Solucionar problemas de proteção de script na AMP para endpoints

Contents

Introduction

Este documento descreve a configuração do mecanismo de proteção de script no AMP (Advanced Malware Protection, Proteção avançada contra malware) para endpoints.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso do administrador ao console AMP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Conector versão 7.2.1 ou posterior
- Windows 10 versão 1709 e posterior ou Windows Server 2016 versão 1709 e posterior

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O mecanismo de proteção de script oferece a capacidade de detectar e bloquear scripts executados em seus endpoints e ajuda a proteger contra ataques baseados em script comumente

usados por malware. A trajetória do dispositivo oferece visibilidade na execução da cadeia, para que você possa observar os aplicativos que executam os scripts em seus dispositivos.

O Engine permite que o conector examine os seguintes tipos de arquivos de script:

Aplicativo	Extensão de arquivo
Aplicativo HTML	HTA
Scripts	BAT, CMD, VB, VBS, JS
Script criptografado	JSE, VSE
Windows Script	WS, WASF, SWC, WSH
PowerShell	PS1, PS1XML, PSC1, PSC2, MSH, MSH1, MSH2, MSHXML, MSH1XML, MSH2XML
Atalho	SCF
Link	LNK
Instalação	INF, INX
Registro	REG
Palavra	DOCX, DOTX, DOCM, DOTM
Excel	XLS, XLSX, XLTX, XLSM, XLTM, XLAM
PowerPoint	PPT, PPTX, POTX, POTM, PPTM, PPAM, PPSM, SLDM

A proteção de script funciona com os seguintes intérpretes de script:

- PowerShell (V3 e posterior)
- Windows Script Host (wscript.exe e cscript.exe)
- JavaScript (não navegador)
- VBScript
- Macros do Office VBA

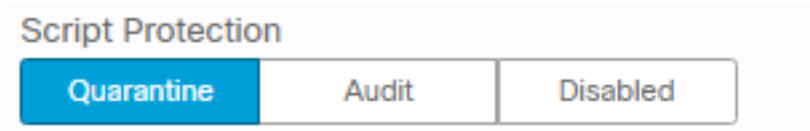
Aviso: a proteção de scripts não fornece visibilidade nem proteção de interpretadores de script que não sejam da Microsoft, como Python, Perl, PHP ou Ruby.

Cuidado: o modo de Convicção de Quarentena tem potencial para afetar os aplicativos do usuário, como Word, Excel e Powerpoint. Se esses aplicativos tentarem executar um script de VBA mal-intencionado, o aplicativo será interrompido.

A proteção de script homenageia o **modo de execução ativo**, funciona em dois modos diferentes: **Ativo** e **passivo**. No modo Ativo, os scripts são bloqueados para serem executados até que o conector receba informações sobre se é ou não mal-intencionado ou se um tempo limite é atingido. No modo Passivo, os scripts podem ser executados enquanto o script é pesquisado para determinar se é ou não mal-intencionado.

Configuração

Para habilitar a Proteção de script, navegue até suas configurações de política e, em Modos e mecanismos, selecione o modo de condenação para Auditoria, Quarentena ou Desabilitado, como mostrado na imagem.

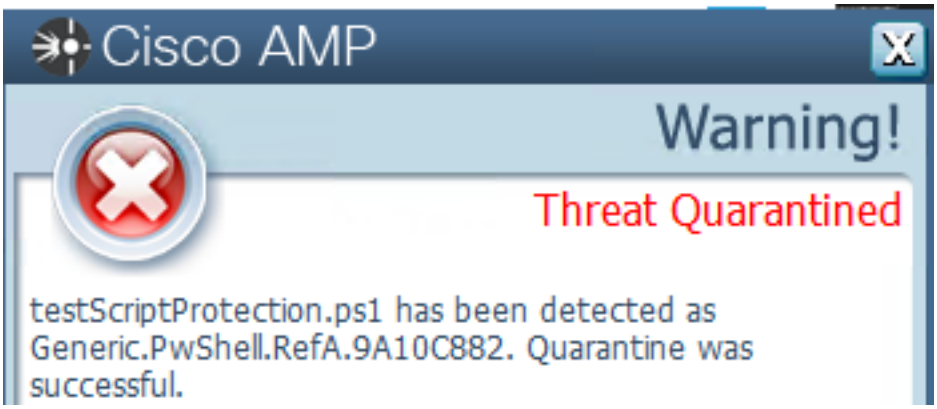


Observação: a proteção de script não depende do TETRA, mas se o TETRA estiver ativado,

ele o usará para fornecer proteção adicional.

Detecção

Quando a detecção é acionada, uma notificação pop-up é exibida no endpoint, como mostrado na imagem.



O console exibe um evento Detectado por Ameaça, como mostrado na imagem.

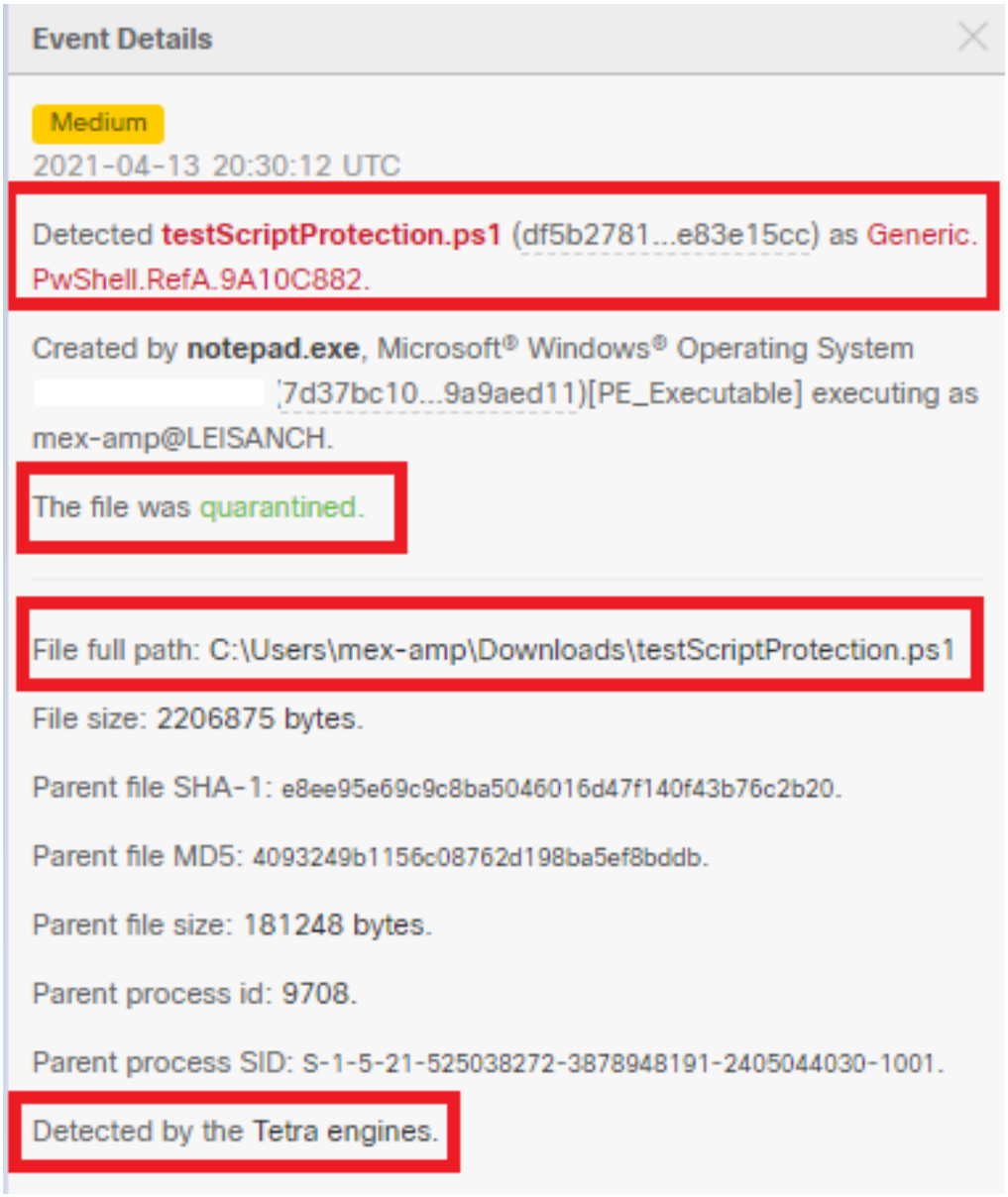
Note: O modo de auditoria cria um evento quando um script mal-intencionado é executado, no entanto, ele não é colocado em quarentena.

Troubleshoot

A proteção de script não tem um tipo de evento específico quando a detecção é acionada no console, uma forma de identificar quem detecta o arquivo mal-intencionado é baseada no tipo de arquivo e onde ele é executado.

1. De acordo com os interpretadores de script suportados, identifique a extensão do arquivo, para este exemplo é um script .ps1.

2. Navegue até **Device Trajettory > Event Details**, nesta seção serão exibidos mais detalhes relacionados ao arquivo detectado, como SHA256, um caminho onde o arquivo foi localizado, nome da ameaça, ação tomada pelo conector AMP e o mecanismo que o detecta. Caso o TETRA não esteja ativado, o mecanismo exibido é o mecanismo SHA, por exemplo, o TETRA é exibido porque quando o TETRA está ativado, ele trabalha com Proteção de script para fornecer proteção adicional, como mostrado na imagem.

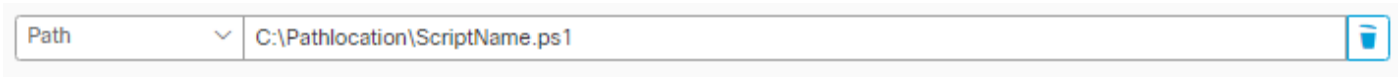


Investigar a detecção

Para determinar se a detecção é realmente mal-intencionada ou não, você pode usar a trajetória do dispositivo para fornecer visibilidade dos eventos que ocorreram enquanto o script foi executado, como processos principais, conexões com hosts remotos e arquivos desconhecidos que podem ser baixados por malware.

Detecção Falsa Positiva

Depois que a detecção é identificada e se o script é confiável e conhecido pelo seu ambiente, ele pode ser chamado de Falso positivo. Para evitar que o conector o examine, você pode criar uma exclusão desse script, como mostrado na imagem.



Note: Verifique se o conjunto de exclusões foi adicionado à política aplicada ao conector afetado.

Informações Relacionadas

- Guia do usuário da AMP
- Suporte Técnico e Documentação - Cisco Systems