Risoluzione dei problemi relativi a Protezione script in AMP for Endpoints

Sommario

Introduzione

In questo documento viene descritta la configurazione del motore di protezione dello script in Advanced Malware Protection (AMP) for Endpoints.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso amministrativo alla console AMP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Connector versione 7.2.1 o successiva
- Windows 10 versione 1709 e successive o Windows Server 2016 versione 1709 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il motore di protezione degli script consente di rilevare e bloccare gli script eseguiti sugli endpoint e di proteggersi dagli attacchi basati su script comunemente utilizzati dal malware. La traiettoria dei dispositivi fornisce visibilità nell'esecuzione della catena, in modo da poter osservare le applicazioni che eseguono gli script sui dispositivi.

Il motore consente al connettore di analizzare i seguenti tipi di file script:

Applicazione	Estensione file
Applicazione HTML	HTA
Script	BAT, CMD, VB, VBS, JS
Script crittografato	JSE, VSE,
Script di Windows	WS, WASF, SWC, WSH
PowerShell	PS1, PS1XML, PSC1, PSC2, MSH, MSH1, MSH2, MSHXML, MSH1XML, MSH2XML
Collegamento	SCF
Collegamento	LINK
Configurazione	INF, INX
Registro	REG
Word	DOCX, DOTX, DOCM, DOTM
Excel	XLS, XLSX, XLTX, XLSM, XLTM, XLAM
PowerPoint	PPT, PPTX, POTX, POTM, PPTM, PPAM, PSM, SLDM

Script Protection funziona con i seguenti interpreti script:

- PowerShell (V3 e versioni successive)
- Windows Script Host (wscript.exe e cscript.exe)
- JavaScript (non browser)
- VBScript
- Macro VBA di Office

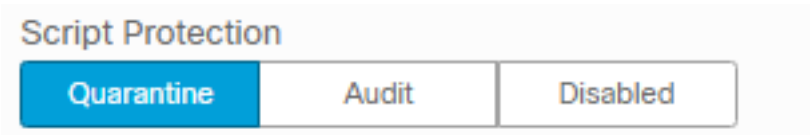
> **Avviso**: la protezione degli script non fornisce visibilità né protezione da interpreti di script non Microsoft, ad esempio Python, Perl, PHP o Ruby.

> **Attenzione**: la modalità di condanna della quarantena può influire sulle applicazioni dell'utente quali Word, Excel e Powerpoint. Se queste applicazioni tentano di eseguire uno script VBA dannoso, l'applicazione viene arrestata.

Script Protection rispetta la **modalità On Execute**, funziona in due diverse modalità: **Attivo** e **passivo**. In modalità attiva, l'esecuzione degli script viene bloccata finché il connettore non riceve informazioni che indicano se è dannoso o se è stato raggiunto un timeout. In modalità passiva, gli script possono essere eseguiti mentre lo script viene cercato per determinare se è dannoso o meno.

Configurazione

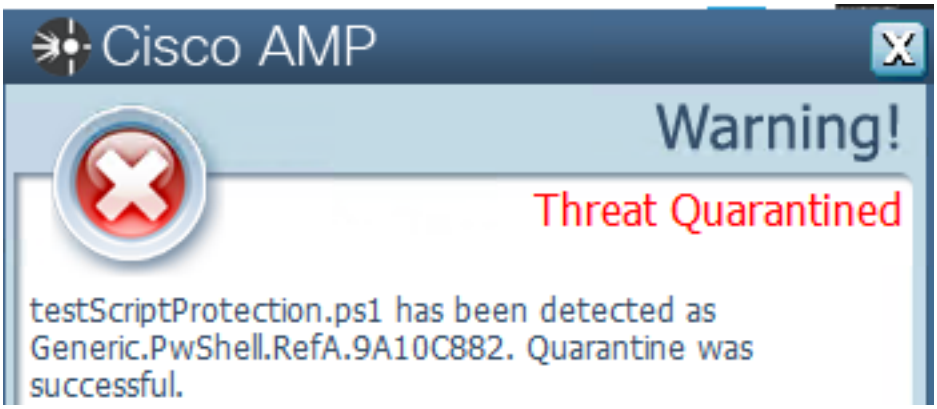
Per abilitare la protezione tramite script, passare alle impostazioni dei criteri, quindi in Modalità e moduli di gestione selezionare la modalità di sospensione da Audit, Quarantena o Disabilitato, come mostrato nell'immagine.



Nota: la protezione degli script non dipende da TETRA, ma se TETRA è abilitato la usa per fornire protezione aggiuntiva.

Rilevamento

Una volta attivato il rilevamento, sull'endpoint viene visualizzata una notifica popup, come mostrato nell'immagine.



La console visualizza un evento di rilevamento minacce, come mostrato nell'immagine.

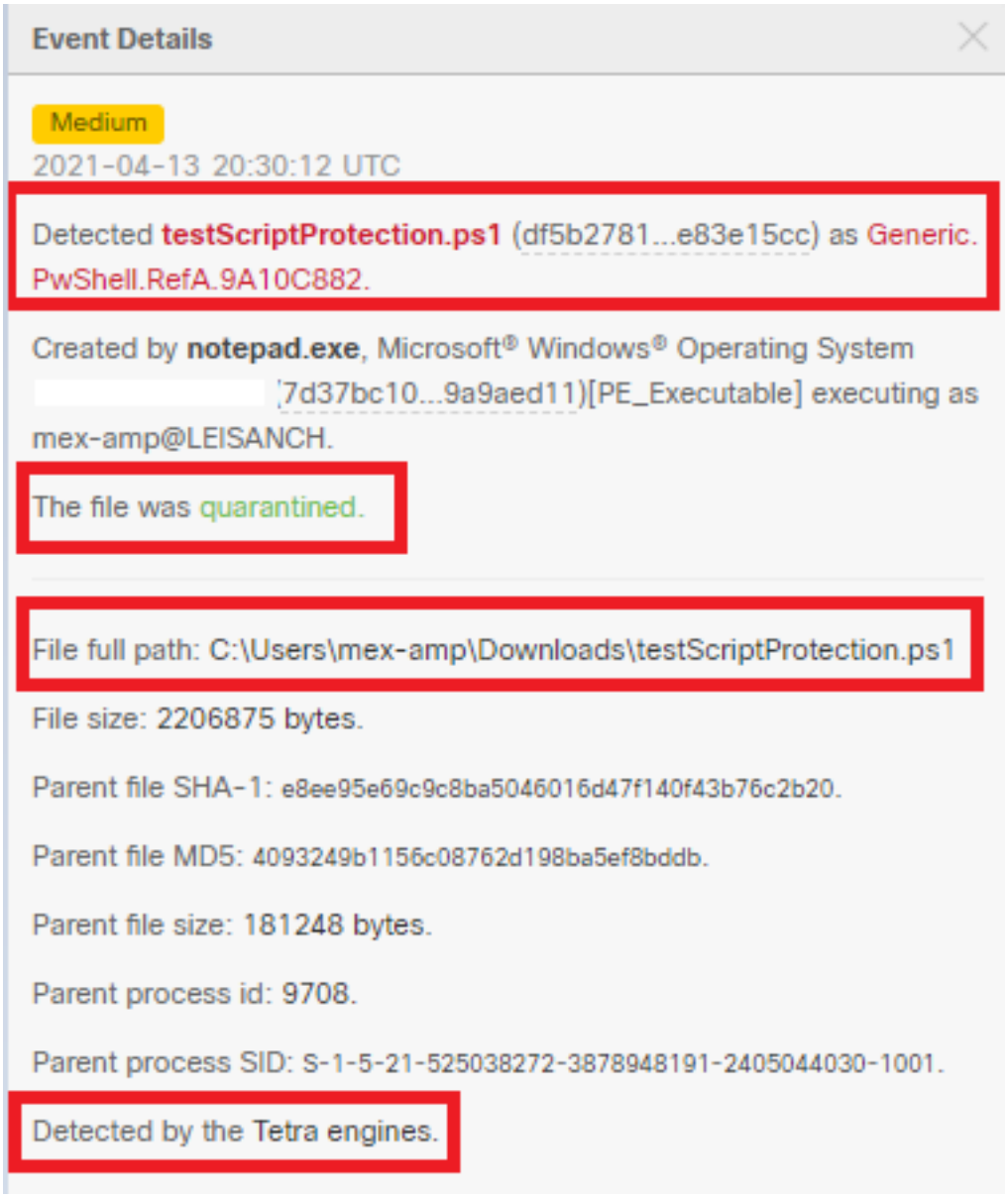
Nota: La modalità di controllo crea un evento quando viene eseguito uno script dannoso, che tuttavia non viene messo in quarantena.

Risoluzione dei problemi

Quando nella console viene attivato il rilevamento, la protezione script non dispone di un tipo di evento specifico. Un modo per identificare chi rileva il file dannoso è basato sul tipo di file e sulla posizione in cui viene eseguito.

1. In base agli interpreti di script supportati, identificare l'estensione del file, ad esempio uno script .ps1.

2. Passare a **Traiettoria dispositivo > Dettagli evento**. In questa sezione vengono visualizzati ulteriori dettagli relativi al file rilevato, ad esempio SHA256, il percorso in cui si trova il file, il nome della minaccia, l'azione eseguita dal connettore AMP e il motore che lo rileva. Se TETRA non è abilitato, il motore visualizzato è il motore SHA. Per questo esempio, viene visualizzato TETRA perché quando TETRA è abilitato, funziona con Script Protection per fornire una protezione aggiuntiva, come mostrato nell'immagine.

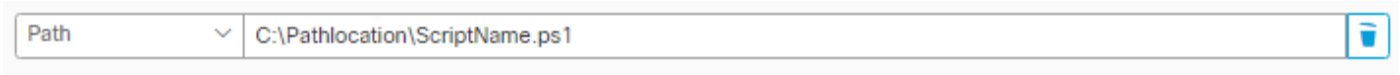


Analizza rilevamento

Per determinare se il rilevamento è dannoso o meno, è possibile utilizzare Traiettoria dispositivi per fornire visibilità sugli eventi che si sono verificati durante l'esecuzione dello script, ad esempio i processi padre, le connessioni agli host remoti e i file sconosciuti che possono essere scaricati dal malware.

Rilevamento falsi positivi

Una volta identificato il rilevamento e se lo script è attendibile e conosciuto dall'ambiente, può essere definito falso positivo. Per evitare che il connettore esegua la scansione, è possibile creare un'esclusione dello script, come mostrato nell'immagine.



Nota: Verificare che il set di esclusione sia aggiunto al criterio applicato al connettore interessato.

Informazioni correlate

- Guida per l'utente di AMP
- Documentazione e supporto tecnico – Cisco Systems