ソリューション概要

ステガノグラフィーの脅威から保護する

ステガノグラフィーは情報を隠すための技術で、デジタル世界でも利用されています。メッセージは、画像、オーディオ トラック、ビデオ クリップ、テキスト ファイルなどに隠すことができます。この技術は、正規の目的で利用されている場合もありますが、大半はマルウェアによって利用されています。

検出を回避するため、一部のマルウェアはステガノグラフィーを利用して、一見無害に見えるカバー ファイルに不正なコンテンツを隠します。ほとんどのマルウェア対策は構成ファイル内の不正なコンテンツを検出しますが、ステガノグラフィーでは、構成ファイルがカバー ファイルに埋め込まれています。ステガノグラフィーで作成されたファイルはメイン メモリーに展開される場合があり、検出はさらに困難になります。ステガノグラフィーで作成されたファイルに潜む構成ファイル、バイナリ アップデート、ボット コマンドを検出するのは容易ではありません。攻撃側はステガノグラフィーを簡単に使用できますが、残念ながら検出は難しいのが現状です。

ステガノグラフィーの脅威を阻止するポリシーと手順

McAfeeでは、ステガノグラフィーの脅威から保護するために、次のことを推奨します。

- **内部脅威に対する保護に使用されるソフトウェア配信メカニズムを厳格化する。**信頼できるアプリケーションのリポジトリを一元管理し、承認されたソフトウェアをダウンロードできるようにします。提供元が不明のソフトウェアをユーザーがダウンロードできないようにします。
- **画像をよく分析する。**画像編集ソフトウェアを利用して、画像内の微妙な色の違いなど、ステガノグラフィーのマーカーを探しましょう。画像内に重複する色が大量にある場合、ステガノグラフィーが利用されている可能性があります。
- **ステガノグラフィー ソフトウェアの使用を制限する。**ビジネス目的で特に必要でない限り、ステガノグラフィー ソフトウェアの使用を禁止するべきです。このタイプのソフトウェアは、他から遮断されたネットワーク セグメントでのみ許可しましょう。
- **信頼されたベンダーの署名だけを許可する。**信頼されたベンダーの署名付きアプリケーション以外はインストールしてはなりません。

McAfee™
Together is power.

- **バインダーを検出するようにマルウェア対策を設定する。**ステガノグラフィーの画像はバインダーに含まれている可能性があります。このバインダーの存在を識別できるように、マルウェア対策ソフトウェアを設定しましょう。
- **ネットワークをセグメント化する。**信頼性の高い仮想化アーキテクチャを利用し、ネットワークを適切にセグメント化することで、ステガノグラフィーを利用した脅威の拡散を防ぐことができます。保護された環境で検証可能なブートプロセスを実行し、トラフィックを継続的に監視することで、アプリケーションを隔離できます。
- **送信トラフィックを監視する。**送信トラフィックを監視して、ステガノグラフィー攻撃の存在を確認しましょう。

マルウェアに含まれるステガノグラフィー コードを阻止するMcAfee製品

McAfee Endpoint Security

脅威対策

ステガノグラフィー コードを含む既知のマルウェアを阻止できるように、McAfee Endpoint Security（ENS）を設定しましょう。

- 最新のパッチ、DAT、スキャン エンジンが使用されるように、McAfee ENSを常に最新の状態に保ちましょう。
- 環境内のすべてのシステムを保護し、最新の状態にしましょう。
- 種類に関係なく、ファイルの読み取り時と書き込み時にスキャンを実行するように、リアルタイム スキャン（オンアクセス スキャン）を設定しましょう。危険度低のプロセスを設定する場合を除き、読み取り時のスキャンを無効にしてはなりません。
- スキャンの除外ルールは最小限にし、必要な場合にのみ使用しましょう。マルウェアの可能性がある場合には、スキャンの除外機能を一時的に無効にしましょう。除外項目の設定方法については、Knowledge Baseの記事KB88595をご覧ください。
- 危険度高/デフォルト/危険度低の設定がパフォーマンスに及ぼす影響を理解しましょう。特に、使用頻度の高い環境や、最低限のハードウェア セキュリティしか実装されていない環境の場合は注意が必要です。McAfee Endpoint Securityでパフォーマンスを改善する方法については、KB88205をご覧ください。
- McAfee Global Threat Intelligence（GTI）ファイル レピュテーション機能を使用するように、McAfee ENSを設定しましょう。この技術により、ゼロデイの脅威とシグネチャによる検出のギャップを埋めることができます。McAfee GTIファイル レピュテーションがKB74983に記載されています。また、詳細については、KB53735をご覧ください。
- autorun.infファイルの作成を禁止するMcAfee ENSアクセス保護ルールを作成しましょう。
- アクセス保護ルールを使用して、未知の脅威の侵入を防ぎましょう。

Web管理

McAfee ENS Web管理は、McAfee GTIのWebレピュテーションとWeb カテゴライゼーション サービスをベースにしています。多くの場合、ステガノグラフィーに感染したソフトウェアはマルウェア配信サイトにも存在します。

McAfee ENS Web管理は、ユーザーがサイトを閲覧する前に、マルウェアの存在や感染、不適切なコンテンツの有無を確認します。

McAfee Web管理:

- Webサイトの相対的な安全性を色別で表します。
  - 緑 = 安全（リスクがないか、ほとんどない）
  - 黄 = 注意（マイナー リスク）
  - 赤ー = 警告（重大なリスク）
  - グレー = 不明（未評価のため、注意が必要）
  - McAfee Secure = 毎日、安全性の診断を行っています。
- 配備と設定は、McAfee ePolicy Orchestrator で簡単に行うことができます。
- エンドポイント保護に新しい保護層を追加します。Internet Explorer、Firefox、Chromeから実行できます。
- 効果的なスパム対策を利用し、ネットワークへの不正なメールの侵入を阻止します。

詳細情報: McAfee Endpoint Security製品ガイド ー ENS Web管理の使用

適応脅威対策

- McAfee Real Protectを有効にすると、機械学習を利用して高度な脅威を識別できます。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。
  詳細情報: 適応脅威対策—Real Protect
- McAfee Dynamic Application Containmentを実装すると、推奨のベストプラクティスを実行できます。詳細情報: KB87843

McAfee VirusScan Enterprise

最新のMcAfee ENSを配備していない場合には、ステガノグラフィー コードを含む既知のマルウェアを阻止できるように、McAfee VirusScan Enterprise（VSE）を設定しましょう。

- 最新のパッチ、DAT、スキャン エンジンが使用されるように、McAfee VSEを常に最新の状態に保ちましょう。
- 環境内のすべてのシステムを保護し、最新の状態にしましょう。
- 種類に関係なく、ファイルの読み取り時と書き込み時にスキャンを実行するように、リアルタイム スキャン（オンアクセス スキャン）を設定しましょう。危険度低のプロセスを設定する場合を除き、読み取り時のスキャンを無効にしてはなりません。
- スキャンの除外ルールは最小限にし、必要な場合にのみ使用しましょう。マルウェアの可能性がある場合には、スキャンの除外機能を一時的に無効にしましょう。除外項目の設定方法については、Knowledge Baseの記事KB50998をご覧ください。
- 使用頻度の高い環境や、最低限のハードウェア セキュリティしか実装されていない環境の場合には、危険度高/デフォルト/危険度低プロセスの設定を使用し、ステガノグラフィーの脅威に対する露出を制限しましょう。この機能の詳細は、KB55139に記載されています。また、設定方法については、KB58692をご覧ください。
- McAfee Global Threat Intelligence（GTI）ファイル レピュテーション機能を使用するように、McAfee VSEを設定しましょう。この技術により、ゼロデイの脅威とシグネチャによる検出のギャップを埋めることができます。McAfee GTIファイル レピュテーションの推奨設定がKB74983に記載されています。詳細については、KB53735をご覧ください。
- autorun.infファイルの作成を禁止するMcAfee VSEアクセス保護ルールを作成しましょう。
- アクセス保護ルールを使用して、未知の脅威の侵入を防ぎましょう。

McAfee Application Control
McAfee Application Controlは、サーバー、会社のデスクトップ、専用デバイスで未承認のアプリケーションとコードを効率的にブロックします。McAfee Application Controlは、ファイルの感染を未然に防ぎ、ネットワークを介した感染の拡大を防ぎます。

McAfee Application Controlは次の2つの領域を保護します。

- **ファイルの保護:** ステガノグラフィーを利用した脅威の多くは、ファイルに対して攻撃を仕掛けてきます。たとえば、新しいアプリケーションを実行したり、現在のアプリケーションを変更しようとします。
- **メモリーの保護:** メモリーに対する攻撃を阻止します。この攻撃は、インターネットやネットワーク経由だけでなく、ローカル ファイルの実行によって開始する場合もあります。

ファイルの保護
ホワイトリストにないアプリケーションは未承認で、保護もされません。逆に、ホワイトリストに登録されたアプリケーションは承認済みで、保護されます。ダウンロード、ネットワーク アクセス、ローカルのフラッシュドライブやCDなどから未承認のアプリケーションを取得した場合、エンドポイントにコピーしたり、フォルダー間で移動することはできますが、実行はブロックされます。このタイプには、次のようなイベントがあります。

実行の拒否	ホワイトリストに登録されていないアプリケーションの実行を試みると、McAfee Application Controlが実行をブロックします。
ActiveXのインストール禁止	未承認のActiveXコントロールをインストールしようとすると、McAfee Application Controlがインストールを阻止します。

未承認のプロセス（リモート エンドポイントでの不正なファイルの実行など）や未承認のユーザーが保護されたファイルの変更、移動、削除、名前の変更を試みると、McAfee Application Controlがこのような処理をブロックします。このタイプには、次のようなイベントがあります。

ファイルの書き込み拒否	ホワイトリストに登録されたアプリケーションに未承認のプロセスが変更を試みると、McAfee Application Controlが変更を阻止します。
パッケージ変更の拒否	MSI形式のインストーラー パッケージを使用するアプリケーションが未承認の方法でインストール、変更、削除を実行しようとすると、McAfee Application Controlがこのような処理を阻止します。

詳細情報: McAfee Application Controlベストプラクティス

McAfee Advanced Threat Defense
McAfee Advanced Threat Defense（ATD）は、革新的な多層型のアプローチで、ステルス型の巧妙なパッカー、暗号化されたペイロード、ゼロデイ マルウェアを検出します。マルウェア対策のシグネチャ、レピュテーション、リアルタイム エミュレーションと詳細な静的コード分析、動的なマルウェア分析（サンドボックス）を組み合わせ、マルウェアの実際の挙動を分析します。

詳細情報: McAfee Advanced Threat DefenseのFAQ

詳細情報

McAfee Security Advice Center: フィッシング詐欺対策

脅威状況ダッシュボード: 2016年後半にSundownエクスプロイト キットの新しいバージョンが確認されました。このバージョンは、ステガノグラフィーでエクスプロイト キットの存在を隠蔽しています。

マカフィー株式会社
〒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）
www.mcafee.com/jp