ソリューション概要

ファイルレス マルウェアに対する防御

『**McAfee® Labs脅威レポート: 2015年11月**』では、ファイルレス マルウェアについて（特に、Kovter）詳しく分析しています。ファイルレス マルウェアは、ディスク上にバイナリを残さず、感染先のホストのレジストリに自身のコードを隠蔽します。マルウェアの作成者は、ポリモーフィズム、ウォッチドッグの埋め込み、権限の取り消しなどで検出の回避を試みてきました。2015年は、Microsoft Windows Management Instrumentation（WMI）やWindows PowerShellなどの機能を利用し、ディスク上にバイナリの残さず、エンドポイントに侵入を試みる攻撃が発生しました。このようなマルウェアの追跡は容易なことではありません。

メモリー常駐型のファイルレス マルウェアは以前から存在しています。ファイルレスといいながらも、以前のマルウェア ファミリはメイン メモリーに侵入する前にディスク上にわずかな痕跡を残しています。しかし、Kovter、Powelike、XswKitなどの新しいファイルレス マルウェアはディスク上に痕跡を残しません。ディスク上にあるファイルを分析する検出方法では、このような脅威の検出は困難です。

ファイルレス マルウェアは次の3種類に分類できます。

- **メモリー常駐型**: このタイプのファイルレス マルウェアは、正規のWindowsファイルのメモリー空間を利用します。自身のコードをメモリー空間に読み込み、コードがアクセスまたはアクティブ化されるまでメモリーに常駐します。コードの実行は正規のファイルのメモリー空間で行われますが、実行を開始または再開するためのファイルが休眠状態で存在します。厳密な意味では、この種類のマルウェアはファイルレスとはいえません。
- **ルートキット**: この種類のファイルレス マルウェアは、ユーザー レベルまたはカーネル レベルのアプリケーション プログラミング インターフェース（API）に自身の存在を隠蔽します。マルウェアのファイルはディスク上にステルス モードで存在します。
- **Windowsレジストリ**: この種類のファイルレス マルウェアは、Windows OSのレジストリに侵入します。マルウェアの作成者は、Windowsエクスプローラーのサムネイル ビューで使用する画像の格納場所（Windowsサムネイル キャッシュ）などを悪用します。サムネイル キャッシュは、マルウェアを持続させる手段として使用されます。他のマルウェアと同様に、この種のファイルレス マルウェアがシステムに侵入するには静的なバイナリ ファイルが必要です。大半のファイルレス マルウェアは、システムへの侵入手段としてメールを使用しています。ユーザーが添付ファイルをクリックすると、マルウェアは暗号化された完全なペイロードをWindowsレジストリ ハイブに書き込みます。書き込みの完了後、自身を削除してシステムから痕跡を消します。

intel Security

Kovter、Powelike、XswKitなどのファイルレス マルウェア ファミリは非常に巧妙で、ファイル システムに痕跡を残しません。ファイルをまったく使用せずにWindowsレジストリに侵入します。攻撃の実行環境はファイル内のコードを実行して準備する必要がありますが、攻撃が可能な状態になると、準備に使用したファイルを消去します。

ファイルレス マルウェアから保護するIntel Securityのソリューション

痕跡を残さないファイレス マルウェアを完全に検出するために様々な対策が行われていますが、簡単に検出できるものではありません。このようなマルウェアを阻止するには、適切なセキュリティ対策で攻撃の侵入口を防ぐ必要があります。

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、わずかな痕跡しか残さないファイルレス マルウェアを阻止します。

- **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 Global Threat Intelligence（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ルウェア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実行できるので、特定のマルウェアがもたらす脅威を正確に把握できます。
- **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、ファイルレス マルウェア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できます。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。

McAfee Web Gateway
ファイルレス マルウェアは、ドライブバイ ダウンロードや、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 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。

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**: 大半のファイルレス マルウェアは、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。
- **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できます。ファイルレス マルウェアは静的なバイナリ ファイルを介してシステムに侵入するので、これらの攻撃の多くはネットワークに侵入する前に阻止できます。

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