ソリューション概要

ランサムウェアから大切なデータを守る

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。

ランサムウェアの詳細

ランサムウェアの技術的な詳細については『**McAfee Labs脅威レポート: 2015年5月**』で解説しています。『**McAfee Labs脅威レポート: 2014年11月**』では、2015年に発生する主な脅威を9つ予測しました。ランサムウェアについては「ランサムウェアがその拡散方法や暗号化の方法を進化させ、攻撃対象を広げる可能性があります」と予想しました。その後まもなくランサムウェアが急増し、Teslacryptなどの新しいファミリや、CTB-Locker、CryptoWall、TorrentLockerなどの新しい亜種が出現しました。

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。ランサムウェアは進化を続けています。現在では標的の言語で巧妙に作成されたランサムウェアが増えています。

この数年で新しい技術が組み込まれ、より強力なランサムウェアが出現しています。

- **仮想通貨: 身代金の支払い方法として仮想通貨**が利用されるようになりました。金銭の受け取りに銀行にいく必要がなく、送金が追跡される危険もありません。
- **Torネットワーク: Torネットワーク**を利用することで、秘密鍵のある指令サーバーの位置を簡単に隠すことができます。Torにより、犯罪インフラを長期間維持できるようになり、他の攻撃にインフラを貸し出したり、アフィリエイトプログラムの実施が可能になりました。
- **モバイルへの移行:** 2014年6月、Androidデバイスのデータを暗号化するランサムウェアが初めて出現しました[1]。PletorはスマートフォンのメモリーカードカードのデータをAESで暗号化し、Tor、SMS、HTTPで攻撃者に接続します。
- **大容量ストレージに対する攻撃:** 2014年8月、SynolockerがSynologyのネットワーク接続ストレージ（NAS）ディスクとラック ステーションに対する攻撃を開始しました[2]。このマルウェアは、パッチ未適用のNASサーバーの脆弱性を攻撃し、RSAの2,048ビット鍵または256ビット鍵を使用してサーバー上のすべてのデータをリモートから暗号化します。

intel Security

ランサムウェアに対する対策

ランサムウェアの脅威から自身と組織を守るため、いくつかのプラクティスとポリシーを紹介します。

- **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。
- **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。
- **添付ファイルを開くときには十分に注意する。**メールやインスタント メッセージの添付ファイルを自動的にスキャンするように、ウイルス対策ソフトウェアを設定しましょう。また、メール プログラムで添付ファイルを自動的に開いたり、画像を自動的に表示しないように設定し、プレビュー ウィンドウを非表示にしてください。未請求メールや予期しない添付ファイルは絶対に開かないでください。知人からのメールも例外ではありません。
- **スパムを利用したフィッシング詐欺に注意する。**メールやインスタントメッセージにあるリンクをクリックしないでください。

ランサムウェアを阻止するIntel Securityのソリューション

McAfee Web Gateway

マルバタイジング、ドライブバイ ダウンロード、信頼されたWebサイトに埋め込まれた不正なURLは、ランサムウェアを配布する手口の一例に過ぎません。**McAfee Web Gateway**は、このような脅威を阻止し、会社の保護対策を強化する強力な製品です。

- **McAfee Gateway Anti-Malware Engine:** シグネチャを使用しない意図解析により、Webトラフィックから不正なコンテンツをリアルタイムで排除します。プロアクティブなエミュレーションと動作分析でゼロデイ攻撃や標的型攻撃を阻止します。McAfee Gateway Anti-Malware Engineはファイルを検査し、不正なファイルのダウンロードをブロックします。
- **McAfee Global Threat Intelligence（McAfee GTI）との統合:** McAfee Web Gatewayは、McAfee GTIからリアルタイムで提供されるファイル レピュテーション、Webレピュテーション、Webカテゴライゼーションにより、最新の脅威を阻止します。既知の不正なサイトに対する接続だけでなく、不正な広告ネットワークを使用しているサイトへの接続も拒否します。

McAfee Advanced Threat Defense

McAfee Advanced Threat Defenseは多層型のマルウェア検出ソリューションです。複数の検査エンジンを搭載し、シグネチャ/レピュテーションによる検査、リアルタイム エミュレーション、完全な静的コード分析、サンドボックスでの動的分析などを実行します。McAfee Advanced Threat Defenseは、CTB-Locker、CryptoWallなどの有名なランサムウェアも阻止します。

- **シグネチャ ベースの検出:** ウイルス、ワーム、スパイウェア、ボット、トロイの木馬、バッファーオーバーフロー、複合型の攻撃を検出します。McAfee Labsでは、豊富な経験と知識に基づき、1億5,000万件を超えるシグネチャ（CTB-Locker、CryptoWall、亜種を含む）を登録しています。
- **レピュテーション ベースの検出:** McAfee GTIサービスからファイルのレピュテーションを取得し、新たに発生した脅威を検出します。
- **リアルタイムの静的分析とエミュレーション:** リアルタイムの静的分析とエミュレーション機能により、シグネチャやレピュテーションでは識別できないマルウェアとゼロデイ脅威を迅速に検出します。

- **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、その属性と命令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。包括的な解凍機能により、様々な圧縮ファイルを開いてコードの分析とマルウェアの分類を行い、特定のマルウェアがもたらす脅威を識別します。
- **サンドボックスでの動的分析:** 仮想のランタイム環境でコードを実行し、動作を検証します。仮想環境は会社のホスト環境に合わせて設定できます。Windows 7（32/64ビット）、Windows XP、Windows Server 2003、Windows Server 2008（64ビット）、Androidのカスタム OSイメージを使用できます。

McAfee Threat Intelligence Exchange
情報プラットフォームは環境の要件に合わせて拡張していく必要があります。**McAfee Threat Intelligence Exchange**を使用すると、環境内で実行される不明なファイルやアプリケーションなど、組織の脅威状況を正確に把握できます。これにより、攻撃のリスクを劇的に減らすことができます。不明な実行ファイルや新しい実行ファイルをブロックすることで、ランサムウェアによる被害を未然に防ぐことができます。

- **包括的な脅威情報:** グローバルなソースから総合的な脅威情報を収集できます。情報ソースの調整も簡単です。McAfee GTIだけでなく、サードパーティのソースも利用できます。ローカルの脅威情報だけでなく、エンドポイント、ゲートウェイ、その他のセキュリティ コンポーネントからリアルタイムで受信したイベント データや履歴データも使用できます。
- **実行防止と修復:** McAfee Threat Intelligence Exchangeは、環境内で不明なアプリケーションの実行を防止します。実行が許可されたアプリケーションが後で不正なプログラムと認識された場合、McAfee Threat Intelligence Exchangeは、強力な一元管理機能とポリシー施行機能により、アプリケーションに関連する実行中のプロセスを無効にします。
- **可視性:** McAfee Threat Intelligence Exchangeは、圧縮された実行ファイルを追跡し、環境内での最初の実行だけでなく、以降の変更も監視します。インストール後のアプリケーションまたはプロセスをすべて追跡するので、対応と修復を迅速に行うことができます。
- **侵害の兆候（IoC）:** 既知の不正ファイル ハッシュをMcAfee Threat Intelligence Exchangeにインポートしてポリシーを施行することで、これらの既知の不正ファイルから環境を保護できます。環境でIoCを確認すると、McAfee Threat Intelligence ExchangeがIoCに関係するすべてのプロセスとアプリケーションを終了します。

McAfee VirusScan Enterprise
McAfee VirusScan® Enterpriseを使用すると、ランサムウェアを簡単に検出し、攻撃を防ぐことができます。McAfee VirusScan Enterpriseは、実績豊富なマカフィーのスキャン エンジンを搭載し、ウイルス、ワーム、ルートキット、トロイの木馬などの高度な脅威を阻止します。

- **攻撃をプロアクティブに阻止:** マルウェア対策と侵入防止機能が統合され、アプリケーションのバッファー オーバーフローを狙うエクスプロイトを阻止します。
- **非常に強力なマルウェア検出・駆除機能:** 高度な動作分析により、ルートキットやトロイの木馬などの脅威を阻止します。ポート ブロック、ファイル名でのブロック、フォルダー/ディレクトリのロック、ファイル共有のロック、感染の追跡/ブロックにより、マルウェアの侵入を阻止します。
- **McAfee GTIの統合でリアルタイムのセキュリティを実現:** 市場で最も包括的な脅威情報プラットフォームにより、ファイル、Web、メール、ネットワークを介して侵入する既知の脅威だけでなく、新たに発生する脅威も阻止します。

McAfee Network Security Platform

McAfee Network Security Platformは、ネットワーク トラフィックを詳細に検査します。McAfee Network Security Platformは、完全なプロトコル分析、脅威レピュテーション、動作分析、高度なマルウェア分析などの高度な調査技術により、TorやIRCなどのネットワーク プロトコル経由で侵入を試みるランサムウェアを検出し、被害を未然に防ぎます。

- **包括的なマルウェア対策:** McAfee GTIのファイル レピュテーション、JavaScriptの検査を含む詳細なファイル分析、シグネチャを使用しない高度なマルウェア解析により、ゼロデイ脅威、カスタム マルウェア、ステルス攻撃を阻止します。
- **高度な調査技術を使用:** 完全なプロトコル分析、脅威レピュテーション、動作分析機能により、ネットワーク上の既知の脅威とゼロデイ攻撃を検出し、被害を未然に防ぎます。
- **McAfee GTIとの統合:** リアルタイムのファイル レピュテーション、IP レピュテーション、位置情報を組み合わせ、ユーザー、デバイス、アプリケーションに関するコンテキスト データを提供します。これにより、ネットワーク攻撃を正確に特定し、迅速に対応することができます。
- **Security Connected:** McAfee Network Security PlatformはMcAfee Advanced Threat Defenseと統合されています。監視対象のトラフィックで不審なファイルを検出すると、McAfee Advanced Threat Defenseに送信して分析を行い、その結果に基づいてトラフィックを拒否または許可します。

これらのIntel Security製品の他にも役立つにセキュリティ技術があります。

- **メール ゲートウェイ セキュリティ:** 大半のランサムウェアは、メールの添付ファイルを介してシステムに侵入します。この種の攻撃を阻止するには、強固なメール ゲートウェイ セキュリティ製品ですべての添付ファイルをスキャンする必要があります。

ランサムウェアによる攻撃が増加している現在、組織の貴重なデータを攻撃から保護することは簡単ではありません。Intel Securityのテクノロジは、ランサムウェアのような脅威からエンドポイントとネットワークの両方をプロアクティブに保護します。

1. **https://threatpost.com/android-ransomware-first-to-encrypt-data-on-mobile-devices/106535**
2. **http://forum.synology.com/enu/viewtopic.php?f=108&t=88770**

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エスト 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