ソリューション概要

GPUマルウェアに対する防御

『McAfee® Labs脅威レポート: 2015年8月』では、エンドポイントのシステムメモリーやCPUではなく、グラフィックス処理装置（GPU）を攻撃するマルウェアを詳しく解説しています。

エンドポイントのGPUを悪用するマルウェアは新しいものではありません。4年ほど前には、感染先でBitcoinマイニングの処理速度を向上させるためにGPUを利用したトロイの木馬が確認されています。GPUマルウェアが再び注目を集めているのは、GPUの機能を全く新しい方法で悪用する概念検証コードが公開されたためです。前述のレポートに詳しく説明されていますが、この特徴をまとめると、次のようになります。

- GPUからCPUホスト メモリーにアクセスする
- その後にCPUホスト ファイルを削除する
- ウオーム リブート後も削除されない
- GPU分析ツールが存在しない

このような攻撃を行うマルウェアはまだ概念検証の段階であり、実際の攻撃は確認されていませんが、GPUに対する脅威が現実のものであることには変わりありません。GPUのフォレンジック分析を行うツールが存在しないため、GPUに対する脅威のリバースエンジニアリングとフォレンジック分析はメモリーやCPUの脅威よりも複雑で、厄介な作業になっています。攻撃者は不正なコードをCPUとメモリーから移すことで検出を回避しようとしていますが、エンドポイントで脅威の痕跡が完全になくなるわけではありません。

攻撃者にとってGPUマルウェアは有効な手段であることは確かですが、どの程度のメリットがあるのかはまだ分かりません。

GPUマルウェアに対する防御

McAfee Labsでは、GPUに対する攻撃からシステムを保護するため、いくつかの方法を推奨しています。

- システムの自動更新を有効にする。あるいは、OSの更新を定期的にダウンロードし、オペレーティング システムにパッチを適用して既知の脆弱性を解決する。
- ソフトウェア ベンダーが公開したパッチを速やかに適用する。
- すべてのエンドポイントにセキュリティ ソフトウェアを配備し、ウイルス対策のシグネチャを常に最新の状態にしておく。
- アプリケーションをホワイトリストに登録して、未承認のアプリケーションの実行を防ぐ。
- 可能であれば、管理者モードでアプリケーションを実行しない。

intel Security

GPUマルウェアから保護するIntel Securityのソリューション

McAfee Advanced Threat Defense

McAfee Advanced Threat Defenseは複数の検出エンジンを統合し、多層型のマルウェア検出ソリューションを提供します。McAfee Advanced Threat Defense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、高度な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 Advanced Threat Defenseは、1億5,000万件を超えるシグネチャなど、McAfee Labsが提供する総合的な情報を利用します。
- **レピュテーション ベースの検出:** McAfee Global Threat Intelligence（McAfee GTI）サービス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マルウェアやゼロデイ脅威を迅速に検出します。
- **コードの完全な静的分析:** 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:** 仮想のランタイム環境でファイルのコードを実行し、動作を検証します。仮想環境は会社のホスト環境に合わせて設定できます。Microsoft Windows 7（32/64ビット）、Windows XP、Windows Server 2003、Windows Server 2008（64ビット）、Androidのカスタム オペレーティング システム（OS）イメージを使用できます。

McAfee VirusScan Enterprise

McAfee VirusScan® Enterpriseは、実績豊富なIntel Securityのスキャン エンジンを搭載し、ウイルス、ワーム、ルールキット、トロイの木馬などの高度な脅威を阻止します。

- **攻撃をプロアクティブに阻止:** マルウェア対策と侵入防止機能が統合され、アプリケーションに存在するバッファー オーバーフローの脆弱性に対する攻撃を阻止します。
- **非常に強力なマルウェア検出/駆除機能:** 高度な動作分析により、ルートキットやトロイの木馬などの脅威を阻止します。ポート ブロック、ファイル名でのブロック、フォルダー/ディレクトリのロック、ファイル共有のロック、感染の追跡/ブロックにより、マルウェアの侵入を阻止します。
- **McAfee GTIの統合でリアルタイムのセキュリティを実現:** 市場で最も包括的な脅威情報プラットフォームにより、ファイル、Web、メール、ネットワークを介して侵入する既知の脅威だけでなく、新たに発生する脅威も阻止します。

McAfee Threat Intelligence Exchange

McAfee Threat Intelligence Exchangeは、環境の要件に合わせて拡張できるインテリジェントなプラットフォームを採用しています。不明なファイルやアプリケーションなど、組織に存在する脅威を正確に把握し、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 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(IoC):** 既知の不正ファイル ハッシュをMcAfee Threat Intelligence Exchangeにインポートしてポリシーを施行することで、これらの既知の不正ファイルから環境を保護できます。環境でIoCを確認すると、McAfee Threat Intelligence ExchangeがIoCに関係するすべてのプロセスとアプリケーションを終了します。

McAfee Application Control

McAfee Application Controlでは、動的ホワイトリストとポリシーの施行により、環境内で実行を許可するアプリケーションを制御できます。この機能は、ネットワークに接続しているエンドポイントだけでなく、接続していないエンドポイントにも実行できます。これにより、脆弱なアプリケーションや既知の不正なアプリケーションから組織を保護できます。

- **動的ホワイトリスト:** システムにパッチが適用され、最新の状態になると、ホワイトリストが自動的に作成されます。ホワイトリストに登録されたアプリケーションを効率的に管理できます。
- **ファイル レピュテーション:** McAfee GTIとの統合により、McAfee Application Controlはファイルのレピュテーション情報(正常、不正、不明)をリアルタイムに取得します。この情報とホワイトリスト機能により、改ざんの可能性があるアプリケーションを常に監視し、対策を講じることができます。
- **接続状態に関係のない保護:** 接続または切断状態のサーバー、仮想マシン、エンドポイント、POSなどの専用端末を保護します。

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