ソリューション概要

スクリプトベースのマルウェアを阻止する

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。

この10年の間に、Microsoft Windows Management Instrumentation (WMI) やWindows PowerShellなどの機能を悪用し、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は、感染先のホストのレジストリに不正なコードを直接埋め込むため、追跡は容易ではありません。

スクリプトを悪用した感染が確認されてから数年が経ちます。ファイルレスといいながらも、以前のマルウェア ファミリは攻撃の初期段階でメイン 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した。

しかし、スクリプトを悪用し、最新の回避技術を駆使するマルウェアはディスクに全く痕跡を残しません。静的ファイルを分析する方法では、このような脅威の検出は難しくなっています。スクリプトを悪用するマルウェアの詳細については、『McAfee脅威レポート: 2017年9月』をご覧ください。

スクリプトベースのマルウェアは次の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。
- **ルートキット:** このタイプのマルウェアは、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:** 高度なスクリプト マルウェアの一部はWindowsレジストリに潜伏します。これまでマルウェアの作成者は、攻撃の持続手段としてエクスプローラーのサムネイル ビューで使用される画像の格納場所（Windowsサムネイル キャッシュ）などを利用します。このタイプのマルウェアでも、システムへの侵入に静的なバイナリ ファイルが必要になります。大半のマルウェアはシステムへの侵入経路としてメールを利用します。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。

スクリプトを悪用する現在のマルウェアは非常に巧妙で、ファイル システムに痕跡を残さず、静的ファイルを全く使用せずにWindowsレジストリを攻撃します。ファイル内のコードを実行して実行環境を準備しますが、攻撃が可能な状態になると、準備に使用したファイルは削除されます。

スクリプト ベースのマルウェアを阻止するためのポリシーと手順

McAfeeが推奨する最新のベストプラクティスは、ネットワークとエンドポイントで次のような脅威回避策を実施することです。

- スクリプト マルウェアの感染からシステムを保護する最も良い方法は、感染を未然に防ぐことです。コンピューターのマルウェア感染を防ぐために最も重要なポイントはユーザーです。出所の分からない怪しいアプリケーションをダウンロードしたり、インストールするリスクを十分に理解させなければなりません。感染で最も多いのは、警戒心の低いユーザーが閲覧中に誤ってマルウェアをダウンロードしてしまうケースです。
- アプリケーションとオペレーティング システムにセキュリティ更新とパッチを適用しましょう。
- Webブラウザーとアドオンを常に最新の状態にしておきましょう。エンドポイントとネットワーク ゲートウェイのマルウェア対策も最新バージョンにアップグレードまたは更新する必要があります。
- 会社のITセキュリティ部門が認定または提供しているコンピューターのみを使用しましょう。保護されていない資産を会社のネットワークに接続すると、スクリプト マルウェアの拡散を引き起こす可能性があります。
- ユーザーにローカル管理者権限を付与し、ユーザー自身がアプリケーションをインストールできるようにしている場合には、有名なベンダーから提供され、信頼された署名が付いたアプリケーションのみをインストールするように徹底する必要があります。無害に見えるアプリケーションにルートキットやスクリプト マルウェアが埋め込まれていることも少なくありません。

- Web以外の場所からアプリケーションをダウンロードしないようにしましょう。Usenetグループ、IRCチャネル、インスタント メッセージ クライアント、ピア ネットワークは、マルウェア感染の可能性が高い経路です。また、IRCやインスタントメッセージに貼り付けられたWebサイトのリンクも、感染したダウンロードに誘導される危険性があります。
- フィッシング詐欺対策の研修を実施しましょう。マルウェアの多くは標的型攻撃のメールで拡散しています。
- 脅威情報フィードとマルウェア対策を活用しましょう。この2つを組み合わせることで、既知のマルウェアだけでなく、新しい脅威も短時間で検出することができます。

スクリプトベースのマルウェアの阻止に役立つMcAfee製品

痕跡を残さないスクリプト マルウェアを検出するために、様々な対策が行われています。しかし、このような脅威は簡単に検出できるものではありません。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塞ぐ必要があります。

McAfee Endpoint Security

McAfee Endpoint Security (ENS) は、エンドポイント セキュリティ環境の複雑さを解消する統合セキュリティ フレームワークを提供します。スクリプト ベースのマルウェアなど、高度な脅威を可視化し、検出から修復までの時間を短縮します。この拡張性に優れたアーキテクチャを利用することで、複数のソリューションを一元的に管理できます。脅威対策の状況を迅速に把握し、管理作業をより簡単に行うことができます。

McAfee ENSには新しい技術が追加され、機能が強化されています。

- **Real Protect:** 機械学習を利用して不正なコードを識別します。シグネチャを使用せずに、状態 (実行前の解析) と挙動 (動的な動作分析) を確認できます。スクリプト マルウェアを効率的に阻止するには、Real Protectは欠かせない機能です。
- **アプリケーションの動的隔離:** プロセスのインスタンスを隔離します。
- **McAfee Client Proxyの統合:** McAfee Endpoint Securityを多層型のWebゲートウェイ セキュリティと統合することで、包括的な保護対策を実現できます。エンドポイントとWeb Gatewayクラウド サービスを接続することで、オフネットワークのギャップを解消できます。
- **ファイアウォール モジュール:** サイバー犯罪者が制御するサーバーとの通信をブロックします。この保護層を追加することで、プロアクティブなセキュリティ対策を実施できます。
- **脅威対策モジュール:** オンデマンド スキャンで、スクリプト マルウェアの阻止に役立つレジストリ スキャン オプションを使用できます。管理者が作成できるカスタム サービスのアクセス保護ルールに、Windows サービスが追加されました。McAfee提供の侵入防止システム (IPS) のシグネチャと一緒に、カスタム アプリケーションのエクスプロイト防止機能を利用できます。また、エクスプロイト対策ルールでWindowsアプリケーションの保護を使用できます。

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) 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 ATD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スクリプト マルウェアを阻止します。

- **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は、総合的なナレッジベースを作成し、維持しています。
- **レピュテーション ベースの検出:** McAfee Global Threat Intelligence (GTI) を使用してファイルのレピュテーションを検索し、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 ATD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 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 (TIE) 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、スクリプト 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。

- **総合的な脅威情報:** 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。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 TIE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 TIE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。
- **可視化:** McAfee TIE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 TIE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

スクリプト 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（MWG）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。

- **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。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:** MW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McAfee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:** 大半のスクリプト 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。このような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。スクリプト 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。

〒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
www.mcafee.com/jp

3529_0917
2017年9月