バックドア型トロイの木馬を阻止する

Adwind リモート管理ツール（RAT）は Java ベースのバックドア型トロイの木馬で、Java ファイルをサポートしている様々なプラットフォームを標的とします。Adwind は脆弱性を悪用しません。通常、メールに添付された .jar ファイルをダブルクリックしたり、感染した Microsoft Word 文書を開いてマルウェアを実行しない限り、感染することはありません。感染するのは、Java Runtime Environment がインストールされている場合だけです。攻撃先のシステムで不正な .jar ファイルが実行されると、マルウェアはユーザーに気づかれずに自身をインストールし、事前に設定されたポートを介してリモート サーバーに接続します。接続後、リモートの攻撃者から命令を受信し、さらなる攻撃を実行します。

略歴

Adwind は Frutas RAT から進化しました。Frutas は 2013 年の初めに見つかった Java ベースの RAT で、ヨーロッパやアジアの大手通信会社、金融機関、政府機関などを狙ったフィッシング詐欺メールでよく利用されました。

McAfee® Labs では、2015 年第 1 四半期から Adwind として識別される .jar ファイルのサンプル数が急増しています。

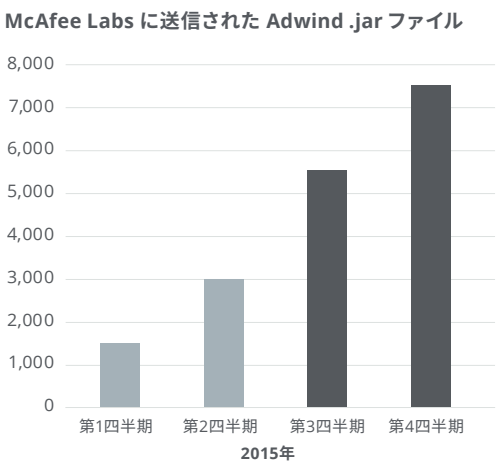

図 1. The2015 年第 1 四半期に McAfee Labs が受信した Adwind .jar ファイルは 1,388 件でしたが、同年の第 4 四半期は 7,295 件で、426% も増加しています。

感染の連鎖

通常、Adwind はスパム メールの添付ファイル、Web ページ、ドライブバイ ダウンロードによって拡散します。配布方法も変化しています。以前のスパム キャンペーンでは、件名や添付ファイルの名前が同じスパム メールを数日から数週間送信していました。このため、セキュリティ ベンダーも Adwind を迅速に検出し、脅威を回避できました。現在ではスパムの配信は短期間で終了し、メールの件名も頻繁に変更されています。Adwind の検出を回避するため、非常に巧妙な添付ファイが作成されています。

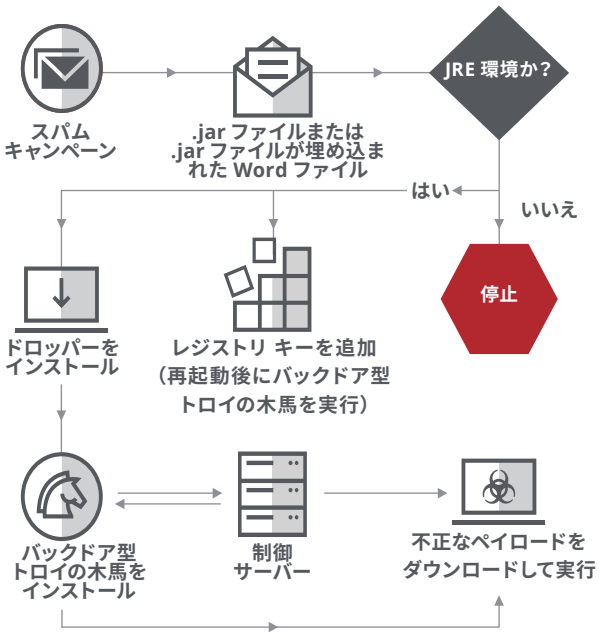

図 2. Adwind の感染の連鎖

システムへの侵入に成功すると、Adwind はキーストロークの記録、ファイルの改ざんと削除、別のマルウェアのダウンロードと実行、スクリーンショットの取得、システム カメラへのアクセス、マウスとキーボードの操作、自身の更新などを実行します。

McAfee が Adwind などのバックドア型トロイの木馬を阻止する方法

McAfee の技術を使用すると、Adwind などのバックドア型トロイの木馬を阻止することができます。以下では、この種の攻撃の組織に役立つ製品を紹介します。

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、バックドア型トロイの木馬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 Global Threat Intelligence（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。

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。これらのエンジンは、不審なオブジェクトに対してシグネチャ ベースの検査、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分析を実行し、攻撃対象のシステムにバイナリをドロップする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 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バックドア型トロイの木馬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、Microsoft Windows XP (32 ビット /64 ビット)、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 Network Security Platform

McAfee Network Security Platform は、ネットワークで巧妙な脅威を検出して阻止するインテリジェントなセキュリティ製品です。単なるパターンの比較を超えた高度な検出機能とエミュレーション技術により、ステルス型攻撃を非常に高い精度で検出し、被害を未然に防ぎます。弊社のオープンな統合アプローチによりセキュリティ管理を簡単になります。McAfee GTI からリアルタイムで脅威情報が提供されるので、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 データを使用してネットワークに対する攻撃を迅速に検出し、的確な対応を行うことができます。

- **シグネチャレスの防御 :** ステルス型のマルウェア、高度な持続型脅威 (APT)、ボット、ゼロデイ攻撃などの巧妙な脅威は、シグネチャベースの保護対策を回避します。McAfee Network Security Platform は、シグネチャを必要としない高度なエンジンを複数搭載し、未知の脅威や高度な脅威を阻止します。シグネチャレスの検出では、エミュレーションにより、Web コンテンツ、PDF ファイル、Flash ファイル、JavaScript の動作をほぼリアルタイムで解析します。
- **エンドポイントのインテリジェント エージェント :** McAfee Network Security Platform は、エンドポイントのトラフィック フローの相関分析をリアルタイムで行います。エージェントは、複数のソースから取得したレピュテーション情報を使用して、ネットワーク トラフィック フローの動作分析を行います。ネットワークと Windows ホストの情報を利用し、エンドポイントの実行ファイルとネットワーク トラフィック フローの関係を特定します。これにより、不正なネットワーク接続と実行ファイルをリアルタイムに識別できます。エージェントは、詳細なコンテキスト情報を使用して不正な通信をブロックし、高度なマルウェアの拡散を防ぎます。さらに、感染したホストを隔離し、問題を修復します。

McAfee Web Gateway

バックドア型トロイの木馬は、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。

- **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や、指令サーバーであることが確認され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 :** 大半のバックドア型トロイの木馬は、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。

〒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