エンドポイント用AMPのスクリプト保護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、Advanced Malware Protection(AMP)for EndpointsでのScript Protection(PPROTECTION)エンジンの設定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。

- AMPコンソールへの管理者アクセス

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。

- コネクタバージョン7.2.1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

Script Protection Engineは、エンドポイントで実行されるスクリプトを検出してブロックする機

能を提供し、マルウェアが一般的に使用するスクリプトベースの攻撃から保護します。デバイストラジェクトリーは、チェーン実行を可視化するため、デバイスでスクリプトを実行するアプリケーションを確認できます。

エンジンを使用すると、コネクタは次のスクリプトファイルタイプをスキャンできます。

アプリケーション	ファイル拡張子
HTMLアプリケーション	HTA
スクリプト	BAT、CMD、VB、VBS、JS
暗号化スクリプト	JSE、VSE
Windowsスクリプト	WS、WASF、SWC、WSH
PowerShell	PS1、PS1XML、PSC1、PSC2、MSH、MSH1、MSH2、MSHXML、MSH1XM
ショートカット	SCF
リンク	LNK
セットアップ	INF、INX
レジストリ	REG
WORD	DOCX、DOTX、DOCM、DOTM
Excel	XLS、XLSX、XLTX、XLSM、XLTM、XLAM
PowerPoint	PPT、PPTX、POTX、POTM、PPTM、PPAM、PPSM、SLDM

スクリプト保護は、次のスクリプトインタープリタで動作します。

- PowerShell（V3以降）
- Windowsスクリプトホスト（wscript.exeおよびcscript.exe）
- JavaScript（ブラウザ以外）
- VBScript
- Office VBAマクロ

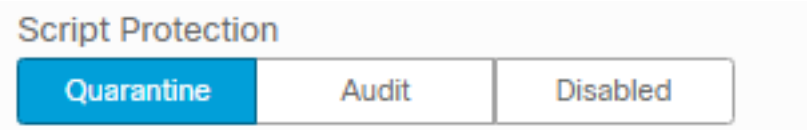
警告：スクリプト保護では、Python、Perl、PHP、またはRubyなどのMicrosoft以外のスクリプトインタプリタからの可視性と保護は提供されません。

注意：検疫の有罪判決モードは、Word、Excel、Powerpointなどのユーザーのアプリケーションに影響を与える可能性があります。これらのアプリケーションが悪意のあるVBAスクリプトを実行しようとすると、アプリケーションは停止します。

スクリプト保護は**On Execute Mode**を優先し、2つの異なるモードで動作します。**アクティブ**および**パッシブ**。Activeモードでは、コネクタが悪意があるかタイムアウトに達したかの情報を受信するまで、スクリプトの実行がブロックされます。パッシブモードでは、スクリプトが検索される間にスクリプトが実行され、悪意があるかどうかを判断できます。

コンフィギュレーション

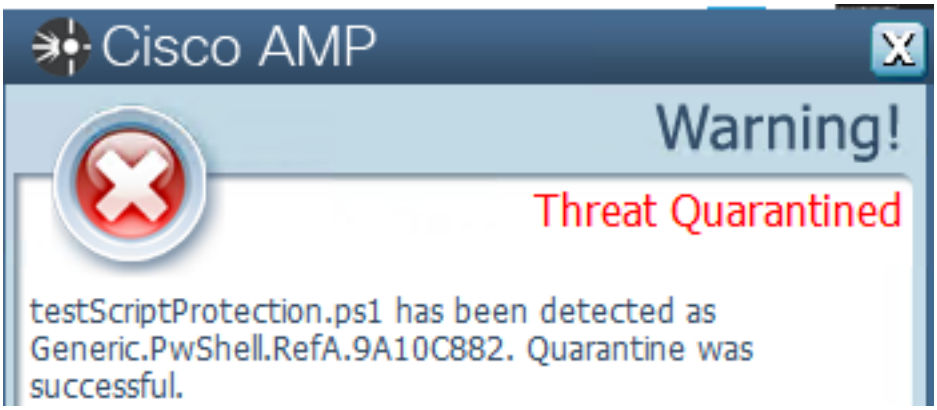
[Script Protection]を有効にするには、ポリシー設定に移動し、[Modes and Engines]で[Certification mode]から[Audit]、[Quarantine]、または[Disabled]を選択します（図を参照）。



注：スクリプト保護はTETRAに依存しませんが、TETRAが有効な場合は、TETRAを使用して保護を追加します。

検出方法

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



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

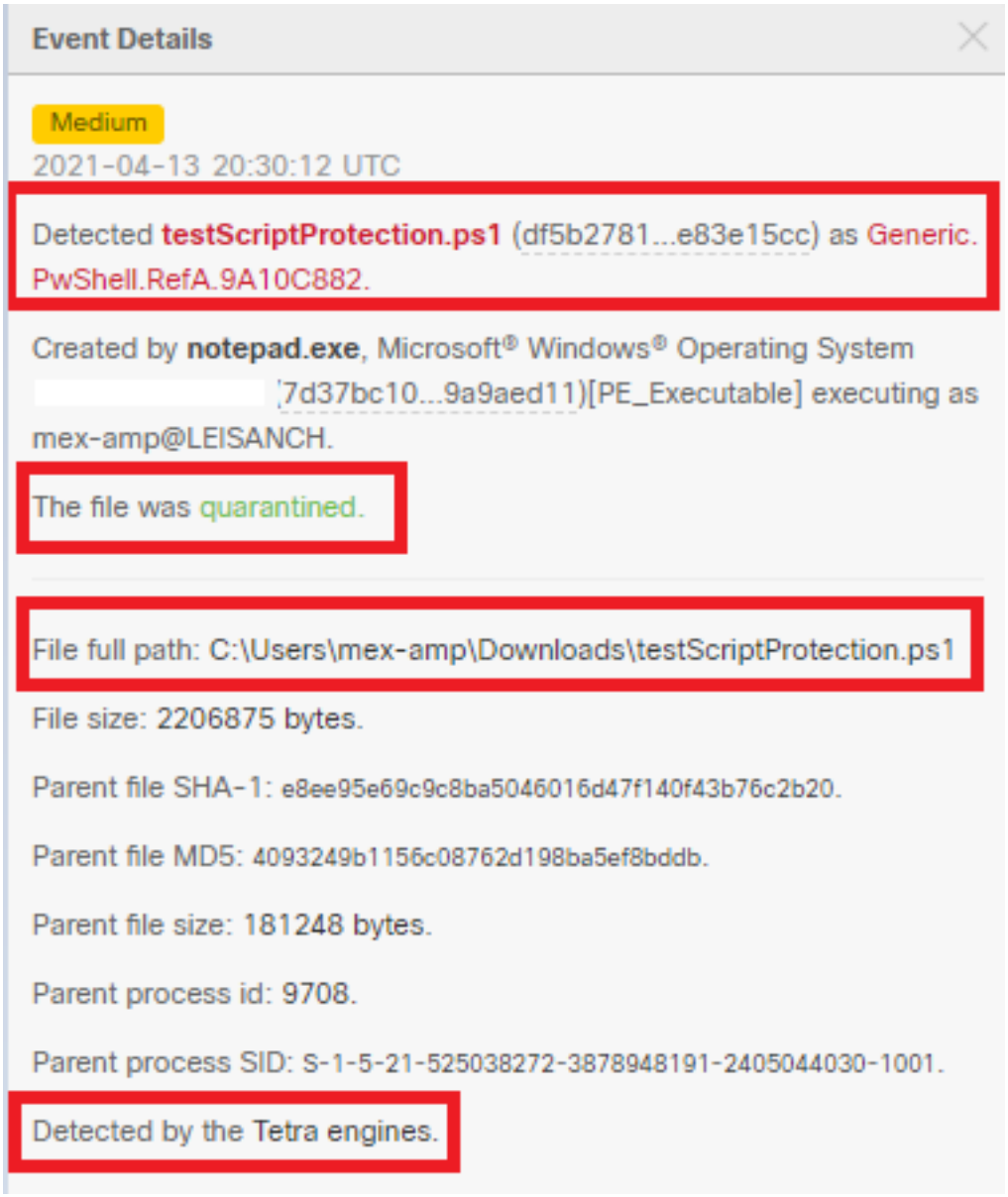
注：監査モードでは、悪意のあるスクリプトが実行されたときにイベントが作成されますが、検疫されません。

トラブルシュート

コンソールで検出がトリガーされた場合、スクリプト保護には特定のイベントタイプはありません。悪意のあるファイルを検出したユーザを特定する方法は、ファイルのタイプと実行場所に基づいています。

1.サポートされているスクリプトインタプリタに従って、ファイル拡張子を特定します。この例では.ps1スクリプトです。

2. [Device Trajectory] > [Event Details]に移動します。このセクションでは、SHA256、ファイルが存在したパス、脅威名、AMPコネクタで実行されたアクション、検出したエンジンなど、検出されたファイルに関する詳細が表示されます。TETRAが有効でない場合、表示されるエンジンはSHAエンジンです。この例では、TETRAが有効な場合、スクリプト保護と連携して図に示すように追加の保護を提供するため、TETRAが表示されます。



検出の調査

検出が実際に悪意があるかどうかを判断するには、デバイストラジェクトリーを使用して、スクリプトの実行中に発生したイベント（親プロセス、リモートホストへの接続、マルウェアによるダウンロードが可能な未知のファイルなど）を可視化します。

誤検出

検出が特定され、そのスクリプトが信頼され、環境で認識されている場合は、誤検出と呼ばれます。コネクタによるスキャンを防ぐために、図に示すように、スクリプトを除外できます。

> **注**：影響を受けるコネクタに適用されるポリシーに除外セットが追加されていることを確認します。

関連情報

- AMPユーザガイド
- テクニカル サポートとドキュメント – Cisco Systems