Dépannage de la protection de script dans AMP for Endpoints

Contenu

Introduction

Ce document décrit la configuration du moteur Script Protection dans Advanced Malware Protection (AMP) for Endpoints.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès administrateur à la console AMP

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Connecteur version 7.2.1 ou ultérieure
- Windows 10 versions 1709 et ultérieures ou Windows Server 2016 versions 1709 et ultérieures

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le moteur de protection de script permet de détecter et de bloquer les scripts exécutés sur vos terminaux et contribue à la protection contre les attaques basées sur des scripts couramment utilisées par les programmes malveillants. La trajectoire de périphérique fournit une visibilité dans l'exécution de la chaîne, afin que vous puissiez observer les applications qui exécutent les scripts sur vos périphériques.

Le moteur permet au connecteur d'analyser les types de fichiers de script suivants :

Application	Extension de fichier
Application HTML	HTA
Scripts	MTD, CMD, VB, VBS, JS
Script chiffré	JSE, VSE
Script Windows	WS, WASF, SWC, WSH
PowerShell	PS1, PS1XML, PSC1, PSC2, MSH, MSH1, MSH2, MSHXML, MSH1XML, MSH2XML
Raccourci	SCF
Liaison	LNK
Configuration	INF, INX
Registre	REG
Word	DOCX, DOTX, DOCM, DOTM
Excel	XLS, XLSX, XLTX, XLSM, XLTM, XLAM
PowerPoint	PPT, PPTX, POTX, POTM, PPTM, PPAM, PPSM, SLDM

Script Protection fonctionne avec les interpréteurs de script suivants :

- PowerShell (V3 et versions ultérieures)
- Hôte de script Windows (wscript.exe et cscript.exe)
- JavaScript (non navigateur)
- VBScript
- Macros Office VBA

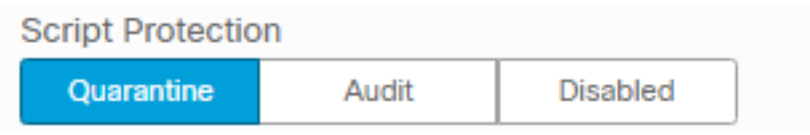
> **Avertissement** : Script Protection ne fournit pas de visibilité ni de protection contre les interpréteurs de script non Microsoft tels que Python, Perl, PHP ou Ruby.

> **Attention** : le mode Quarantine Conviction peut avoir un impact sur les applications utilisateur telles que Word, Excel et Powerpoint. Si ces applications tentent d'exécuter un script VBA malveillant, l'application est arrêtée.

Script Protection honore le **mode On Execute**, il fonctionne sur deux modes différents : **Actif** et **passif**. En mode actif, les scripts ne peuvent pas être exécutés tant que le connecteur ne reçoit pas d'informations indiquant s'il est malveillant ou non ou si un délai d'attente est atteint. En mode passif, les scripts sont autorisés à être exécutés pendant que le script est recherché pour déterminer s'il est malveillant ou non.

Configuration

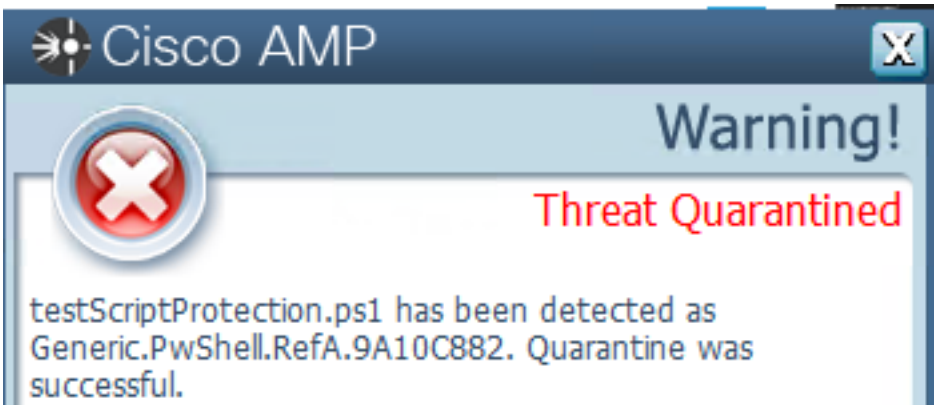
Afin d'activer la protection de script, accédez à vos paramètres de stratégie, puis sous Modes et moteurs, sélectionnez le mode Conviction Audit, Quarantine ou Disabled, comme illustré dans l'image.



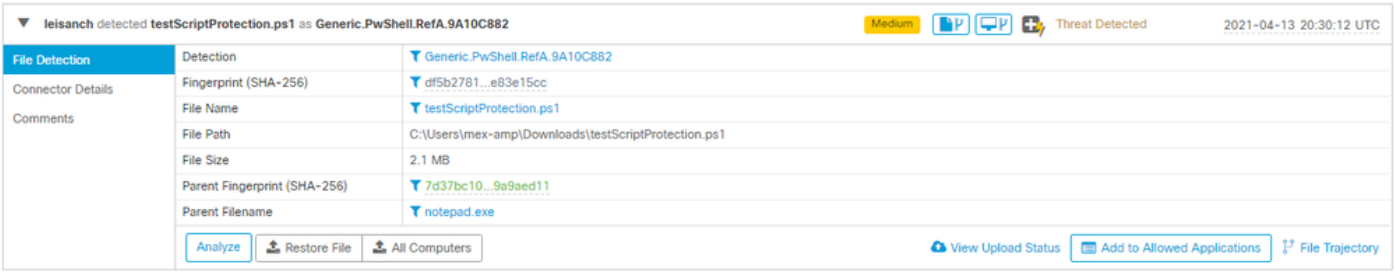
Remarque : la protection de script ne dépend pas de TETRA, mais si TETRA est activé, il l'utilise pour fournir une protection supplémentaire.

Détection

Une fois la détection déclenchée, une notification contextuelle s'affiche sur le point de terminaison, comme le montre l'image.



La console affiche un événement Threat Detected, comme l'illustre l'image.



Note: Le mode d'audit crée un événement lorsqu'un script malveillant est exécuté, mais il n'est pas mis en quarantaine.

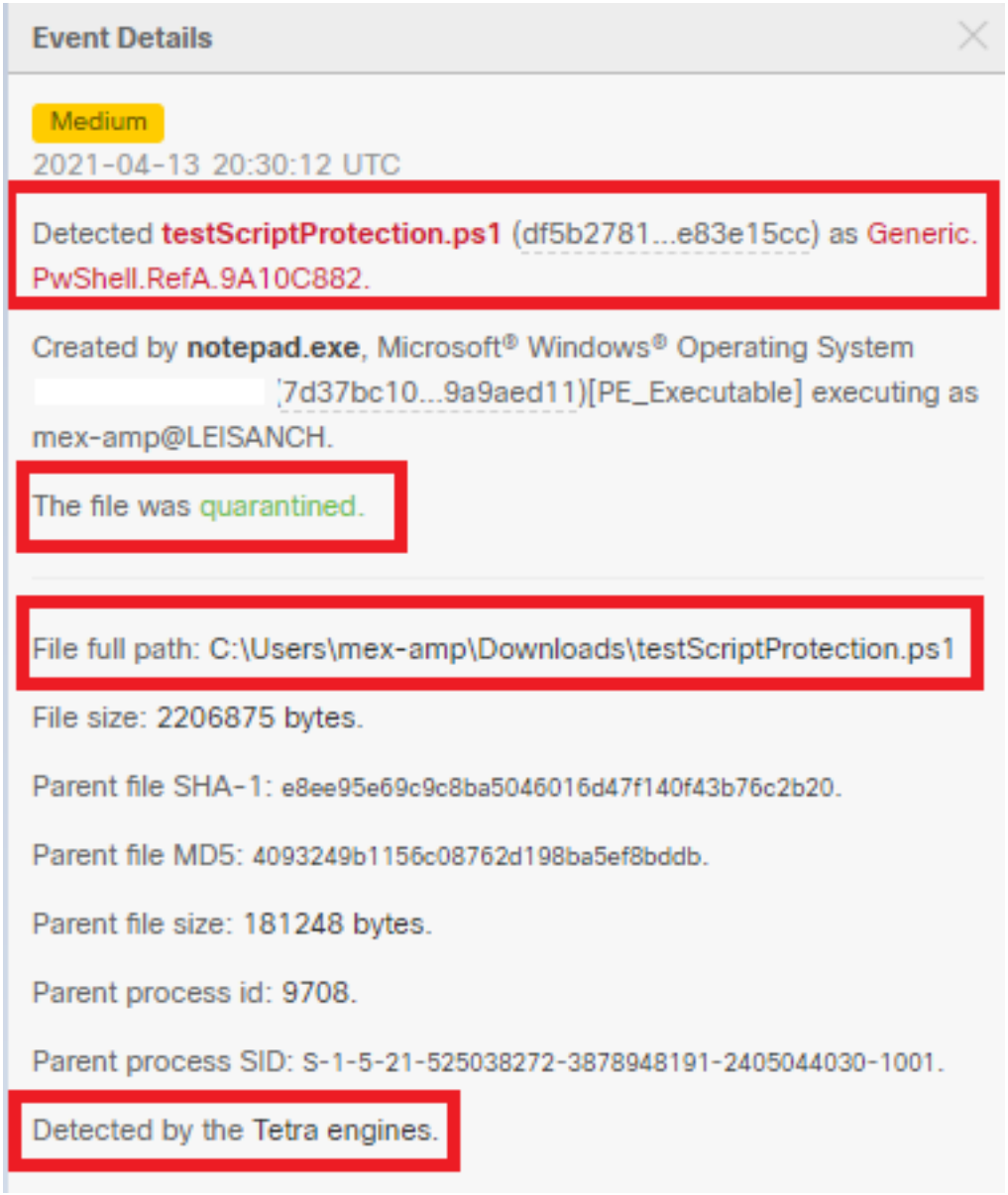
Dépannage

Script Protection ne dispose pas d'un type d'événement spécifique lorsque la détection est déclenchée dans la console, un moyen d'identifier qui détecte le fichier malveillant est basé sur le type de fichier et l'endroit où il s'exécute.

1. En conséquence, pour les interpréteurs de script pris en charge, identifiez l'extension de fichier, pour cet exemple, il s'agit d'un script .ps1.

2. Accédez à **Device Trajectory > Event Details**, dans cette section, plus de détails relatifs au fichier détecté sont affichés, tels que SHA256, un chemin d'accès au fichier, le nom de la menace,

l'action effectuée par le connecteur AMP et le moteur qui le détecte. Dans le cas où TETRA n'est pas activé, le moteur affiché est le moteur SHA, par exemple, TETRA est affiché car lorsque TETRA est activé, il fonctionne avec Script Protection pour fournir une protection supplémentaire, comme illustré dans l'image.

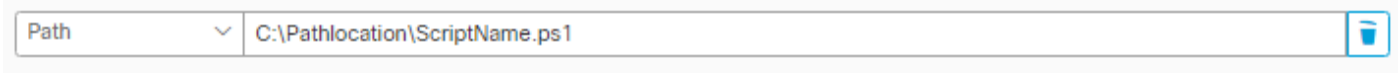


Étudier la détection

Afin de déterminer si la détection est effectivement malveillante ou non, vous pouvez utiliser Device Trajectory pour vous fournir une visibilité sur les événements qui se sont produits pendant l'exécution du script, tels que les processus parents, les connexions aux hôtes distants et les fichiers inconnus qui peuvent être téléchargés par un programme malveillant.

Détection de faux positifs

Une fois la détection identifiée et si le script est approuvé et connu par votre environnement, il peut être appelé False Positive. Afin d'empêcher le connecteur de l'analyser, vous pouvez créer une exclusion de ce script, comme indiqué dans l'image.



Note: Assurez-vous que le jeu d'exclusions est ajouté à la stratégie appliquée au connecteur affecté.

Informations connexes

- Guide de l'utilisateur AMP
- Support et documentation techniques - Cisco Systems