Secure Endpointの不正利用防止のトラブルシューティング

内容

概要

このドキュメントでは、Secure EndpointコンソールのExploit Prevention(VIPS)エンジンの設定と、基本的な分析の実行方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアエンドポイントコンソールへの管理者アクセス
- セキュアエンドポイントコネクタ
- Exploit Prevention機能が有効

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Connectorバージョン7.3.15以降
- Windows 10バージョン1709以降またはWindows Server 2016バージョン1709以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントで説明する手順は、コンソールでトリガーされるイベントに基づいて基本的な分析を実行する方法に役立ちます。プロセスを把握し、環境で使用する場合は、エクスプロイト防止の除外を推奨します。

エクスプロイト防止エンジンは、マルウェアやパッチが適用されていないソフトウェアの脆弱性に対するゼロデイ攻撃で一般的に使用されるメモリ注入の攻撃からエンドポイントを保護する機能を提供します。保護されたプロセスに対する攻撃を検出すると、そのプロセスはブロックされ、イベントが生成されますが、隔離されません。

保護されたプロセス

Exploit Prevention Engineは、次の32ビットおよび64ビット（Secure Endpoint Windowsコネクタバージョン6.2.1以降）プロセスとその子プロセスを保護します。

- Microsoft Excelアプリケーション
- Microsoft Wordアプリケーション
- Microsoft PowerPointアプリケーション
- Microsoft Outlookアプリケーション
- Internet Explorerブラウザ
- Mozilla Firefoxブラウザ
- Google Chromeブラウザ
- Microsoft Skypeアプリケーション
- TeamViewerアプリケーション
- VLC Media Playerアプリケーション
- Microsoft Windowsスクリプトホスト
- Microsoft Powershellアプリケーション
- Adobe Acrobat Readerアプリケーション
- Microsoft Register Server
- Microsoftタスクスケジューラエンジン
- Microsoft Run DLLコマンド
- Microsoft HTMLアプリケーションホスト
- Windowsスクリプトホスト
- Microsoftアセンブリ登録ツール
- ZOOM
- スラック
- Cisco Webex Teams
- Microsoft Teams

除外されたプロセス

これらのプロセスは、互換性の問題により、Exploit Preventionエンジンから除外されます（モニタされません）。

- McAfee DLPサービス
- McAfeeエンドポイントセキュリティユーティリティ

Exploit Preventionバージョン5（Connectorバージョン7.5.1以降）

Secure Endpoint Windowsコネクタ7.5.1には、悪用の防止に関する重要なアップデートが含まれています。このバージョンの新機能は次のとおりです。

- ネットワークドライブの保護：ネットワークドライブから実行されるプロセスを、ランサムウェアなどの脅威から自動的に保護
- リモートプロセスの保護：ドメイン認証されたユーザー(admin)を使用する保護されたコンピューターでリモートで実行されるプロセスを自動的に保護します
- AppControlがrundll32をバイパスする：解釈されたコマンドの実行を許可する、特別に巧妙に細工されたrundll32コマンドラインを停止します
- UACバイパス：悪意のあるプロセスによる権限昇格をブロックし、Windowsユーザーアカウント制御メカニズムのバイパスを防ぐ
- ブラウザ/Mimikatz資格情報の資格情報：エクスプロイト防止を有効にすると、Microsoft Internet Explorerおよびエッジブラウザでクレデンシャルの盗難から保護されます
- シャドウコピーの削除：シャドウコピーの削除をトレースし、Microsoftボリュームシャドウコピーサービス(vssvc.exe)のCOM APIをインターセプトします
- SAMハッシュ：MimikatzによるSAMハッシュの資格情報の盗難から保護し、レジストリハイブComputer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users内のすべてのSAMハッシュを列挙および復号化する試みを傍受します。

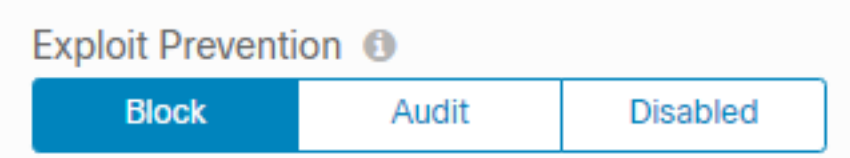
- 実行された保護プロセス：エクスプロイト防止インスタンス(explorer.exe、lsass.exe、spoolsv.exe、winlogon.exe)より前に起動したプロセスは、実行するプロセスにインジェクトします。

これらの機能はすべて、ポリシーでExploit Preventionが有効になっている場合にデフォルトで有効になります。

コンフィギュレーション

エクスプロイト防止エンジンを有効にするには、図に示すように、ポリシーで[Modes and Engines] に移動し、[Audit mode]、[Block mode]、または[Disabled mode]を選択します。

> **注**：監査モードは、Secure Endpoint Windowsコネクタ7.3.1以降でのみ使用できます。以前のバージョンのコネクタでは、監査モードはブロックモードと同じように扱われます。



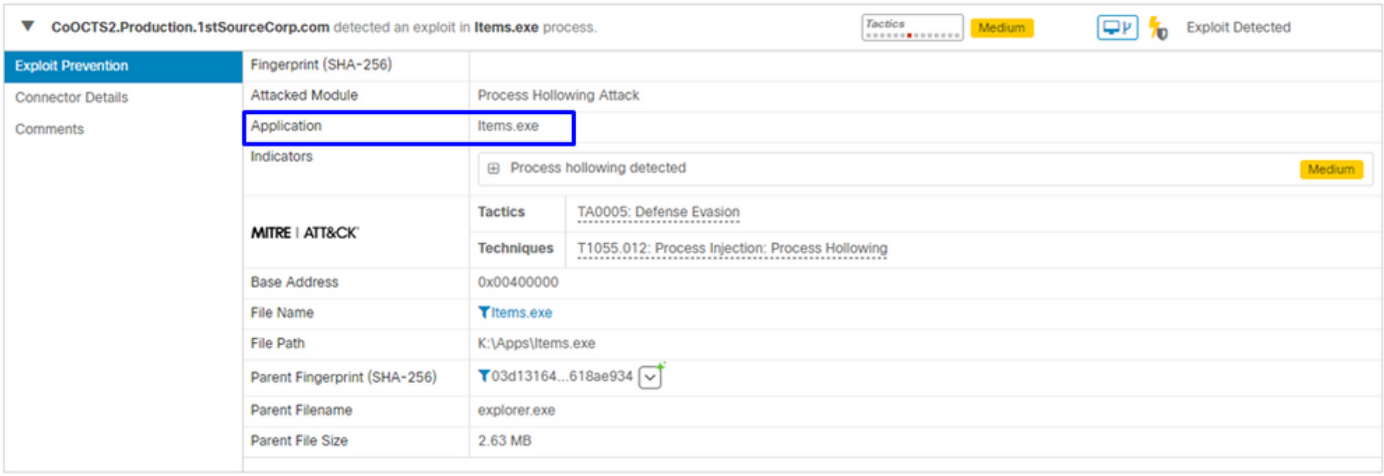
> **注**：Windows 7およびWindows Server 2008 R2では、コネクタをインストールする前に、Microsoft Security Advisory 3033929のパッチを適用する必要があります。

検出方法

検出がトリガーされると、図に示すように、ポップアップ通知がエンドポイントに表示されます

。

図に示すように、コンソールにExploit Preventionイベントが表示されます。

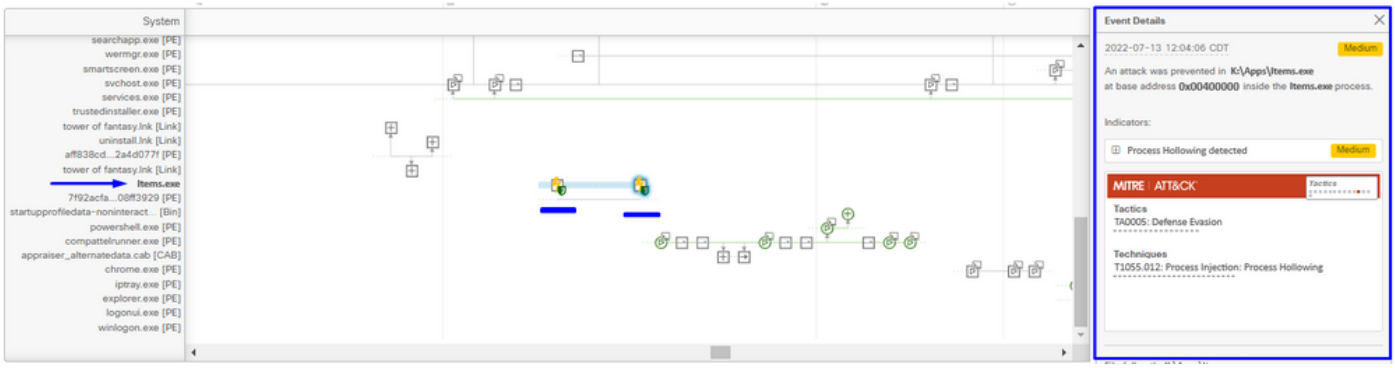


トラブルシュート

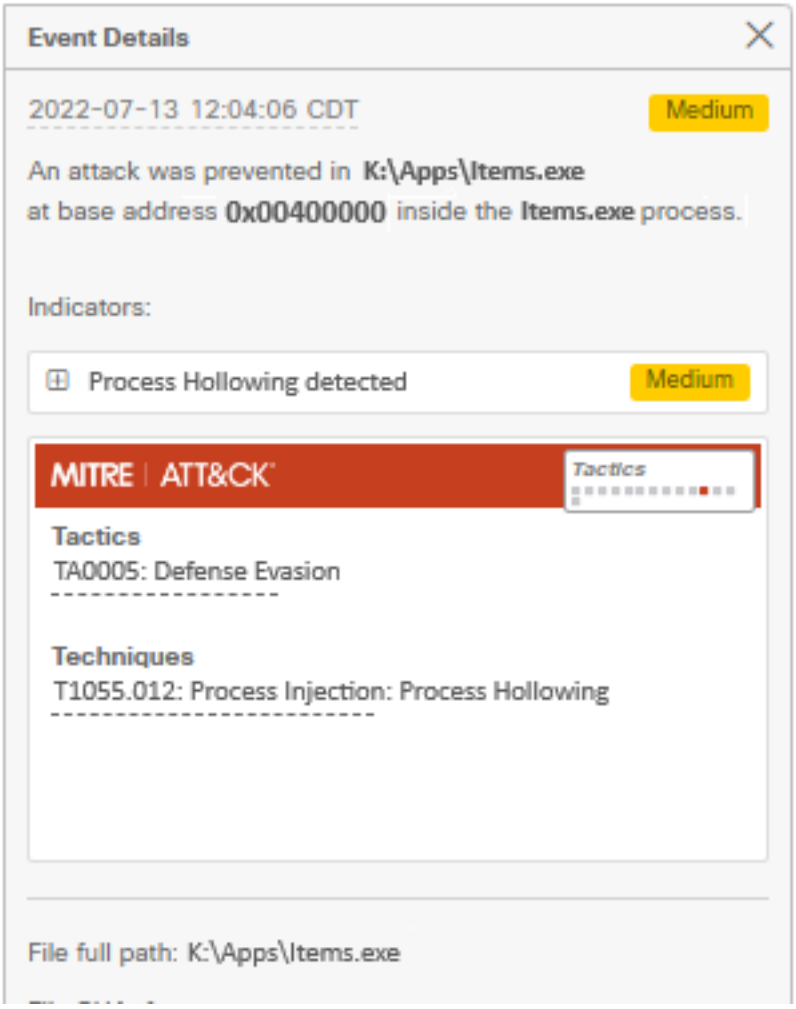
コンソールでExploit Preventionイベントがトリガーされると、検出されたプロセスを識別する方法が詳細に基づいて実行され、アプリケーションまたはプロセスの実行中に発生したイベントを確認できます。**デバイストラジェクトリ**に移動できます。

ステップ1：図に示すように、Exploit Preventionイベントに表示される**Device Trajectory**アイコンをクリックします。

ステップ2：図に示すように、[Event Details] セクションを表示するには、デバイストラジェクトリのタイムラインで[Exploit Prevention]アイコンを見つけます。



ステップ3：イベントの詳細を特定し、プロセスまたはアプリケーションが環境内で信頼されているか、または既知であるかを評価します。



誤検出

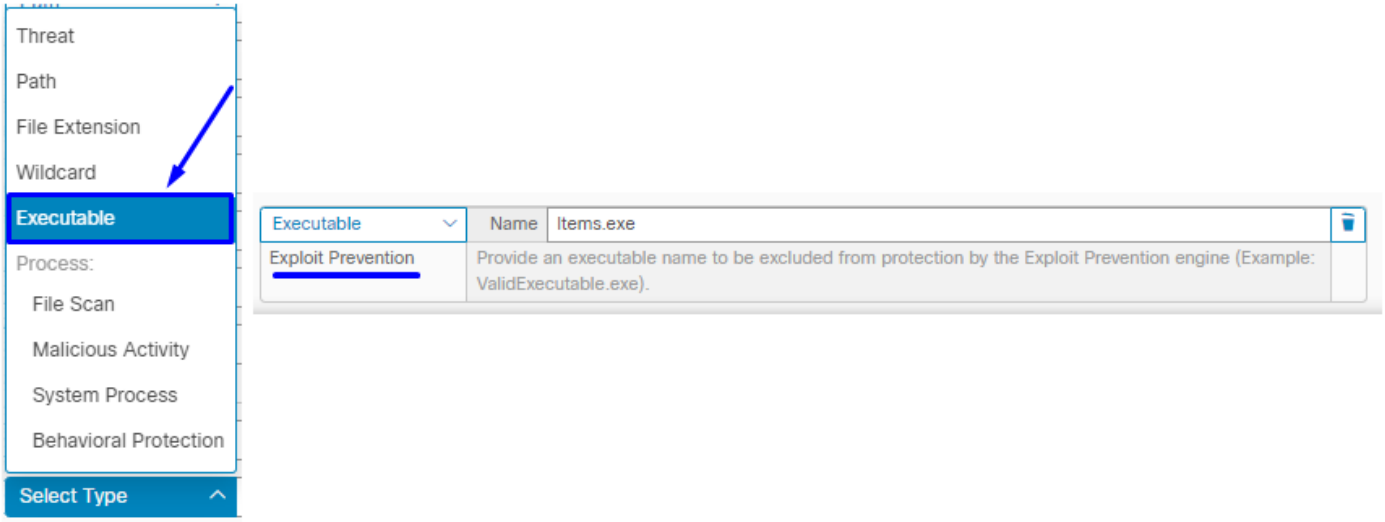
検出が特定され、プロセス/実行可能ファイルが信頼され、環境で認識されている場合は、除外として追加できます。コネクタがスキャンされるのを防ぐため。

実行可能な除外は、エクスプロイト防止（コネクタバージョン6.0.5以降）が有効になっているコネクタにのみ適用されます。実行可能除外は、特定の実行可能ファイルをエクスプロイト防止エンジンから除外するために使用されます。

> **注意**：ワイルドカードとexe以外の拡張子はサポートされていません。

保護されたプロセスのリストを確認し、Exploit Preventionエンジンから任意のプロセスを除外できます。アプリケーション除外フィールドに実行可能ファイル名を指定する必要があります。エンジンからアプリケーションを除外することもできます。実行可能ファイルの除外は、図に示すように、**name.exe**形式の実行可能ファイル名と正確に一致する必要があります。

> **注**：エクスプロイト防止から除外する実行可能ファイルは、除外がコネクタに適用された後で再起動する必要があります。また、Exploit Preventionを無効にした場合は、アクティブな保護されたプロセスを再起動する必要があります。



注：除外セットが、該当するコネクタに適用されるポリシーに追加されていることを確認します。

最後に、動作を監視できます。

不正利用の防止の検出が引き続き行われる場合は、TACサポートに連絡して、詳細な分析を実行してください。必要な情報は次のとおりです。

- Exploit Preventionイベントのスクリーンショット
- デバイストラジェクトリとイベントの詳細のスクリーンショット
- 該当するアプリケーション/プロセスのSHA256
- この問題は、Exploit Preventionがディセーブルになっている場合に発生しますか。
- この問題は、Secure Endpoint Connectorサービスが無効になっている場合に発生しますか。
- エンドポイントに他のセキュリティソフトウェアまたはアンチウイルスソフトウェアがあるか。
- 影響を受けるアプリケーション機能の説明
- 問題が発生したときにデバッグモードが有効になっている診断ファイル（デバッグバンドルログ）(この記事では、診断ファイルの収集方法について説明しています)

関連情報

- セキュアエンドポイントユーザガイド
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。