで不要なサービスやポートを無効にすると、侵入の可能性があるポイントの露出を減らすことができます。
- エンドポイントを保護する。エンドポイント保護と高度な保護機能を使用しましょう。多くの場合、クライアントではデフォルトの機能しか有効になっていません。高度な機能（一時フォルダーからの実行ファイルの実行を阻止する、など）を実行すると、より多くのマルウェアを検出し、ブロックすることができます。
- 可能であれば、ローカル ディスクへの重要データの保存を禁止する。データを安全なネットワーク ドライブに保存する必要があります。感染システムの復旧が簡単になるため、ダウンタイムを短縮することができます。
- スパム対策を実施する。大半のランサムウェアは、リンクや特定の種類の添付ファイルを含むフィッシング詐欺メールで攻撃を開始します。.scrファイルまたは他の不明なファイル形式にランサムウェアが組み込まれている場合、これらの添付ファイルをブロックするスパム ルールを簡単に設定できます。.zipファイルを許可している場合には、.zipファイルを2つ以上のレベルでスキャンし、不正なコンテンツが存在するかどうか確認しましょう。
- 不要なプログラムとトラフィックをブロックする。Torの必要がなければ、ネットワーク上でTorアプリケーションとトラフィックをブロックしてください。Torをブロックすれば、ランサムウェアが指令サーバーからRSA公開鍵を取得できなくなり、ランサムウェアによる暗号化を防ぐことができます。
- 治療に必要な重要デバイスのネットワークを分離する。
- バックアップを安全な場所に隔離する。本稼働ネットワークのシステムからアクセスできない場所に、バックアップ システム、ストレージ、テープを保管してください。ランサムウェアの感染が広がると、バックアップ データにも感染する可能性があります。
- 重要な電子カルテシステムに仮想インフラを利用し、本稼働ネットワークの残りの部分から隔離する。
- ユーザーの意識向上に継続的に取り組む。大半のランサムウェアはフィッシング詐欺メールで攻撃を開始します。ユーザーのセキュリティ意識を高めることは非常に重要です。統計によると、攻撃者が送信した詐欺メールの10通に1通は攻撃に成功しています。未確認の送信元や不明な送信元から受信したメールと添付ファイルを開いてはなりません。

ランサムウェアを阻止するIntel Securityのソリューション

McAfee VirusScan EnterpriseとMcAfee Endpoint Security 10

- McAfee VirusScan Enterprise（VSE）またはMcAfee Endpoint Security（ENS）を使用して、次の操作を行います。
  - McAfee ePolicy Orchestrator（ePO）を毎日使用して、最新のDATを配備する。
  - McAfee Global Threat Intelligence（McAfee GTI）を常に有効にする。McAfee GTIは、700万を超えるランサムウェアのシグネチャを保持しています。
  - ランサムウェアのインストールとペイロードを阻止するアクセス保護ルールを作成する。詳細については、アクセス保護ルールに関するKnowledge Baseの記事（KB81095、KB54812）をご覧ください。
  - アプリケーションの動的隔離を使用して、不明なアプリケーションによる不正な活動を防ぐ。

McAfee Threat Intelligence Exchange

- McAfee Threat Intelligence Exchange（TIE）を使用して、次のポリシーを設定します。
  - 監視モードを開始する。
  - エンドポイントで不審なプロセスを検出したときに、システム タグを使用してMcAfee TIE施行ポリシーを適用する。
  - レピュテーションで駆除する（既知の不正なアイテム）
  - レピュテーションでブロックする（不正である可能性が非常に高い）。レピュテーションが不明なファイルをブロックすると、保護対策は強化されますが、初期の管理作業が増えます。
  - レピュテーション レベルが不明以下の場合、McAfee Advanced Threat Defense（ATD）にファイルを送信する。
  - TIEサーバー ポリシー: McAfee TIEで未確認のファイルにMcAfee ATDのレピュテーションを使用する。
- McAfee Threat Intelligence Exchangeの手動操作:
  - ファイル レピュテーションの施行（動作モードによる）
  - 不正な可能性が非常に高い: 駆除/削除
  - 不正な可能性がある: ブロック
  - エンタープライズ レピュテーションでMcAfee GTIのレピュテーションを上書きする。不要なプロセス（非対応または脆弱なアプリケーションなど）をブロックできます。ファイルに「不正な可能性がある」というマークを付けます。
  - 第三者のレピュテーション データをMcAfee TIEに渡し、感染の兆候を識別する。

McAfee Advanced Threat Defense

- McAfee Advanced Threat Defenseには、次のようにすぐに実行できる検出機能が搭載されています。
  - シグネチャ ベースの検出: McAfee Labsでは、1億5,000万件を超えるシグネチャ（CTB-Locker、CryptoWallの亜種も含む）を登録しています。
  - レピュテーション ベースの検出: McAfee GTI
  - リアルタイムの静的分析とエミュレーション: シグネチャ レスの検出で使用
  - カスタムYARAルール
  - 完全な静的コード分析: リバース エンジニアリングでファイルのコードを解析し、その属性と機能セットを特定します。ファイルを実行せずにソース コードを分析します。
  - 動的なサンドボックス分析

- ランサムウェアが実行される可能性が高い場所に分析用のプロファイルを作成する。
  - 一般的なOS、Windows 7、Windows 8、XPなど
  - Windowsアプリケーション（Word、Excel）をインストールして、マクロを有効にします。
- インターネットに接続しているオペレーティング システムごとに固有のプロファイル名を設定する。
  - サンプルの多くは、Microsoft Office文書に含まれるスクリプトを実行し、外部に接続してマルウェアの攻撃を実行します。インターネットに接続する分析用プロファイルを作成すると、検出率が高くなります。

McAfee Application Control

- McAfee Application Controlは、アプリケーション ホワイトリストによる保護対策を提供します。どのデバイスにも対応していますが、次のようなデバイスには特に理想的なソリューションです。
  - 医療機器などの固定デバイス
  - 更新の提供が終了している古いオペレーティング システム
  - 実行可能なサービス数に制限があるアプリケーション サーバー
  - 変更頻度の低いシステム
- 初期インストール
  - McAfee Application Controlは、インストール時にシステム全体をスキャンし、エンドポイント インベントリを作成して、ホワイトリストに追加するアプリケーションを定義します。
- 監視モード
  - 管理者は、新たにインストールまたは実行されたアプリを追跡できます。実行を承認したアプリケーションは一元管理のホワイトリストに追加できます。
  - 環境内で許可するアプリケーションの更新プログラムを設定できます。
  - プロセス、証明書、ディレクトリ、ユーザーを承認してホワイトリストを更新できます。
- 自己承認モード
  - ホワイトリストにないアプリケーションをユーザーが承認できます。これにより、業務への影響を最小限に抑えることができます。
  - 管理者は、ユーザーが承認したコンテンツを追跡し、レピュテーションや組織のポリシーに従ってアプリケーションの許可を承認または却下できます。
- ホワイトリストの施行
  - システムは不明なアプリケーションから完全に保護されます。ランサムウェアなどの不正なアプリケーションも阻止できます。
  - 新しい実行ファイルの承認手順をエンド ユーザーに通知します。

詳細情報

Intel Security Expert Center Community

- McAfee VirusScan Enterprise
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Application Control

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒150-0043 東京都渋谷区道玄坂 1- 12- 1 渋谷マークシティウェスト 20F TEL 03-5428-1100（代）FAX 03-5428-1480
西日本支店　〒530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com