ソリューション概要

ファームウェア/BIOS操作に対する対策

『**McAfee Labs脅威レポート: 2015年5月**』では、Equation Groupとその攻撃について詳しく報告しています。このグループはハードディスクとSSDのファームウェアに攻撃を仕掛けます。Equation Groupという名前は、非常に洗練された暗号化スキーマとマルウェアを使用することから付けられましたが、これまで確認した脅威の中で最も高度な攻撃を実行しています。

最も注目すべき点は、ハードディスク（HDD）とSSD（Solid State Drive）のファームウェアを改変するモジュールの存在です。ファームウェアが改変されたHDD/SSDはシステムの起動時にマルウェアを読み込むため、ドライブをフォーマットしたり、オペレーティング システムを再インストールしても、マルウェアが駆除されることはありません。ドライブが感染すると、改変されたファームウェアと関連マルウェアがセキュリティ ソフトウェアで検出されることはありません。

この数年間、Intel Securityはファームウェアや BIOSを操作するマルウェアを数多く確認しています。この中には、概念レベルのものだけでなく、**CIH/Chernobyl**、Mebromi、**BIOSkit**など、実世界で被害をもたらしたものもあります。また、『**McAfee Labs 2012年の脅威予測**』でもこのような攻撃の出現を予測しました。Equation Groupのサンプルは、これまで確認したファームウェア攻撃の中で最も高度な脅威の一つです。

Equation Groupの攻撃に対する対策:

Equation Groupに類似した攻撃を阻止するための方策と手順は次のとおりです。

- すべてのエンドポイントにエンドポイント セキュリティ ソフトウェアを配備する。
- OSの自動更新を有効にするか、OSの更新を定期的にダウンロードする。オペレーティング システムにパッチを適用して既知の脆弱性を解決する。
- ソフトウェア ベンダーが公開したパッチを速やかに適用する。
- 重要なデータとハードディスクを暗号化する。
- セキュアなゲートウェイ メール フィルタリングを使用して、大量配信のフィッシング詐欺メールを阻止する。
- 送信者の本人確認を行い、サイバー犯罪者のなりすましを防ぐ。
- 高度なマルウェア対策で不正な添付ファイルを検出し、排除する。
- 受信時とクリック時にメール内のURLをスキャンする。
- クリック操作で感染サイトに誘導される前に、Webトラフィックをスキャンしてマルウェアを確認する。
- 不審なメールを検出し、対策を講じるためのベスト プラクティスをユーザーに徹底する。
- データ損失防止を実装し、侵害発生時のデータ漏えいを防ぐ。

intel Security

Equation Groupに類似した攻撃を阻止するIntel Securityのソリューション

組織のセキュリティ対策の中で、ファームウェア/BIOS操作に対する対策を講じておく必要があります。特に必要な対策は次の2つです。

- Equation Groupが最初に配布するマルウェアの検出方法を確立する。攻撃経路としては、フィッシング詐欺、CD、USBドライブが確認されています。これらの領域は特に警戒が必要になります。
- データ漏えいからシステムを保護する。現時点でファームウェア改変モジュールを検出することはできませんが、この攻撃の目的は偵察活動です。偵察活動では、指令サーバーと定期的に通信を行ってデータを送信するため、この挙動を阻止することが非常に重要です。

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を使用すると、Equation Groupが改変したファームウェアが読み込む高度なマルウェアも阻止できます。

- **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を登録しています。
- **レピュテーション ベースの検出:** McAfee Global Threat Intelligence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、動作検証を行います。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、不明なファイルやアプリケーションなど、組織に存在する脅威を正確に把握し、攻撃のリスクを劇的に減らすことができます。

- **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、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 データと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、既知の不正ファイルから環境を保護します。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、ルールキット、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、アプリケーションに存在するバッファー オーバーフローの脆弱性に対する攻撃を阻止します。
- **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、ネットワーク経由で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を搭載しています。これにより、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。

- **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:** 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 Global Threat Intelligence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。

McAfee DLP Monitor

McAfee Data Loss Prevention（DLP） Monitorは、ネットワークで送受信されているデータを収集し、追跡、報告を行います。データに対する未知の脅威を簡単に識別してアクションを実行し、大量のデータ流出を未然に防ぎます。

- **ネットワーク トラフィックの調査:** McAfee DLP Monitorは、業界最高のデータ スキャンと解析機能により、ネットワーク トラフィックを詳しく調査します。
- **データの迅速な識別:** リアルタイム検出機能により、データの使用方法、使用者、送信先などの情報をすばやく入手し、対応に必要な情報を提供します。Network DLP Monitor は任意のポートやプロトコルで送信される300種類以上のコンテンツを検出します。
- **詳細なフォレンジックの実行:** フォレンジック分析では、現在と過去のリスク イベントを関連付け、リスクの傾向と脅威を識別します。状況を迅速に把握し、問題を解決するルールとポリシーを作成できます。

McAfee DLP Prevent

McAfee Data Loss Prevention (DLP) Preventは、不適切なデータが外部に送信されないように保護し、データ漏えいを防ぎます。電子メール、Webメール、インスタント メッセージ、Wiki、ブログ、ポータル、HTTP/HTTPS、FTP転送などに対応しています。侵害を迅速に識別して回避できれば、重要なデータを保護し、被害を未然に防ぐことができます。

- **セキュリティ インシデントの可視化:** カスタム ビューとインシデント レポートにより、セキュリティ インシデントの概要と詳細を把握できます。また、実行されたアクションも確認できます。
- **様々な情報に対してポリシーをプロアクティブに施行:** 重要性が明らかな情報にだけポリシーを施行するのでは不十分です。コンプライアンスから知的財産の適切な使用まで、様々なポリシーを使用することで、文書全体または一部をルールと比較し、重要な情報を保護できます。

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