针对终端的AMP中的脚本保护故障排除

目录

简介

本文档介绍面向终端的高级恶意软件防护(AMP)中脚本保护引擎的配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 管理员对AMP控制台的访问

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 连接器版本7.2.1或更高版本
- Windows 10版本1709及更高版本或Windows Server 2016版本1709及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

脚本保护引擎能够检测和阻止在终端上执行的脚本，并帮助防御恶意软件常用的基于脚本的攻击。Device Trajectory提供链执行的可视性，因此您可以观察在设备上执行脚本的应用。

引擎允许连接器扫描以下脚本文件类型：

应用	文件扩展名

HTML应用程序	HTA
脚本	BAT、CMD、VB、VBS、JS
加密脚本	JSE、VSE
Windows脚本	WS、WASF、SWC、WSH
PowerShell	PS1、PS1XML、PSC1、PSC2、MSH、MSH1、MSH2、MSHXML、MSH1XML、MSH2
快捷方式	SCF
链路	LNK
设置	INF、INX
注册表	注册
字	DOCX、DOTX、DOCM、DOTM
Excel	XLS、XLSX、XLTX、XLSM、XLTM、XLAM
PowerPoint	PPT、PPTX、POTX、POTM、PPTM、PPAM、PPSM、SLDM

脚本保护与以下脚本解释器配合使用：

- PowerShell（V3及更高版本）
- Windows脚本主机（wscript.exe和cscript.exe）
- JavaScript（非浏览器）
- VBScript
- Office VBA宏

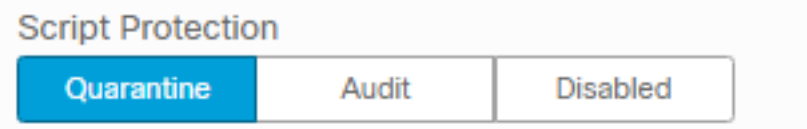
> **警告**：脚本保护不提供可视性，也不提供对非Microsoft脚本解释器（如Python、Perl、PHP或Ruby）的保护。

> **注意**：隔离区判定模式可能会影响用户的应用程序，如Word、Excel和Powerpoint。如果这些应用程序尝试执行恶意VBA脚本，则该应用程序将停止。

脚本保护遵循“**执行时”模**式，它工作于两种不同模式：**主用**和**被动**。在主用模式下，在连接器收到有关脚本是恶意还是超时的信息之前，脚本将被阻止执行。在被动模式下，允许在查找脚本时执行脚本，以确定脚本是否是恶意的。

配置

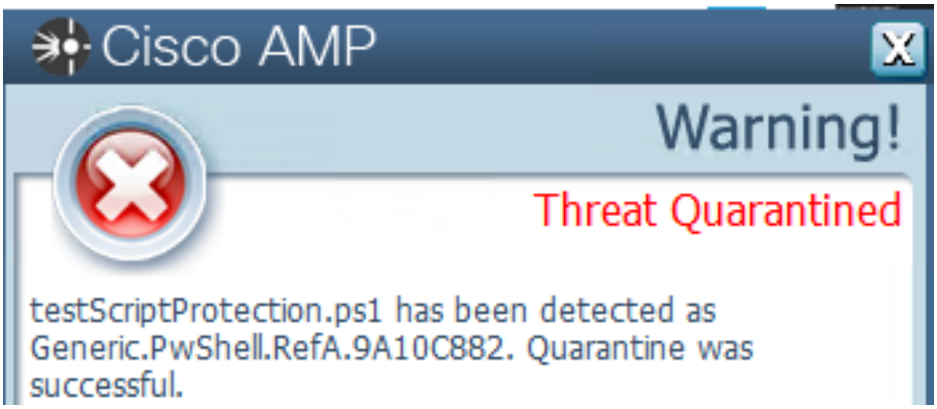
要启用脚本保护，请导航至策略设置，然后在“模式和引擎”下，选择“审核”、“隔离”或“禁用”的“确认”模式，如图所示。



> **注**：脚本保护不依赖于TETRA，但如果启用TETRA，则使用它提供额外保护。

检测

触发检测后，终端上会显示弹出通知，如图所示。



控制台显示Threat Detected事件，如图所示。

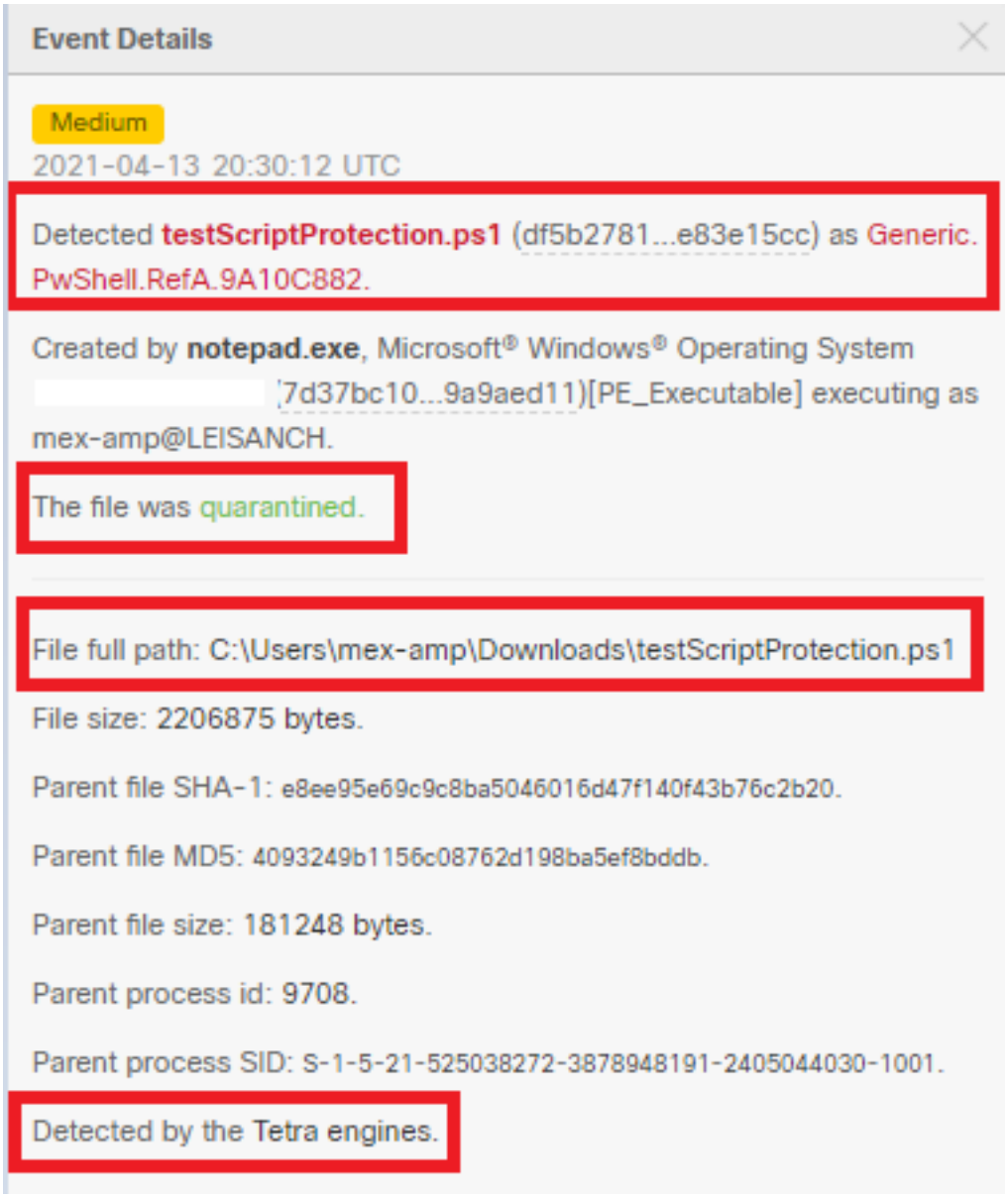
注意：审核模式在恶意脚本执行时创建事件，但是它不会被隔离。

故障排除

在控制台中触发检测时，脚本保护没有特定的事件类型，根据文件类型及其运行位置确定检测恶意文件的人员的方法。

1.相应地，根据支持的脚本解释程序，确定文件扩展名，例如，.ps1脚本。

2.导航至**Device Trajectory > Event Details**，此部分显示与检测到的文件相关的更多详细信息，如SHA256、文件所在的路径、威胁名称、AMP连接器采取的操作以及检测到该文件的引擎。如果未启用TETRA，则显示的引擎为SHA引擎，例如，显示TETRA，因为启用TETRA后，它与脚本保护配合工作以提供其他保护，如图所示。



检查检测

为了确定检测是否确实是恶意的，您可以使用Device Trajectory来查看脚本运行期间发生的事件，例如父进程、与远程主机的连接以及恶意软件可下载的未知文件。

误报检测

一旦检测被识别，并且脚本被您的环境信任和知道，则可将其称为误报。为防止连接器扫描该脚本，可以创建该脚本的排除项，如图所示。

注意：确保将排除集添加到应用于受影响连接器的策略。

相关信息

- AMP用户指南

- 技术支持和文档 - Cisco Systems