Solución de problemas de protección de scripts en AMP para terminales

Contenido

Introducción

Este documento describe la configuración del motor de protección de secuencias de comandos en protección frente a malware avanzado (AMP) para terminales.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso de administrador a la consola AMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Conector versión 7.2.1 o posterior
- Windows 10 versión 1709 y posteriores o Windows Server 2016 versión 1709 y posteriores

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El motor de protección de secuencias de comandos proporciona la capacidad de detectar y

bloquear secuencias de comandos ejecutadas en los terminales y ayuda a proteger frente a los ataques basados en secuencias de comandos que suele utilizar el malware. La trayectoria de dispositivos proporciona visibilidad en la ejecución de la cadena, de modo que puede observar las aplicaciones que ejecutan las secuencias de comandos en sus dispositivos.

El motor permite que el conector analice los siguientes tipos de archivo de script:

Aplicación	Extensión de Archivo
Aplicación HTML	HTA
Guiones	BAT, CMD, VB, VBS, JS
Guión cifrado	JSE, VSE
Windows Script	WS, WASF, SWC, WSH
PowerShell	PS1, PS1XML, PSC1, PSC2, MSH, MSH1, MSH2, MSHXML, MSH1XML, MSH2XML
Acceso directo	SCF
Enlace	LNK
Configuración	INF, INX
Registro	REG
Palabra	DOCX, DOTX, DOCM, DOTM
Excel	XLS, XLSX, XLTX, XLSM, XLTM, XLAM
PowerPoint	PPT, PPTX, POTX, POTM, PPTM, PPAM, PPSM, SLDM

La protección de secuencias de comandos funciona con los siguientes intérpretes de secuencias de comandos:

- PowerShell (V3 y posteriores)
- Windows Script Host (wscript.exe y cscript.exe)
- JavaScript (sin explorador)
- VBScript
- macros VBA de Office

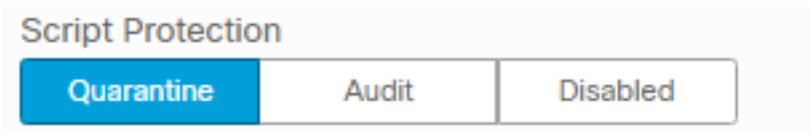
Advertencia: la protección de secuencias de comandos no proporciona visibilidad ni protección de intérpretes de secuencias de comandos que no sean de Microsoft, como Python, Perl, PHP o Ruby.

Precaución: el modo de condena de cuarentena puede afectar a las aplicaciones del usuario como Word, Excel y PowerPoint. Si estas aplicaciones intentan ejecutar un script de VBA malicioso, la aplicación se detiene.

Script Protection honra el **On Execute Mode**, funciona en dos modos diferentes: **Activo** y **Pasivo**. En el modo Activo, los scripts se bloquean para que no se ejecuten hasta que el conector reciba información sobre si son maliciosos o si se alcanza un tiempo de espera. En el modo pasivo, se permite ejecutar secuencias de comandos mientras se busca el script para determinar si son o no maliciosas.

Configuración

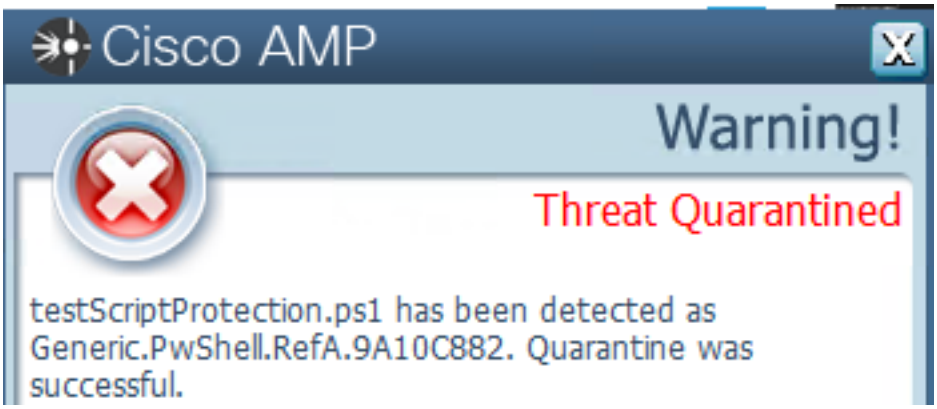
Para habilitar la protección de secuencias de comandos, desplácese a la configuración de la directiva y, a continuación, en Modos y motores, seleccione el modo Conviction en Audit, Quarantine o Disabled, como se muestra en la imagen.



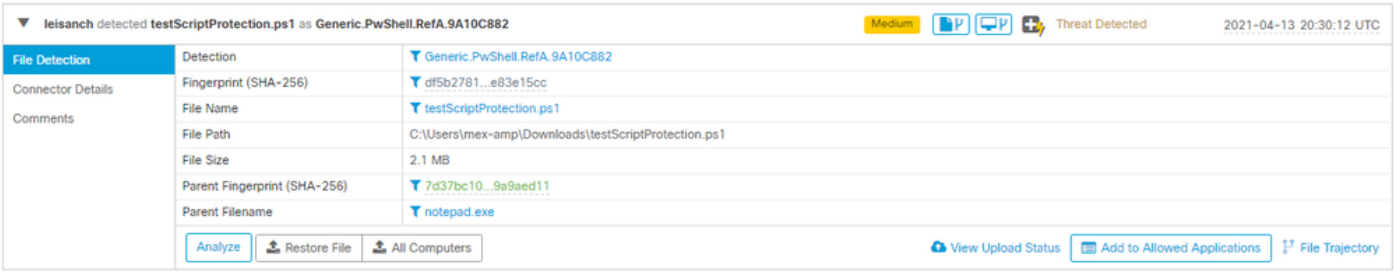
Nota: La protección de secuencias de comandos no depende de TETRA, pero si TETRA está habilitado, la utiliza para proporcionar protección adicional.

Detección

Una vez que se activa la detección, se muestra una notificación emergente en el terminal, como se muestra en la imagen.



La consola muestra un evento Threat Detected, como se muestra en la imagen.



Nota: El modo de auditoría crea un evento cuando se ejecuta una secuencia de comandos malintencionada; sin embargo, no se pone en cuarentena.

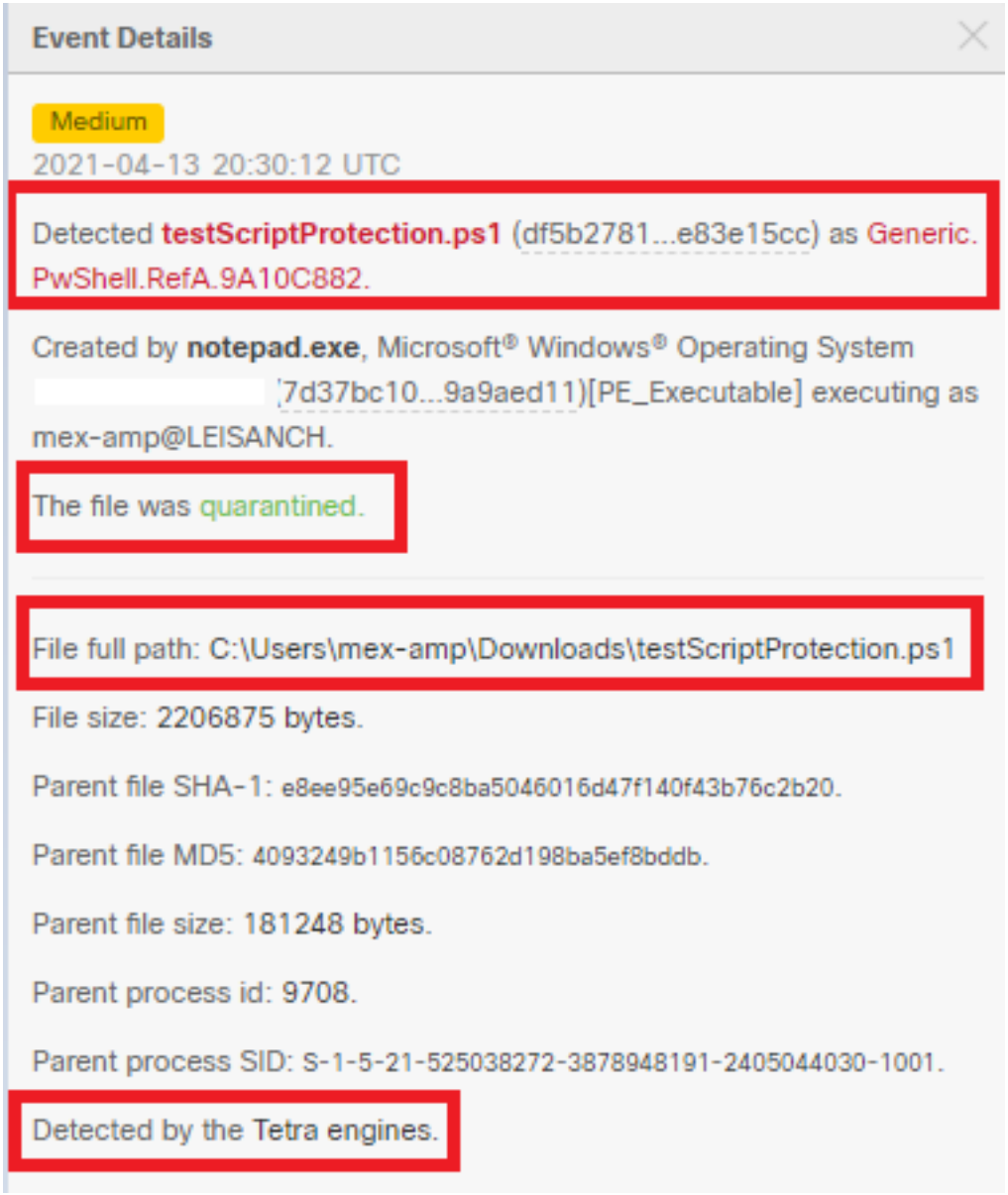
Troubleshoot

La protección de secuencias de comandos no tiene un tipo de evento específico cuando se activa la detección en la consola, una forma de identificar quién detecta el archivo malicioso se basa en el tipo de archivo y dónde se ejecuta.

1. De acuerdo con los intérpretes de secuencias de comandos soportados, identifique la extensión del archivo; para este ejemplo, es un script .ps1.

2. Vaya a **Device Trajectory > Event Details**, en esta sección se muestran más detalles relacionados con el archivo detectado, como SHA256, una ruta de acceso en la que se localizó el

archivo, el nombre de la amenaza, las acciones realizadas por el conector AMP y el motor que lo detecta. En caso de que TETRA no esté habilitado, el motor mostrado es el motor SHA, por ejemplo, TETRA se muestra ya que cuando TETRA está habilitado, funciona con Protección de Secuencia de Comandos para proporcionar protección adicional, como se muestra en la imagen.

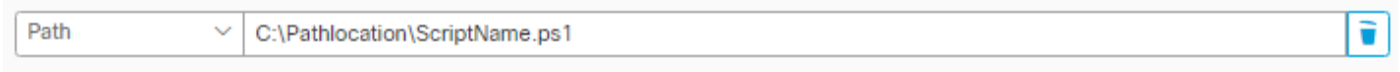


Investigar la detección

Para determinar si la detección es realmente maliciosa o no, puede utilizar la trayectoria del dispositivo para proporcionarle visibilidad de los eventos que ocurrieron mientras el script se ejecutaba, como procesos principales, conexiones a hosts remotos y archivos desconocidos que pueden ser descargados por el malware.

Detección de falsos positivos

Una vez que se identifica la detección y si el entorno confía y conoce el script, se le puede llamar falso positivo. Para evitar que el conector lo escanee, puede crear una exclusión de ese script, como se muestra en la imagen.



Nota: Asegúrese de que el conjunto de exclusión se agrega a la política aplicada al conector afectado.

Información Relacionada

- Guía del usuario de AMP
- Soporte Técnico y Documentación - Cisco Systems