ソリューション概要

マクロ ウイルスに対する防御

『**McAfee® Labs脅威レポート: 2015年11月**』では、マクロ ウイルスについて詳しく解説しています。1990年代に猛威を振るったマクロ ウイルスが再び息を吹き返しました。ステルス化が進んだマクロ ウイルスを散布する巧妙なソーシャル エンジニアリング攻撃が増加しています。マクロを使用すると、頻繁に実行するタスクを簡単に自動化できるため、大規模な組織でこの機能がよく利用されています。マクロは文書内に埋め込まれたコードで、プログラミング言語で記述します。Microsoft Office文書の場合、マクロを記録するとVisual Basic for Applicationsのプログラムが生成されます。Microsoftは、マクロ ウイルスを阻止する対策を講じ、マクロを有効にするときに許可を求めるように設定を変更しました。現在のMicrosoft Officeでは、デフォルトですべてのマクロが無効になり、ユーザーの許可なくマクロが実行されないようになっています。これにより、マクロ ウイルスは下火になり、不正なマクロによる脅威も減少しました。しかし、昨年、ステルス化が進んだ新種のマクロ ウイルスを拡散させるソーシャル エンジニアリング攻撃が特定の組織に対して繰り返し実行されました。新しいマクロ ウイルスのサンプル数はこの6年間で最大になっています。

マクロ ウイルスの作成者は、フィッシング詐欺メールの添付ファイル、スパム、感染サイト、ドライブバイ ダウンロードなどの方法でマルウェアを散布しています。これらの手口は、マクロ ウイルスが最初に現れた1990年代よりもはるかに進化しています。攻撃の標的が限定され、スパムの配信期間も短くなっています。また、検出を回避するため、非常に巧妙な添付ファイルが使用されているため、攻撃の検知は非常に難しくなっています。

次のような方策と手順を実施して、マクロ ウイルスを阻止しましょう。

- オペレーティング システムの自動更新を有効にするか、更新を定期的にダウンロードし、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。
- Microsoft Officeの更新を適用する。このような攻撃に対する保護機能が強化されます。
- すべてのMicrosoft Office製品で、マクロ セキュリティの既定値を「高」に設定する。
- すべてのメールとインスタント 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、マルウェア対策を設定する。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ましょう。

intel Security

- ブラウザーのセキュリティ設定を「中」以上に設定する。
- 添付ファイルを開くときは十分に注意する。特に、.docや.xlsファイルを開く場合には警戒が必要です。
- 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。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。
- 1.3.1.2、2.2.1.1など、予期しないIPアドレスに対する内部コンピューターからのpingを監視する。
- マクロを含む領収書や請求書に注意する。このような文書でマクロが必要になることはありません。
- コンテンツを表示するためにマクロを有効にするように指示する空の文書に注意する。

マクロ ウイルスから保護するIntel Securityのソリューション

McAfee Web Gateway
マクロ ウイルスは、マルバタイジング、ドライブバイ ダウンロード、フィッシング詐欺メールに埋め込まれた不正なURLによって配布されます。**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により、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 VirusScan® Enterprise
McAfee VirusScan Enterpriseを使用すると、マクロ ウイルスを検出し、簡単に駆除することができます。McAfee VirusScan Enterpriseは実績豊富なMcAfee Labs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。また、ポートとファイル名によるブロック、フォルダー/ディレクトリ/ファイル共有のロック、感染の追跡/ブロック機能により組織を保護します。

- **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、Microsoft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。ポートとファイル名でのブロック、フォルダー/ディレクトリ/ファイル共有のロック、感染の追跡/ブロックなどの技術により、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脅威を検出します。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 Advanced Threat Defense
McAfee Advanced Threat Defenseは、複数の検出エンジンを統合した多層型のマルウェア検出製品です。McAfee Advanced Threat Defenseは、シグネチャ ベースの複数の検査エンジン、レピュテーション ベースの検査、リアルタイムのエミュレーション、コードの完全な静的分析、動的サンドボックスを搭載し、マクロを含む文書を検出してマルウェアの散布を防ぐだけでなく、マクロ実行後のマルウェアのダウンロードも検出し、攻撃を阻止します。

- **シグネチャ ベースの検出**: McAfee Labsの豊富な経験と知識に基づき、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。
- **レピュテーション ベースの検出**: McAfee GTI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、シグネチャベースの技術やレピュテーションでは識別できないマクロ ウイルスや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把握することができます。
- **動的なサンドボックス分析**: 前述の検出エンジンで安全性が確認できないファイルは、McAfee Advanced Threat Defenseが仮想環境でファイルのコードを実行し、動作を確認します。この仮想環境は、ホスト環境に合わせて構成できます。McAfee Advanced Threat Defenseは、Windows XP SP2/SP3、Windows 7（32ビット/64ビット）、Windows 8（32ビット/64ビット）、Windows Server 2003、Windows Server 2008（64ビット）、Androidのカスタム イメージに対応しています。

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、マクロ ウイルスによる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。これらの情報ソースは簡単に調整できます。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。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ローカルのイベント 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、以降の動作も監視します。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**: 既知の不正なファイル ハッシュをにインポートしてポリシーを施行することで、これらの脅威から環境を保護します。環境で侵害の兆候を確認すると、McAfee Threat Intelligence Exchangeが関連するプロセスとアプリケーションをすべて終了します。

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**: 大半のマクロ ウイルスは、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。
- **ファイアウォール**: ファイアウォール技術は、システムの保護に不可欠なセキュリティです。ファイアウォールは境界で多くの脅威を検出し、信頼されたネットワークへの侵入を阻止します。

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