Bescherming van probleemoplossing in Advanced Malware Protection voor endpoints

Inhoud

Inleiding

Dit document beschrijft de configuratie van de Script Protection Engine in Advanced Malware Protection (AMP) voor endpoints.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Admin-toegang tot AMP-console

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Aansluitversie 7.2.1 of hoger
- Windows 1709 en hoger of Windows Server 2016, versie 1709 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

De Script Protection Engine biedt de mogelijkheid om scripts op uw endpoints te detecteren en te

blokkeren en helpt te beschermen tegen script-gebaseerde aanvallen die door malware worden gebruikt. Apparaattraject biedt zichtbaarheid in de kettinguitvoering, zodat u de toepassingen kunt observeren die de scripts op uw apparaten uitvoeren.

De motor laat de connector de volgende script bestandstypen scannen:

Toepassing	Bestandsuitbreiding
HTML-toepassing	HAT
Schriften	BBT, CMD, VB, VBS, JS
Versleuteld scripts	JSE, VSE
Windows Script	WS, WASF, SWC, WSH
PowerShell	PS1, PS1XML, PSC1, PSC2, MSH, MSH1, MSH2, MSHXML, MSH1XML, MSH2XML
Snelheid	SCF
Koppelen	LNK
Instellen	INF, INX
griffie	REG
Word	DOCX, DOTX, DOCM, DOTM
Excel	XLS, XLSX, XLTX, XLSM, XLTM, XLAM
PowerPoint	PPT, PPTX, POTX, POTM, PPTM, PPAM, PPSM, SLDM

Script Protection werkt met de volgende script tolken:

- PowerShell (V3 en hoger)
- Windows Script Host (wscript.exe en cscript.exe)
- JavaScript (niet-browser)
- VBScript
- Office VBA macros

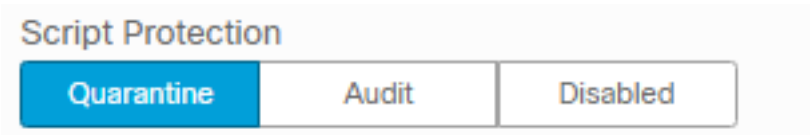
Waarschuwing: Script Protection biedt geen zichtbaarheid of bescherming tegen niet-Microsoft script interpreters zoals Python, Perl, PHP of Ruby.

Waarschuwing: de Quarantine Conviction-modus kan invloed hebben op de toepassingen van de gebruiker, zoals Word, Excel en PowerPoint. Als deze toepassingen proberen een kwaadaardig VBA-script uit te voeren, wordt de toepassing gestopt.

De **On Execute Mode**-bescherming van scripts werkt op twee verschillende modi: **Actief** en **passief**. In Active Mode worden scripts geblokkeerd van het uitvoeren totdat de connector informatie ontvangt over of het al dan niet kwaadaardig is of wanneer een timeout wordt bereikt. In Passive mode mogen scripts worden uitgevoerd terwijl het script wordt opgezocht om te bepalen of het al dan niet kwaadaardig is.

Configuratie

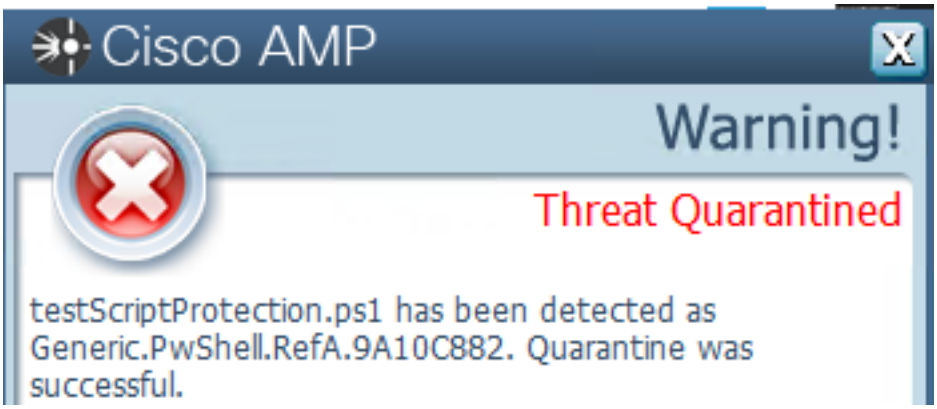
Om Script Protection in te schakelen, navigeer naar uw beleidsinstellingen en selecteer vervolgens onder Modus en Motoren de conversiemodus naar Auditing, quarantaine of Uitgeschakeld, zoals in de afbeelding wordt weergegeven.



Opmerking: de bescherming van scripts is niet afhankelijk van TETRA, maar als TETRA is ingeschakeld, gebruikt het deze om extra bescherming te bieden.

Detectie

Zodra de detectie is geactiveerd, wordt een pop-upbericht weergegeven op het eindpunt, zoals in het beeld wordt weergegeven.



De console toont een gebeurtenis die werd herkend, zoals in de afbeelding.

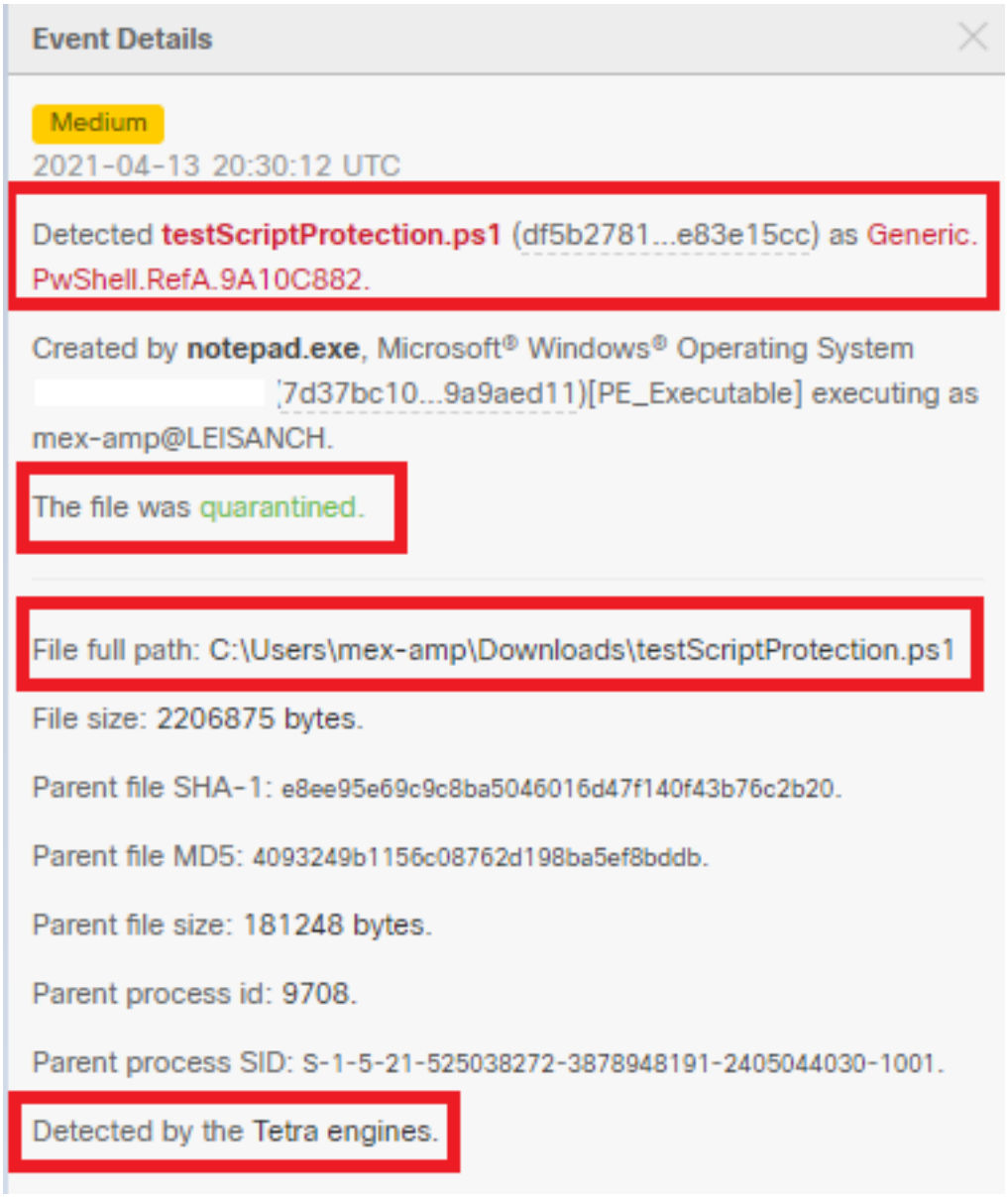
Opmerking: De wijze van de controle creëert een gebeurtenis wanneer een kwaadaardig script wordt uitgevoerd, echter, het is niet in quarantaine geplaatst.

Problemen oplossen

Script Protection heeft geen specifiek Event Type wanneer detectie wordt geactiveerd in de console, is een manier om te identificeren wie het kwaadwillige bestand detecteert gebaseerd op het bestandstype en waar het draait.

1. Dienovereenkomstig aan de ondersteunde script tolken, identificeer de file extensie, bijvoorbeeld is dit voorbeeld een .ps1 script.

2. Navigeer naar **Apparaattraject > Event Details**, in deze sectie worden meer details met betrekking tot het gedetecteerde bestand weergegeven, zoals SHA256, een pad waar het bestand zich bevond, bedreigingsnaam, actie ondernomen door de AMP-connector, en de motor die het detecteert. Indien TETRA niet is ingeschakeld, is de weergegeven motor een SHA-motor. In dit voorbeeld wordt TETRA weergegeven omdat, wanneer TETRA is ingeschakeld, de machine met Script Protection werkt om extra bescherming te bieden, zoals in het beeld wordt getoond.

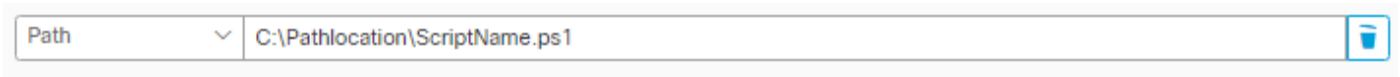


De detectie onderzoeken

Om te bepalen of de detectie inderdaad kwaadaardig is of niet, kunt u de Transjectory van het Apparaat gebruiken om u zicht te verschaffen in de gebeurtenissen die plaatsvonden terwijl het script uitgevoerd werd zoals ouderprocessen, verbindingen naar verafgelegen hosts en onbekende bestanden die door malware kunnen worden gedownload.

Ongeldige positieve detectie

Zodra de detectie is geïdentificeerd en als het script vertrouwd en bekend is door uw omgeving, kan het een False Positive worden genoemd. Om te voorkomen dat de connector het scant, kunt u een uitsluiting van dat script creëren, zoals in de afbeelding wordt weergegeven.



Opmerking: Zorg ervoor dat de uitsluitingsset is toegevoegd aan het beleid dat op de betreffende connector is toegepast.

Gerelateerde informatie

- AMP-gebruikershandleiding
- Technische ondersteuning en documentatie – Cisco Systems