ソリューション概要

正規のソフトウェアがトロイの木馬に

感染と拡散を防ぐIntel® Security製品

インターネットでソフトウェアを配信する方法がマルウェアやウイルスの攻撃でも利用されています。10年前の不正なバインダーに比べると、その手口は明らかに進化しています。現在では、ソフトウェアの配信前や配信中に、正規のソフトウェアがトロイの木馬に変えられています。

トロイの木馬が進化しても、基本的な攻撃手順に変わりはありません。

- ソフトウェアの武器化: 配信可能なアプリケーションにマルウェアを挿入する。
- 配信: トロイの木馬に感染したソフトウェアを検出されない方法で攻撃対象に転送する。
- 侵入: トロイの木馬のコードを実行して潜伏する。
- 拡散: 持続性を維持し、他のシステムへの拡散を試みる。

最近の攻撃では、正規のダウンロードの途中で不正なコードを混入し、検出を免れています。攻撃の方法は、元のアプリケーションに不正なコードを混ぜることです。

攻撃対象に確実に侵入するため、この攻撃ではリスナーとバインダーという2つのコンポーネントを使用します。リスナーがHTTPダウンロード要求を傍受して変更し、バインダーがその要求に感染してバイナリを配布します。

現在のアルゴリズムは、マルウェアの感染ルーチンとネットワーク リダイレクト攻撃から構成され、アプリケーションのコードには変更を行いません。これにより、市販のアプリケーションやオープンソースのソフトウェアから署名付きの実行ファイルを生成できます。最初の実行前に署名が自動的に検査されなければ、攻撃に成功します。

トロイの木馬に感染したアプリケーションを実行すると、バインダー プロセスが独自のファイルを生成して、追加の実行ファイルを埋め込みます。これにより、ファイルが挿入されたコードは次の実行時には姿を変えているため、セキュリティ対策の検出を逃れることができます。元のアプリケーションは改ざんされていないため、署名付きのファイルに添付されたマルウェアによる攻撃が続く可能性があります。

intel Security

ポリシーと手順

Intel Security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。

- 信頼されていないネットワークに接続する場合には仮想プライベート ネットワークを使用する。セキュリティ ソフトウェアは常に最新の状態にしてください。偽装が疑われる兆候ではなく、信頼性の高い兆候を使用してください。アプリケーションに署名し、信用チェーンで検証してください。フォレンジック分析を行い、信頼されたソースとハッシュの関連付けを行ってください。
- セキュリティ ソフトウェアで動的分析を行い、最初のバイナリ検査の結果に関係なく、不正なアクションにフラグを設定する。最初の検査では静的なスキャンしか実行されません。動作モニタリング、WebとIPのレピュテーション、メモリー スキャン、アプリケーションの隔離などは、ソリューションを構成する重要な要素となります。
- ベンダーのダウンロードは安全な接続を使用し、すべてのコードに署名を付けてから行う。これにより、仲介者攻撃の発生率を劇的に抑えることができます。ソフトウェア ベンダーは自社のアプリケーションに自己検証機能を追加する必要があります。コードを定期的に監査し、静的コード分析ツールを使用して評価を行う必要があります。社内で信頼されたアプリケーションをリポジトリで一元管理し、それ以外の場所からのダウンロードを禁止することで、承認済みのインストーラーの実行をユーザーに許可することができます。
- 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する。
- ホスト侵入検出/防止アプリケーションを使用して、パケットを検査し、不正なペイロードかどうかを識別する。
- 信頼された仮想化アーキテクチャのみを使用し、適切なネットワーク分割を行う。信頼された仮想化アーキテクチャでは、安全で検証可能な方法で起動プロセスを実行します。ネットワーク セグメントは、トラフィックを監視し、攻撃が発生した場合には、イベントに応じてアプリケーションを隔離します。この2つを組み合わせことで最新のマルウェア対策で保護することができます。
- トロイの木馬化したソフトウェアが配布するマルウェアを特定するため、送信トラフィックを監視する。インターネットにトラフィックが送信されることもあり、修復中に感染マシンが露出する可能性があります。

Intel Security

Intel Securityの製品は、トロイの木馬化した正規のソフトウェアを識別し、埋め込まれたマルウェアの脅威を阻止します。また、侵害を検出し、迅速に対応します。

McAfee VirusScan® Enterprise 8.8**または**McAfee Endpoint Security 10

- 常に最新のDATファイルを使用します。
- McAfee Global Threat Intelligence（McAfee GTI）を使用します。McAfee GTIは600万を超えるランサムウェアのシグネチャを保持しています。
- アクセス保護ルールを作成して、ランサムウェアのインストールを阻止します。
  - アクセス保護ルールの詳細は、KnowledgeBaseの記事KB81095、KB54812を参照してください。
  - McAfee VirusScan 8.8 Enterpriseの設定に関するベストプラクティスを参照してください（PD22940）。
  - McAfee Endpoint Security の設定に関するベストクラクティスを参考してください（KB86704）。

McAfee Host Intrusion Prevention

- McAfee Host Intrusion Preventionはマルウェアの拡散を阻止します。IPSカスタム シグネチャを使用してルールを作成すると、マルウェアが行うファイル操作（作成、書き込み、不正なコードなど）を阻止できます。
- Host Intrusion Preventionのシグネチャ3894 Access Protection—Prevent svchost.exe executing non-Windows executables（アクセス保護－svchost.exe によるWindows以外の実行ファイルの実行阻止）を有効にします。
- Host Intrusion Preventionシグネチャ6010と6011を有効にして、インジェクションをすぐにブロックします。
- サブルールには次の2種類あります。

1. Filesエンジンと次の条件のサブルールを使用してIPSカスタム シグネチャを作成します。
   - Name: <名前を挿入>
   - Rule type: Files
   - Operations: Create, Execute, Read, Write
   - Parameters: Include - Files - <マルウェアのパス/ファイル名>
     - ファイル名はパスにする必要があります。パスにワイルドカードを使用する場合、**\ または?:\というファイル名で始めます。ドライブ文字をワイルドカードで表すこともできます。例: **\<ファイル名>.exe、?:\<ファイル名>.exe
     - FilesパラメーターでMD5ハッシュを使用できません。使用できるのはパス/ファイル名だけです。
     - ドライブの種類を指定して、特定のドライブへのパスに限定できます（例: ハードディスク、CD-ROM、USB、ネットワーク、フロッピーなど）。
   - Executables: ファイル操作を実行する特定のプロセス（explorer.exe、cmd.exeなど）にシグネチャを制限する場合を除き、何も指定する必要はありません。
2. Programエンジンと次の条件のサブルールを使用して、IPSカスタム シグネチャを作成します。
   - Name: <名前を挿入>
   - Rule type: Program
   - Operations: Run target executable
   - Parameters: <空白にします>
   - Executables: ソースの実行ファイルとして特定のプロセスにシグネチャを制限する場合を除き、何も指定する必要はありません。たとえば、explorer.exeが対象の実行ファイル（notepad.exeなど）を実行しないように設定します。
   - Target Executables: ブロックする実行ファイルのプロパティを定義します。たとえば、notepad.exeの実行をブロックする場合には、この実行ファイルのパスとファイル名を指定します。1つ以上の条件（ファイルの説明、ファイル名、フィンガープリント、署名者）を使用して、実行ファイルを定義します。

McAfee SiteAdvisor® Enterprise**または**McAfee Web Protection

• Webサイトのレピュテーションにより、トロイの木馬を配布するサイトの利用を阻止または警告します。

McAfee Threat Intelligence ExchangeとMcAfee Advanced Threat Defense

- Threat Intelligence Exchangeのポリシー設定:
  - 監視モードを開始します。エンドポイントで不審なプロセスを検出したときに、システム タグを使用してTIE施行ポリシーを適用します。
  - 駆除: 既知の不正な項目
  - ブロック: 不正である可能性が非常に高い項目。レピュテーションが不明なファイルをブロックすると、保護対策は強化されますが、初期の管理作業が増えます。
  - レピュテーション レベルが不明以下の場合、McAfee Advanced Threat Defenseにファイルを送信します。
  - Threat Intelligence Exchangeサーバーのポリシー: Threat Intelligence Exchangeが未確認のファイルは、Advanced Threat Defenseのレピュテーションを使用します。
- Threat Intelligence Exchangeの手動操作:
  - ファイル レピュテーションの施行（動作モードによる）。 不正な可能性が非常に高い: 駆除/削除
  - 不正な可能性がある: ブロック
- エンタープライズ レピュテーションでMcAfee GTIのレピュテーションを上書きできます。
  - たとえば、非対応または脆弱なアプリケーションの不要をブロックできます。
  - ファイルに「不正な可能性がある」というマークを付けます。
- テスト目的で不要なプロセスを許可します。
  - ファイルに「信頼できる可能性がある」というマークを付けます。

McAfee Advanced Threat Defense

- すぐに使える検出機能:
  - シグネチャ ベースの検出: McAfee Labsが維持するシグネチャは6億個を超えています。
  - レピュテーション ベースの検出: McAfee GTI
  - リアルタイムの静的分析とエミュレーション: シグネチャ レスでの検出に使用されます。
  - カスタムYARAルール
  - 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、その属性と機能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。
  - 動的なサンドボックス分析
- 分析用のプロファイルを作成し、トロイの木馬化されたソフトウェアが実行される可能性が高い場所を特定します。
  - 一般的なOS、Windows 7、8、10
  - Windowsアプリケーション（Word、Excel）をインストールしてマクロを有効にします。
- アナライザーを使用してインターネット アクセスを分類します。
  - サンプルの多くは、Microsoftドキュメントに含まれるスクリプトを実行し、外部に接続してマルウェアによる攻撃を開始します。アナライザーを使用することで、インターネット接続のプロファイリングを行い、検出率を向上させています。

McAfee Network Security Platform

- Network Security Platformは、デフォルト ポリシーに定義されたシグネチャを使用して、マルウェア関連のファイル転送に使用されるTORネットワークを検出します。
- Advanced Threat Defenseとの統合で新しい亜種を検出します。
  - 詳細なマルウェア ポリシーでAdvanced Threat Defenseとの統合を設定します。
  - Network Security Platformが.exe、Microsoft Office、Javaアーカイブ、PDFファイルをAdvanced Threat Protectionに送信し、検査するように設定します。
  - Advanced Threat Protectionの設定がセンサー レベルで適用されていることを確認します。
- コールバック検出ルール（ボットネット用）を更新します。

McAfee Web Gateway

- McAfee Gateway Anti-Malwareによる検査を有効にします。
- McAfee GTIを有効にして、URLとファイルのレピュテーションを使用します。
- Advanced Threat Defenseと統合し、サンドボックスでゼロデイ脅威を分析します。

VirusTotal Convicter: 自動処理

- Convicterは、McAfee ePolicy Orchestrator®（McAfee ePO）の自動応答システムで実行されるPythonスクリプトです。McAfee Threat Intelligence Exchange脅威イベントを生成したファイルをVirusTotalで調査できます。
- GetSuspなど、他の脅威情報交換を参照するようにスクリプトを変更できます。
- コミュニティの信頼しきい値を満たしていれば、スクリプトはエンタープライズ レピュテーションを自動的に設定します。推奨のしきい値: ベンダーの30%と大手2社の同意が必要
- フィルター: 対象のファイル名が次の項目を含まない: McAfeeTestSample.exe
- これは無料のコミュニティ ツールです（Intel Securityのサポートはありません）。

McAfee Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Responseは、高度な脅威を検出し、問題に対応します。McAfee Labs、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新しい脅威を検出し、被害を未然に防ぐことができます。
- カスタム コレクターにより、トロイの木馬化したアプリケーションの侵害兆候を検出し、識別する特定の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、ハッシュまたはファイル名が見つかったときに、削除アクションを自動的に実行します。

詳細情報

Best Practices for how to use McAfee Host Intrusion Prevention rules for a malware outbreak（マルウェア大量発生時のMcAfee Host Intrusion Preventionルールの使用方法）: KB84507

次のKnowledgeBaseの記事には、Trojan-Powelikeに関する詳しい情報が記載されています。

Infection and Propagation Vectors（感染と拡大の経路）: PD25582

SIEM Orchestration: Orchestration Triggers Signs of Malware Infection and Anomalous Behaviors（SIEMオーケストレーション: オーケストレーションでマルウェア感染と異常動作の兆候を把握する）: PD24830

ホワイト ペーパー: Secure Beyond the Signature（シグネチャを超えたセキュリティ）

FAQs for Network Security Platform: Advanced Malware Detection（Network Security PlatformのFAQ）: 高度なマルウェア検出 KB75269

McAfee Web Gateway製品ガイド: Webフィルタリング PD26339

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