Troubleshoot Script Protection in AMP for Endpoints

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[Configuration](#)
[Detection](#)
[Troubleshoot](#)
[Investigate the Detection](#)
[False Positive Detection](#)
[Related Information](#)

Introduction

This document describes the configuration of the Script Protection engine in Advanced Malware Protection (AMP) for Endpoints.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Admin access to AMP console

Components Used

The information in this document is based on these software and hardware versions:

- Connector version 7.2.1 or later
- Windows 10 version 1709 and later or Windows Server 2016 version 1709 and later

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Script Protection engine provides the ability to detect and block scripts executed on your endpoints and helps protect against script-based attacks commonly used by malware. Device

Trajectory provides visibility in the chain execution, so you can observe the applications that execute the scripts on your devices.

The Engine allows the connector to scan the following script file types:

Application	File Extension
HTML Application	HTA
Scripts	BAT, CMD, VB, VBS, JS
Encrypted Script	JSE, VSE
Windows Script	WS, WASF, SWC, WSH
PowerShell	PS1, PS1XML, PSC1, PSC2, MSH, MSH1, MSH2, MSHXML, MSH1XML, MSH2XML
Shortcut	SCF
Link	LNK
Setup	INF, INX
Registry	REG
Word	DOCX, DOTX, DOCM, DOTM
Excel	XLS, XLSX, XLTX, XLSM, XLTM, XLAM
PowerPoint	PPT, PPTX, POTX, POTM, PPTM, PPAM, PPSM, SLDM

Script Protection works with the following script interpreters:

- PowerShell (V3 and later)
- Windows Script Host (wscript.exe and cscript.exe)
- JavaScript (non-browser)
- VBScript
- Office VBA macros

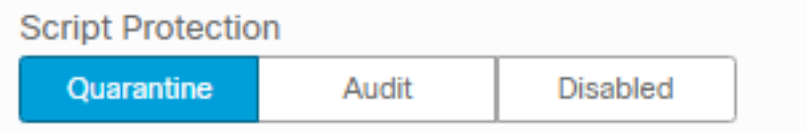
> **Warning**: Script Protection does not provide visibility nor protection from non-Microsoft script interpreters such as Python, Perl, PHP, or Ruby.

> **Caution**: Quarantine Conviction mode has the potential to impact user´s applications such as Word, Excel, and Powerpoint. If these applications attempt to execute a malicious VBA script, the application is stopped.

Script Protection honors the **On Execute Mode**, it works on two different modes: **Active** and **Passive**. In Active mode, scripts are blocked from being executed until the connector receives information of whether or not it is malicious or a timeout is reached. In Passive mode, scripts are allowed to be executed while the script is looked up to determine whether or not it is malicious.

Configuration

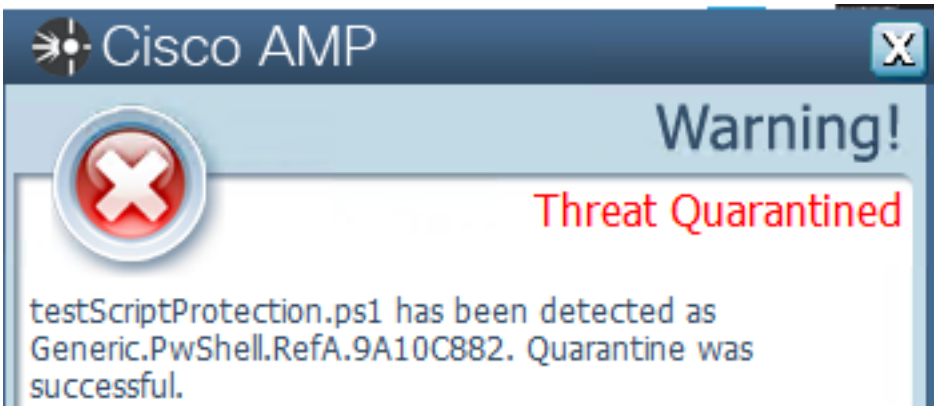
In order to enable Script Protection, navigate to your policy settings, then under Modes and Engines select the Conviction mode to Audit, Quarantine, or Disabled, as shown in the image.



> **Note**: Script Protection is not dependent on TETRA but if TETRA is enabled it uses it to provide additional protection.

Detection

Once the detection is triggered, a pop-up notification is displayed on the endpoint, as shown in the image.



The console displays a Threat Detected event, as shown in the image.

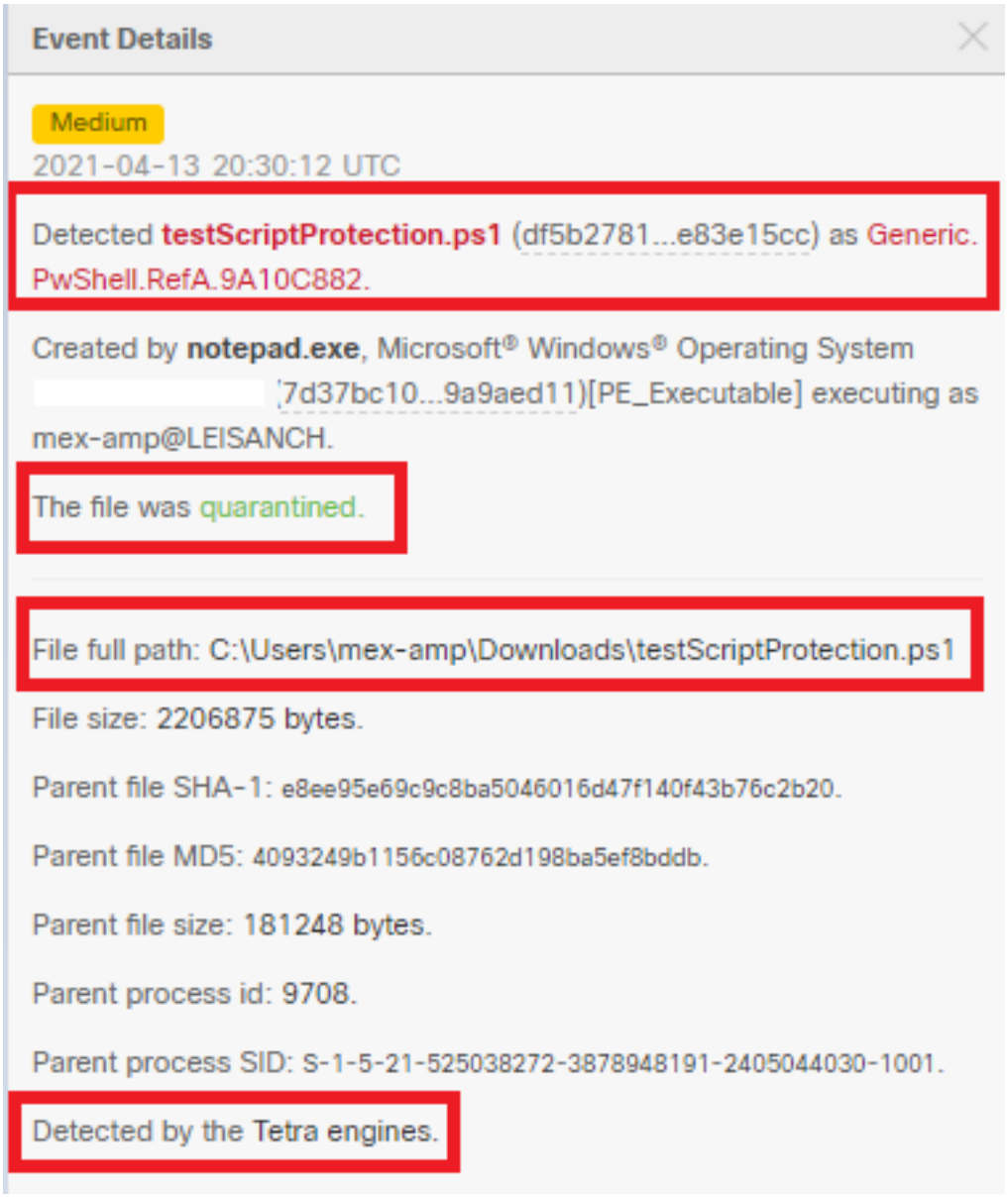
> **Note**: Audit mode creates an event when a malicious script is executed, however, it is not quarantined.

Troubleshoot

Script Protection does not have a specific Event Type when detection is triggered in the console, a way to identify who detects the malicious file is based on the file type and where it runs.

1. Accordingly to the supported script interpreters, identify the file extension, for this example is a .ps1 script.

2. Navigate to **Device Trajectory > Event Details**, in this section more details related to the detected file are displayed, such as SHA256, a path where the file was located, threat name, action taken by the AMP connector, and the engine that detects it. In case TETRA is not enabled, the engine displayed is SHA engine, for this example, TETRA is displayed since when TETRA is enabled, it works with Script Protection to provide additional protection, as shown in the image.

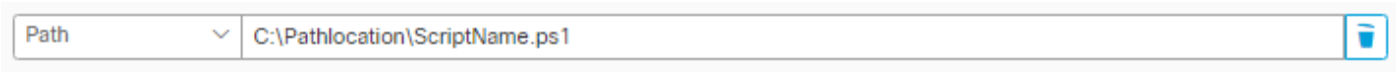


Investigate the Detection

In order to determine if the detection is indeed malicious or not, you can use Device Trajectory to provide you visibility into the events that occurred while the script ran such as parent processes, connections to remote hosts, and unknown files that can be downloaded by malware.

False Positive Detection

Once the detection is identified and if the script is trusted and known by your environment, it can be called a False Positive. In order to prevent the connector scans it, you can create an exclusion that script, as shown in the image.



Note: Ensure the exclusion set is added to the policy applied to the affected connector.

Related Information

- AMP User Guide
- Technical Support & Documentation - Cisco Systems