對面向終端的AMP中的指令碼保護進行故障排除

目錄

簡介

本檔案介紹面向端點的進階惡意軟體防護(AMP)中指令碼保護引擎的組態。

必要條件

需求

思科建議您瞭解以下主題：

- 管理員對AMP控制檯的訪問許可權

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 聯結器版本7.2.1或更高版本
- Windows 10 1709及更高版本或Windows Server 2016 1709及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

指令碼保護引擎能夠檢測和阻止在端點上執行的指令碼，並幫助防禦惡意軟體常用的基於指令碼的攻擊。「裝置軌跡」提供了鏈執行的可視性，因此您可以觀察在裝置上執行指令碼的應用程式。

引擎允許聯結器掃描以下指令碼檔案型別：

應用程式	副檔名

HTML應用程式	HTA
指令碼	BAT、CMD、VB、VBS、JS
加密指令碼	JSE、VSE
Windows指令碼	WS、WASF、SWC、WSH
PowerShell	PS1、PS1XML、PSC1、PSC2、MSH、MSH1、MSH2、MSHXML、MSH1XML、MSH
快捷方式	SCF
連結	LNK
設定	INF，INX
登錄檔	註冊
單詞	DOCX、DOTX、DOCM、DOTM
Excel	XLS、XLSX、XLTX、XLSM、XLTM、XLAM
PowerPoint	PPT、PPTX、POTX、POTM、PPTM、PPAM、PPSM、SLDM

指令碼保護可與以下指令碼解釋程式配合使用：

- PowerShell（V3及更高版本）
- Windows指令碼主機（wscript.exe和cscript.exe）
- JavaScript（非瀏覽器）
- VBScript
- Office VBA宏

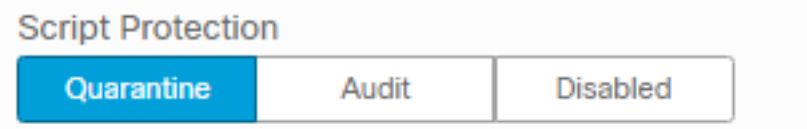
> **警告**：指令碼保護不能提供可視性，也不能防止非Microsoft指令碼直譯器（如Python、Perl、PHP或Ruby）的攻擊。

> **注意**：隔離通知模式可能會影響使用者的應用程式，如Word、Excel和Powerpoint。如果這些應用程式嘗試執行惡意VBA指令碼，則停止該應用程式。

指令碼保護使**用On Execute模式**，它可在兩種不同模式下工作：**主動**和**被動**。在活動模式中，阻止執行指令碼，直到聯結器收到有關指令碼是否為惡意或超時的資訊。在被動模式下，允許執行指令碼，同時查詢指令碼以確定其是否為惡意指令碼。

組態

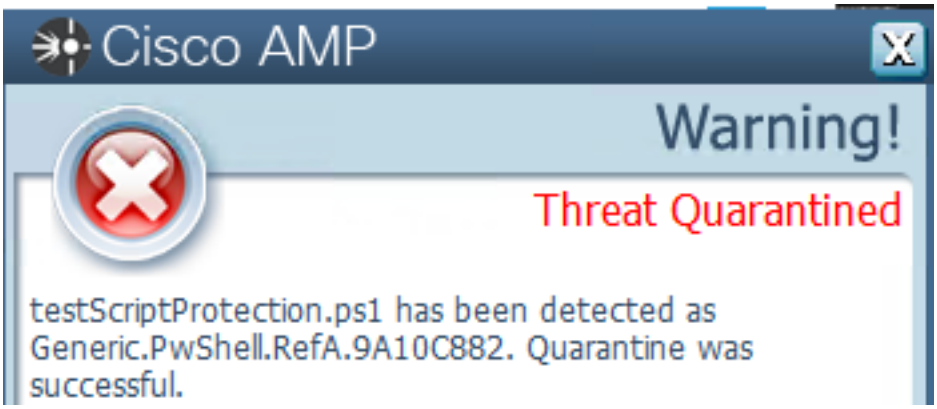
若要啟用指令碼保護，請導航到您的策略設定，然後在「模式和引擎」下選擇要稽核、隔離或禁用的判定模式，如下圖所示。



> **注意**：指令碼保護不依賴於TETRA，但是如果啟用TETRA，則它會使用它來提供額外的保護。

檢測

觸發檢測後，端點會顯示彈出通知，如下圖所示。



控制檯顯示「檢測到威脅」事件，如下圖所示。

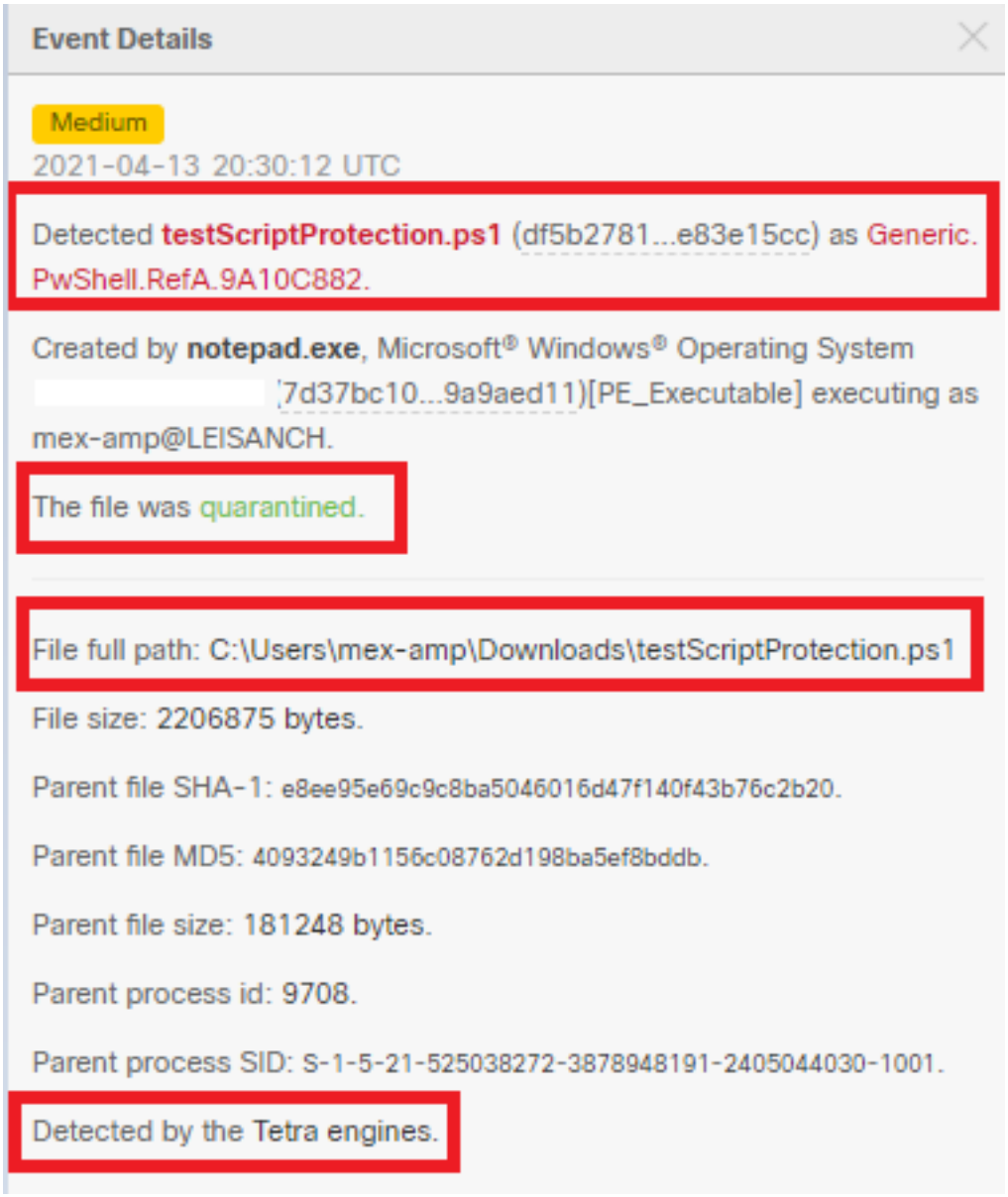
附註：稽核模式會在執行惡意指令碼時建立事件，但不會隔離該指令碼。

疑難排解

當在控制檯中觸發檢測時，指令碼保護沒有特定的事件型別，根據檔案型別及其運行位置來識別誰檢測惡意檔案。

1.根據受支援的指令碼解釋程式，確定副檔名，例如.ps1指令碼。

2.導航到**Device Trajectory > Event Details**，本節顯示與檢測到的檔案相關的更多詳細資訊，例如SHA256、檔案所在的路徑、威脅名稱、AMP聯結器執行的操作以及檢測到它的引擎。如果未啟用TETRA，則顯示的引擎為SHA引擎，例如，此示例將顯示TETRA，因為啟用TETRA後，它會與「指令碼保護」配合使用以提供額外的保護，如圖所示。



調查檢測

為了確定檢測是否確實是惡意的，您可以使用Device Trajectory來檢視運行指令碼時發生的事件，例如父進程、到遠端主機的連線以及惡意軟體可以下載的未知檔案。

誤報檢測

一旦識別出該檢測，並且您的環境信任並瞭解該指令碼，就可以將其稱為「誤報」。為防止聯結器掃描該指令碼，您可以建立一個排除指令碼，如下圖所示。

附註：確保將排除集新增到應用於受影響聯結器的策略中。

相關資訊

- AMP使用手冊

- 技術支援與文件 - Cisco Systems