Fehlerbehebung beim Skriptschutz in AMP für Endgeräte

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration der Script Protection Engine in Advanced Malware Protection (AMP) für Endgeräte.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Administratorzugriff auf die AMP-Konsole

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Connector ab Version 7.2.1
- Windows 10, Version 1709 oder höher, oder Windows Server 2016, Version 1709 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die Script Protection Engine bietet die Möglichkeit, Skripts zu erkennen und zu blockieren, die auf Ihren Endpunkten ausgeführt werden. Sie schützt vor skriptbasierten Angriffen, die häufig von Malware verwendet werden. Device Trajectory bietet Transparenz in der Kettenausführung, sodass Sie die Anwendungen beobachten können, die die Skripte auf Ihren Geräten ausführen.

Die Engine ermöglicht es dem Connector, die folgenden Skriptdateitypen zu durchsuchen:

Anwendung	Dateierweiterung
HTML-Anwendung	HTA
Skripte	BAT, CMD, VB, VBS, JS
Verschlüsseltes Skript	JSE, VSE
Windows-Skript	WS, WASF, SWC, WSH
PowerShell	PS1, PS1XML, PSC1, PSC2, MSH, MSH1, MSH2, MSHXML, MSH1XML, MSH2X
Tastenkombination	SCF
Link	LNK
Einrichtung	INF, INX
Registrierung	REG
Word	DOCX, DOTX, DOCM, DOTM
Excel	XLS, XLSX, XLTX, XLSM, XLTM, XLAM
PowerPoint	PPT, PPTX, POTX, POTM, PPTM, PPAM, PPSM, SLDM

Script Protection funktioniert mit den folgenden Skriptinterpretern:

- PowerShell (V3 und höher)
- Windows Script Host (wscript.exe und cscript.exe)
- JavaScript (kein Browser)
- VBScript
- Office-VBA-Makros

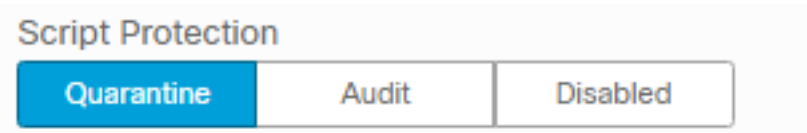
Warnung: Script Protection bietet weder Transparenz noch Schutz vor Skript-Interpretern wie Python, Perl, PHP oder Ruby, die nicht Microsoft-Skripte verwenden.

Vorsicht: Der Quarantäne-Modus hat das Potenzial, Benutzeranwendungen wie Word, Excel und Powerpoint zu beeinflussen. Wenn diese Anwendungen versuchen, ein bösartiges VBA-Skript auszuführen, wird die Anwendung beendet.

Der Skriptschutz ehrt den **On Execute Mode**, er funktioniert in zwei verschiedenen Modi: **Aktiv** und **Passiv**. Im aktiven Modus werden Skripts so lange nicht ausgeführt, bis der Connector Informationen darüber erhält, ob sie schädlich sind oder ein Timeout erreicht wird. Im passiven Modus können Skripts ausgeführt werden, während das Skript gesucht wird, um festzustellen, ob es schädlich ist.

Konfiguration

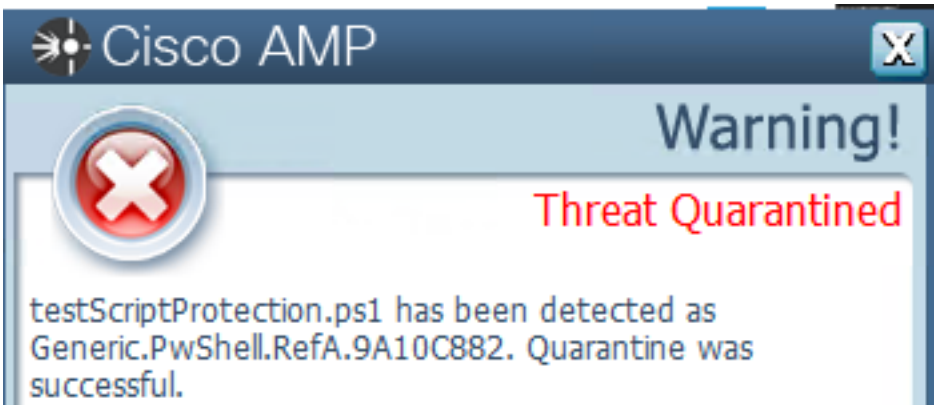
Um den Skriptschutz zu aktivieren, navigieren Sie zu den Richtlinieneinstellungen. Wählen Sie dann unter Modi und Engines (Modi und Engines) den Modus Conviction (Konfiguration) zu Audit, Quarantine (Überwachung) oder Disabled (Deaktiviert) aus, wie im Bild gezeigt.



Hinweis: Der Skriptschutz ist nicht von TETRA abhängig. Wenn TETRA jedoch aktiviert ist, bietet er zusätzlichen Schutz.

Erkennung

Sobald die Erkennung ausgelöst wird, wird eine Popup-Benachrichtigung auf dem Endpunkt angezeigt, wie im Bild gezeigt.



Die Konsole zeigt ein Ereignis mit der Bedrohungserkennung an, wie im Bild gezeigt.

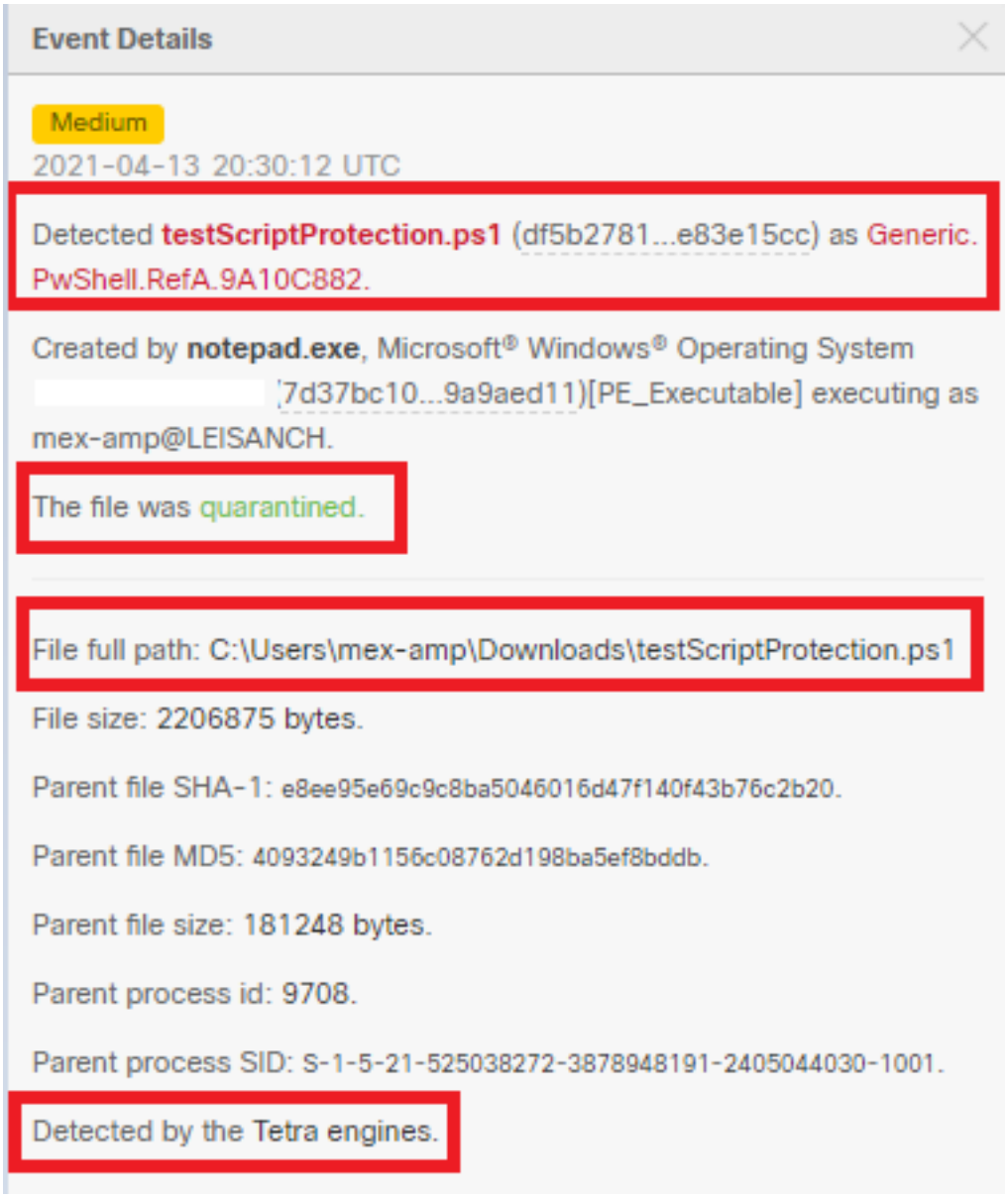
Hinweis: Der Überwachungsmodus erstellt ein Ereignis, wenn ein bösartiges Skript ausgeführt wird, jedoch nicht unter Quarantäne gestellt wird.

Fehlerbehebung

Der Skriptschutz verfügt über keinen bestimmten Ereignistyp, wenn die Erkennung in der Konsole ausgelöst wird. Die Möglichkeit, die Erkennung schädlicher Dateien zu bestimmen, hängt vom Dateityp und von dem Ort ab, an dem sie ausgeführt werden.

1. Entsprechend den unterstützten Skript-Interpretern identifizieren Sie die Dateierweiterung, in diesem Beispiel ist es ein .ps1-Skript.

2. Navigieren Sie zu **Device Trajectory > Event Details**. In diesem Abschnitt werden weitere Details zu der erkannten Datei angezeigt, z. B. SHA256, ein Pfad, in dem sich die Datei befindet, der Name der Bedrohung, die vom AMP-Connector durchgeführte Aktion und das Modul, das sie erkennt. Falls TETRA nicht aktiviert ist, wird das angezeigte Modul SHA-Engine, in diesem Beispiel, TETRA angezeigt, da es bei Aktivierung von TETRA mit Script Protection arbeitet, um zusätzlichen Schutz zu bieten, wie im Bild gezeigt.

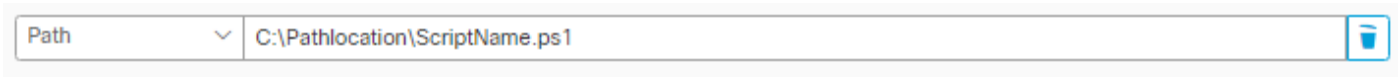


Untersuchung der Erkennung

Um festzustellen, ob die Erkennung tatsächlich schädlich ist oder nicht, können Sie Device Trajectory verwenden, um Ihnen einen Überblick über die Ereignisse zu geben, die während der Ausführung des Skripts aufgetreten sind, z. B. übergeordnete Prozesse, Verbindungen zu Remotehosts und unbekannte Dateien, die von Malware heruntergeladen werden können.

Fehlalarme Erkennung

Sobald die Erkennung identifiziert wurde und das Skript vertrauenswürdig ist und von Ihrer Umgebung bekannt ist, kann es als False Positive bezeichnet werden. Um zu verhindern, dass der Anschluss scannt, können Sie einen Ausschluss dieses Skripts erstellen, wie im Bild gezeigt.



> **Hinweis:** Stellen Sie sicher, dass die Ausschlussgruppe der Richtlinie hinzugefügt wird, die auf den betroffenen Anschluss angewendet wird.

Zugehörige Informationen

- AMP-Benutzerhandbuch
- Technischer Support und Dokumentation für Cisco Systeme