AMP for Endpoints에서 스크립트 보호 문제 해결

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[구성](#)
[탐지](#)
[문제 해결](#)
[탐지 조사](#)
[오탐 탐지](#)
[관련 정보](#)

소개

이 문서에서는 AMP(Advanced Malware Protection) for Endpoints의 스크립트 보호 엔진 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AMP 콘솔에 대한 관리자 액세스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 커넥터 버전 7.2.1 이상
- Windows 10 버전 1709 이상 또는 Windows Server 2016 버전 1709 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

Script Protection 엔진은 엔드포인트에서 실행되는 스크립트를 탐지 및 차단할 수 있는 기능을 제공하며 악성코드가 일반적으로 사용하는 스크립트 기반 공격으로부터 보호합니다.Device Trajectory는 체인 실행에 대한 가시성을 제공하므로 디바이스에서 스크립트를 실행하는 애플리케이션을 관찰할 수 있습니다.

Engine에서는 커넥터가 다음 스크립트 파일 유형을 스캔할 수 있습니다.

애플리케이션	파일 확장명
HTML 응용 프로그램	HTA
스크립트	BAT, CMD, VB, VBS, JS
암호화된 스크립트	JSE, VSE
Windows 스크립트	WS, WASF, SWC, WSH
PowerShell	PS1, PS1XML, PSC1, PSC2, MSH, MSH1, MSH2, MSHXML, MSH1XML, MSH2XM
바로 가기	SCF
링크	LNK
설정	INF, INX
레지스트리	등록
단어	DOCX, DOTX, DOCM, DOTM
Excel	XLS, XLSX, XLTX, XLSM, XLTM, XLAM
PowerPoint	PPT, PPTX, POTX, POTM, PPTM, PPAM, PPSM, SLDM

스크립트 보호는 다음 스크립트 통역과 함께 작동합니다.

- PowerShell(V3 이상)
- Windows 스크립트 호스트(wscript.exe 및 cscript.exe)
- JavaScript(브라우저가 아님)
- VBScript
- Office VBA 매크로

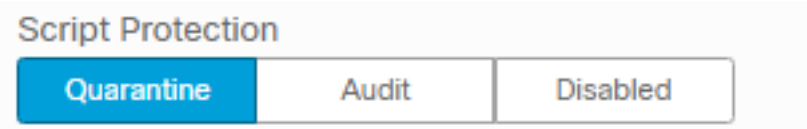
경고: 스크립트 보호는 Python, Perl, PHP 또는 Ruby와 같은 Microsoft 이외의 스크립트 통역사를 가시성 또는 보호하지 않습니다.

주의: Quarantine Conviction 모드에서는 Word, Excel, Powerpoint와 같은 사용자 애플리케이션에 영향을 미칠 수 있습니다.이러한 응용 프로그램이 악성 VBA 스크립트를 실행하려고 하면 응용 프로그램이 중지됩니다.

스크립트 보호는 실행 **모드**를 **준수하며** 두 가지 모드에서 작동합니다.**활성** 및 **수동**.액티브 모드에서는 커넥터가 악의적인지 시간 초과에 도달하는지에 대한 정보를 받을 때까지 스크립트가 실행되지 않습니다.패시브 모드에서는 스크립트가 악성인지 여부를 확인하기 위해 조회되는 동안 스크립트를 실행할 수 있습니다.

구성

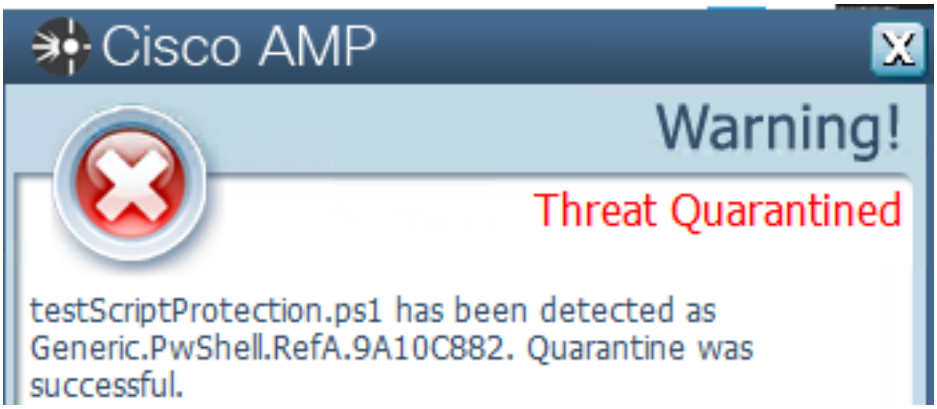
스크립트 보호를 활성화하려면 정책 설정으로 이동한 다음 Modes and Engines(모드 및 엔진)에서 이미지에 표시된 대로 Conviction(확정) 모드를 Audit(감사), Quarantine(격리) 또는 Disabled(비활성화됨)로 선택합니다.



참고: 스크립트 보호는 TETRA에 종속되지 않지만 TETRA가 활성화된 경우 이를 사용하여 추가 보호를 제공합니다.

탐지

탐지가 트리거되면 이미지에 표시된 대로 엔드포인트에 팝업 알림이 표시됩니다.



콘솔에 이미지에 표시된 대로 Threat Detected 이벤트가 표시됩니다.

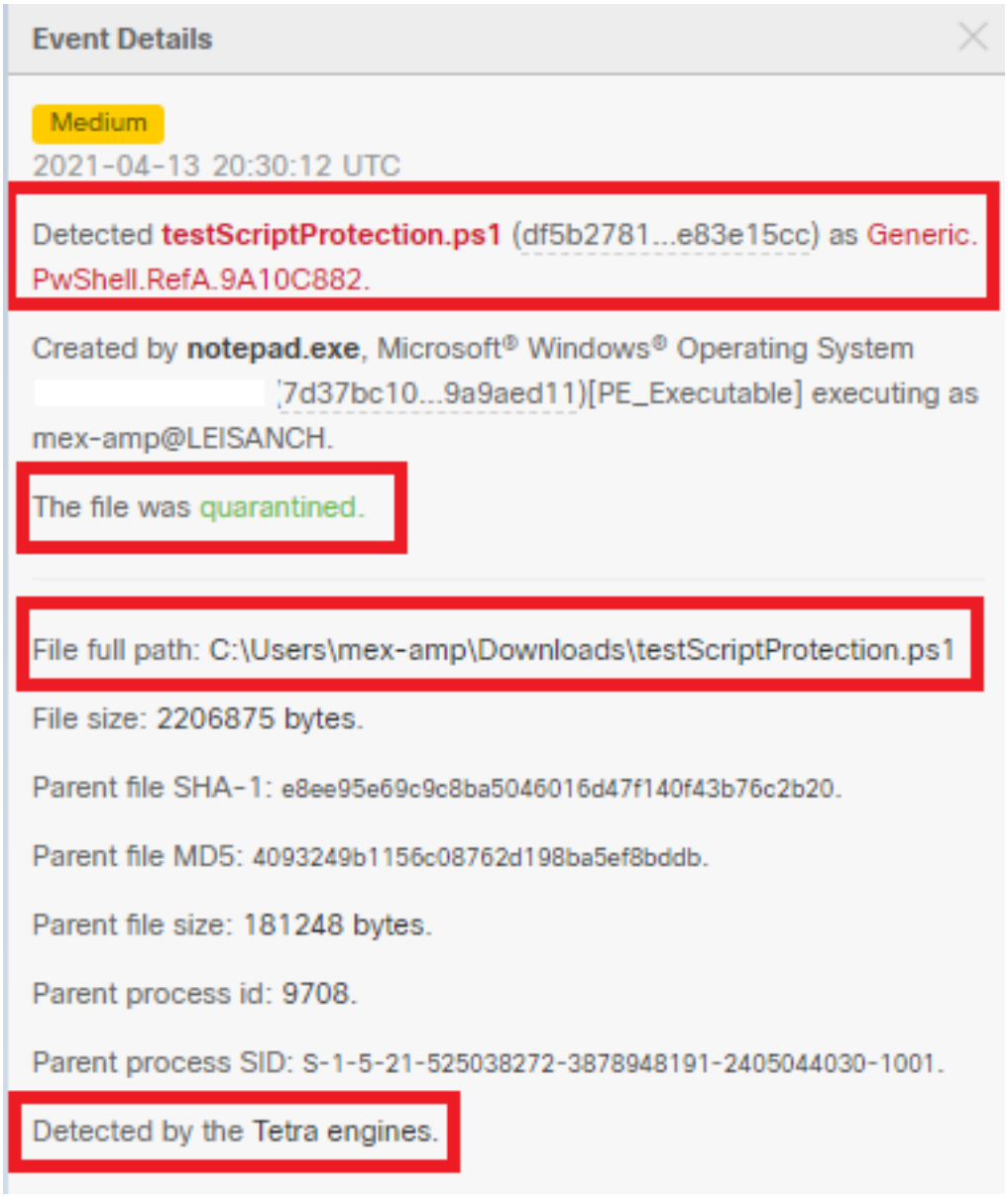
참고:감사 모드에서는 악성 스크립트가 실행될 때 이벤트를 생성하지만, 격리되지 않습니다.

문제 해결

콘솔에서 탐지가 트리거될 때 스크립트 보호에는 특정 이벤트 유형이 없습니다. 악성 파일을 탐지하는 사람을 식별하는 방법은 파일 유형과 실행 위치를 기반으로 합니다.

1. 지원되는 스크립트 통역사 앞에서 파일 확장명을 확인합니다. 이 예는 .ps1 스크립트입니다.

2. Device Trajectory(**디바이스 전파 흔적 분석) > Event Details(이벤트 세부사항)로** 이동합니다. 이 섹션에서는 탐지된 파일과 관련된 추가 세부사항이 표시됩니다(예: SHA256, 파일이 있는 경로, 위협 이름, AMP 커넥터에서 수행한 작업 및 탐지된 엔진).TETRA가 활성화되지 않은 경우 표시되는 엔진은 SHA 엔진입니다. 예를 들어, TETRA가 활성화된 경우 TETRA가 스크립트 보호와 함께 작동하여 이미지에 표시된 대로 추가 보호를 제공합니다.



탐지 조사

탐지가 실제로 악의적인지 확인하기 위해 Device Trajectory를 사용하여 상위 프로세스, 원격 호스트에 대한 연결, 악성코드에 의해 다운로드될 수 있는 알 수 없는 파일 등 스크립트가 실행되는 동안 발생한 이벤트에 대한 가시성을 제공할 수 있습니다.

오탐 탐지

일단 탐지가 식별되고 스크립트가 신뢰되고 사용자 환경에서 알려진 경우 이를 오탐이라고 할 수 있습니다.커넥터가 스캔하지 않도록 하려면 이미지에 표시된 대로 해당 스크립트를 제외시킬 수 있습니다.

참고:해당 커넥터에 적용된 정책에 제외 세트가 추가되었는지 확인합니다.

관련 정보

- AMP 사용 설명서
- 기술 지원 및 문서 – Cisco Systems