Troubleshoot Umbrella Cloud Malware Not Detecting Eicar Test Files in Microsoft 365

Contents

Introduction

This document describes how to troubleshoot Umbrella Cloud Malware not detecting eicar test files in Microsoft 365.

Overview

The eicar test file content is an industry-recognized text string that can be used to confirm antivirus software is functioning across many vendors. If you are using this file to confirm that the Cisco Umbrella Cloud Malware feature is functioning on your Microsoft 365 platform, you might notice that the eicar test files are not shown in your Cloud Malware reports or the Scanned Files section.

Resolution

Cisco provides an Advanced Malware Protection (AMP) test file, which is a file that is detected by the Cloud Malware feature but not by the malware protection built into Microsoft 365. This file can be used to verify the correct functionality of Cloud Malware on the Microsoft platform

You can find the AMP test files (and eicar files) in the Cisco Umbrella documentation.

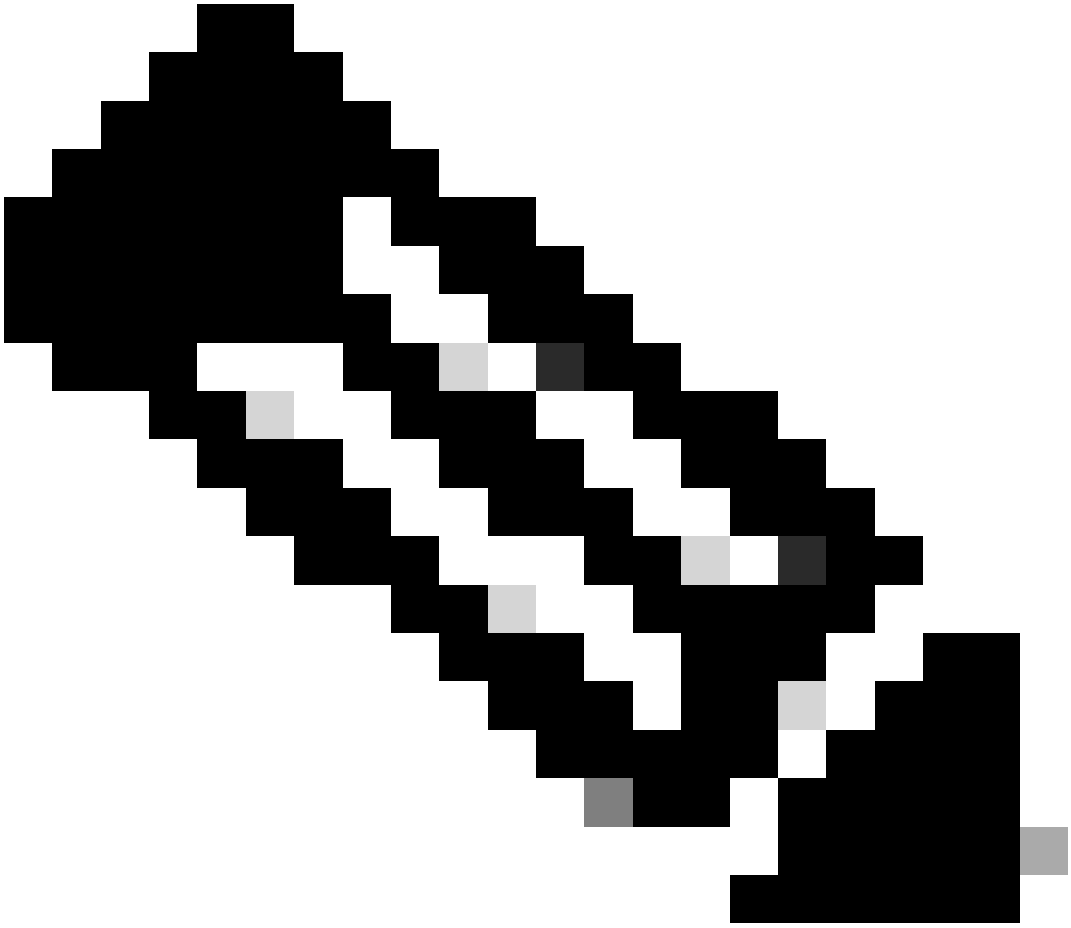
Alternatively, saving a password-protected file to Microsoft is detected as "Suspicious" within the Cloud Malware reporting. Suspicious files display can be toggled via the "Suspect Files" option on the bottom left of the Cloud Malware reporting.

Cause

Microsoft includes a layer of anti-malware protection in their Microsoft subscriptions. You can find more information on this and its configuration in the Microsoft documentation:

- Built-in virus protection in SharePoint Online, OneDrive, and Microsoft Teams
- Safe Attachments for SharePoint, OneDrive, and Microsoft Teams

Microsoft's anti-malware layer detects eicar and as a result, set the malware flag against the file. This, among other things, prevents the file from being shared and also prevents access to it via the API that Cloud Malware uses to integrate with the Microsoft 365 platform.



Note: By default, even though the file is flagged by Microsoft 365 as malware, it still allows the owner to download the file. If this download takes place via Cisco Umbrella Secure Web Gateway (SWG) (with HTTPS inspection enabled), this download is blocked during transfer and appear in the Activity Search report.