ソリューション概要

回避型マルウェアを阻止する

『McAfee Labs脅威レポート: 2017年 6月』で詳しく解説されているように、検出を回避するマルウェアが存在します。これらのマルウェアは、正規のアプリケーションを悪用して自身の存在を隠蔽します。サンドボックスでの解析が始まると、その動きを察知し、実行を遅らせます。攻撃を開始するまでに数日から数週間、中には数か月間も潜伏しているものもあります。

回避型マルウェアを阻止するセキュリティ プログラムの構築は、次の3つのコンポーネントに基づいて行う必要があります。

- **人**: セキュリティ担当者は、セキュリティ インシデントへの適切な対応と、現在のセキュリティ技術の適切な管理方法について研修を受ける必要があります。攻撃者は、ソーシャル エンジニアリングでユーザーを騙し、システムに侵入しようとします。社内の意識向上や研修を行わないと、攻撃者に対して隙だらけになります。
- **プロセス**: セキュリティ担当者が適切に対処できるように、明確な体制と社内プロセスを整えておく必要があります。強力で効果的なセキュリティを行うには、セキュリティのベストプラクティス（更新、バックアップ、ガバナンス、インテリジェンス、インシデント対応計画など）を実施する必要があります。
- **技術**: 技術はチームとプロセスをサポートします。新しい脅威に適応できるように強化する必要があります。

有効な回避型マルウェア対策ポリシーと手順

- マルウェア感染防止策で最も重要な役割を担うのはユーザーです。信頼性の低い提供元からアプリケーションをダウンロードしたり、インストールする危険性をよく理解する必要があります。また、閲覧中に誤ってマルウェアをダウンロードしてしまう可能性もあります。
- 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。
- 信頼されたネットワーク システムで、企業のITセキュリティ グループが配布および承認していないシステムを使用してはなりません。保護されていないシステムが信頼されたネットワークに接続されると、回避型マルウェアは容易に拡散します。

McAfee
Together is power.

- 攻撃者がトロイの木馬に変えた正規のソフトウェアに回避型マルウェアが潜んでいる場合もあります。このような攻撃を阻止するため、ソフトウェアの配布方法を厳重に管理する必要があります。どの環境でも、企業のアプリケーションをリポジトリで一元管理し、そこから承認済みのソフトウェアをダウンロードするようにすると効果的です。
- ITセキュリティ グループで検証されていないアプリケーションのインストールをユーザーに許可する場合には、既知のベンダーが署名した信頼できるアプリケーションだけをインストールするように指示しましょう。オンライン上で無害に見えるアプリケーションに回避型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、ピアツーピア システムは、マルウェアをダウンロードする可能性の高い経路です。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。フィッシング詐欺でマルウェアに感染することも少なくありません。
- 脅威情報フィードとマルウェア対策を活用しましょう。これらを併用することで、脅威をより迅速に検出することができます。

回避型マルウェアを阻止するMcAfee製品

McAfeeが提供する次世代のセキュリティは、最近の回避型マルウェアを阻止するように設計されています。機械学習を利用した強力な解析機能とアプリケーションの隔離ツールにより、隠れた脅威をより迅速に検出し、攻撃を未然に防ぎます。

これらの機能は、次のMcAfee製品に搭載されています。

Real Protect

McAfee Endpoint Protectionの一つであるReal Protectは、McAfeeのエコシステムに統合され、実行前の静的分析と実行後の動作分析を行います。シグネチャや静的分析のみのソリューションよりも多くのマルウェアを検出し、阻止します。Real Protectは、最新の機械学習技術を利用し、静的な特徴（実行前の分析）と処理（動的な動作分析）を詳しく分析し、不正なコードを特定します。これらの分析はすべてシグネチャなしで実行されます。Real Protectは最新の難読化技術を解読し、回避技術を使用した脅威を検出します。ゼロデイ マルウェアも見逃しません。

アプリケーションの動的隔離

McAfee Endpoint Protectionに含まれるアプリケーションの動的隔離（DAC）は、新しいゼロデイ マルウェアの感染からエンドポイントを保護します。エンドポイントが不正なファイルを検出すると、DACは、マルウェアによく見られる動作（レジストリの変更、一時ディレクトリへの書き込み、ファイルの削除など）をすぐにブロックします。ファイルやユーザーの操作を中断する他の技術と異なり、DACは不審なファイルを読み込みますが、エンドポイントに対する変更や他のシステムへの侵入は許可しません。

Real ProtectとDACは統合されています。また、SPLUNK、Avecto、ForeScoutなどの他社製品やMcAfee Endpoint Protectionに統合し、回避型の脅威に対して多層型の防御策を構築できます。高速で自動化されたソリューションにより、検出、修復、予防の脅威対策ライフサイクル全体で問題を解決することができます。

Real ProtectとDACにより、次のことが可能になります。

- 脅威の検出: 難読化を解除するので、より多くのマルウェアを検出できます。
- 影響の軽減: 攻撃の実行前あるいは修復不能な被害が発生する前に、脅威を封じ込めます。
- 追跡と適応: 自動化された統合ソリューションにより、様々な保護作業を簡単に行うことができます。

Real ProtectとDACで回避型のマルウェアを封じ込める方法については、こちらの動画をご覧ください。

アプリケーションの動的隔離を設定する場合のベストプラクティス
McAfee Defaultポリシーの DACルールは、報告のみに設定されているので、誤検知が少なくなります。適応脅威対策には、McAfee DefaultバランスとMcAfee Defaultセキュリティの2つのDACポリシーが事前に定義されています。これらのポリシーでは、セキュリティ プロファイルに基づいて推奨のブロック ルールが設定されています。

- McAfee Defaultバランスでは、一般的な未署名のインストーラーやアプリケーションに対する誤検知を最小限に抑えながら、基本レベルの保護対策を提供します。
- McAfee Defaultセキュリティでは、積極的な保護対策を提供します。未署名のインストーラーやアプリケーションで誤検知の発生頻度が高くなる可能性があります。

McAfee Defaultポリシーで報告用のルールを設定して、DACルールの影響を確認します。ログとレポートをモニタリングして、ブロック ルールを設定するかどうか判断します。McAfee Defaultバランス ポリシーを施行する前に、許可されたDAC違反（イベントID 37280）を収集し、エンタープライス レベルのレピュテーションまたはDACの除外対象を設定します。

DACでは、名前、MD5ハッシュ、署名データ、パスに基づいてプロセスを隔離対象から除外できます。組織で内部用のツールに署名している場合には、誤検知を減らすため、これらのツールの署名を除外対象として追加します。

DACルールではフラッド制御を設定できます。1時間ごと、ルールごと、プロセスごとに同時に生成されるイベント数を制限します。DACフラッド制御はプロセスIDでプロセスを追跡します。プロセスが再開すると、オペレーティング システムはプロセスに新しいIDを割り当てるので、プロセス名が同じであってもフラッド制御がリセットされます。たとえば、プロセスAがDACルールAに1時間で100回違反した場合、1時間に1つのイベントを受信します。1時間以内にプロセスAが再開すると、プロセスAのフラッド制御がリセットされ、DACルールAに対する違反が継続しても別のイベントを受信します。プロセスBが同じDACルールAに違反すると、2つ目のイベント（プロセスBの詳細を含む）を受信します。McAfee定義のDACルールに関するベストプラクティスの詳細については、こちらをご覧ください。

本稼働環境のシステムで、配備の基本イメージにMcAfeeのGetCleanツールを実行し、正常なファイルをMcAfee Global Threat Intelligence（GTI）に送信して分類します。これにより、McAfee GTIからファイルの正しいレピュテーションを取得できます。詳細については、GetClean 製品ガイド（PD23191）をご覧ください。

McAfee Cloud Threat Detection
McAfee Cloud Threat Detection（CTD）を利用して高度な脅威や回避型の脅威を検出することで、McAfeeの保護製品を簡単に強化できます。McAfee ePO CloudにアクセスしてMcAfee CTDを有効にし、McAfee製品に統合しましょう。

McAfeeのセキュリティ製品でMcAfee CTDの機能を利用するには、次の操作を行います。

- McAfee ePO CloudでMcAfee CTDを有効にする。
- McAfeeのセキュリティ製品のインターフェースでMcAfee CTDを有効にし、プロビジョニング キーを取得する。
- McAfee ePO Cloudのインターフェースで、プロビジョニング キーからライセンス登録キーを生成する。
- ライセンス登録キーを使用して、McAfeeのセキュリティ製品を登録する。

プロビジョニング キーの取得と製品登録の手順は製品によって若干異なります。McAfee CTDとご利用のMcAfee製品を統合する方法については、製品ガイドをご覧ください。

統合された製品がMcAfee CTDに分析用のファイルを送信すると、McAfee ePO Cloudの［ご契約情報］ページに使用状況が表示されます。

McAfee Active Response

- McAfee Active Responseは、業界最高の技術を利用して高度な脅威を検出し、阻止します。McAfee GTI、Dell SecureWorks、ThreatConnectなどの脅威フィードと関連付けると、広範囲に拡散する前に回避型の脅威を検出し、被害を未然に防ぐことができます。
- カスタム コレクターを使用すると、トロイの木馬化されたアプリケーションの侵害兆候を検出し、識別するツールを作成できます。
- トリガーや対応はユーザーが作成し、特定の条件下で実行されるアクションを定義します。たとえば、特定のハッシュまたはファイル名見つかったときに、削除アクションを自動的に実行します。

詳細情報

高度脅威の無効化: 包括的なマルウェア対策で多層型の防御を実現

McAfee Security Advice Center: マルウェアとトロイの木馬を防御する最優先の10の方法

McAfee Endpoint Security: よくある質問

McAfee Together is power.
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