對Microsoft 365中的Umbrella雲惡意軟體不檢測Eicar測試檔案進行故障排除

目錄

簡介

概觀

解析

原因

簡介

本文檔介紹如何對Umbrella Cloud惡意軟體進行故障排除，無法檢測Microsoft 365中的早期測試檔案。

概觀

eicar測試檔案內容是行業認可的文本字串，可用於確認防病毒軟體是否在許多供應商中運行。如果您正在使用此檔案來確認Cisco Umbrella雲惡意軟體功能在您的Microsoft 365平台上正常運行，則可能注意到eicar測試檔案未顯示在「雲惡意軟體」報告或「掃描的檔案」部分中。

解析

思科提供高級惡意軟體防護(AMP)測試檔案，該檔案由雲惡意軟體功能檢測，但無法由Microsoft 365內建的惡意軟體防護檢測。此檔案可用於驗證Microsoft平台上雲惡意軟體的正確功能

您可以在Cisco Umbrella文檔中找到AMP測試檔案（和eicar檔案）。

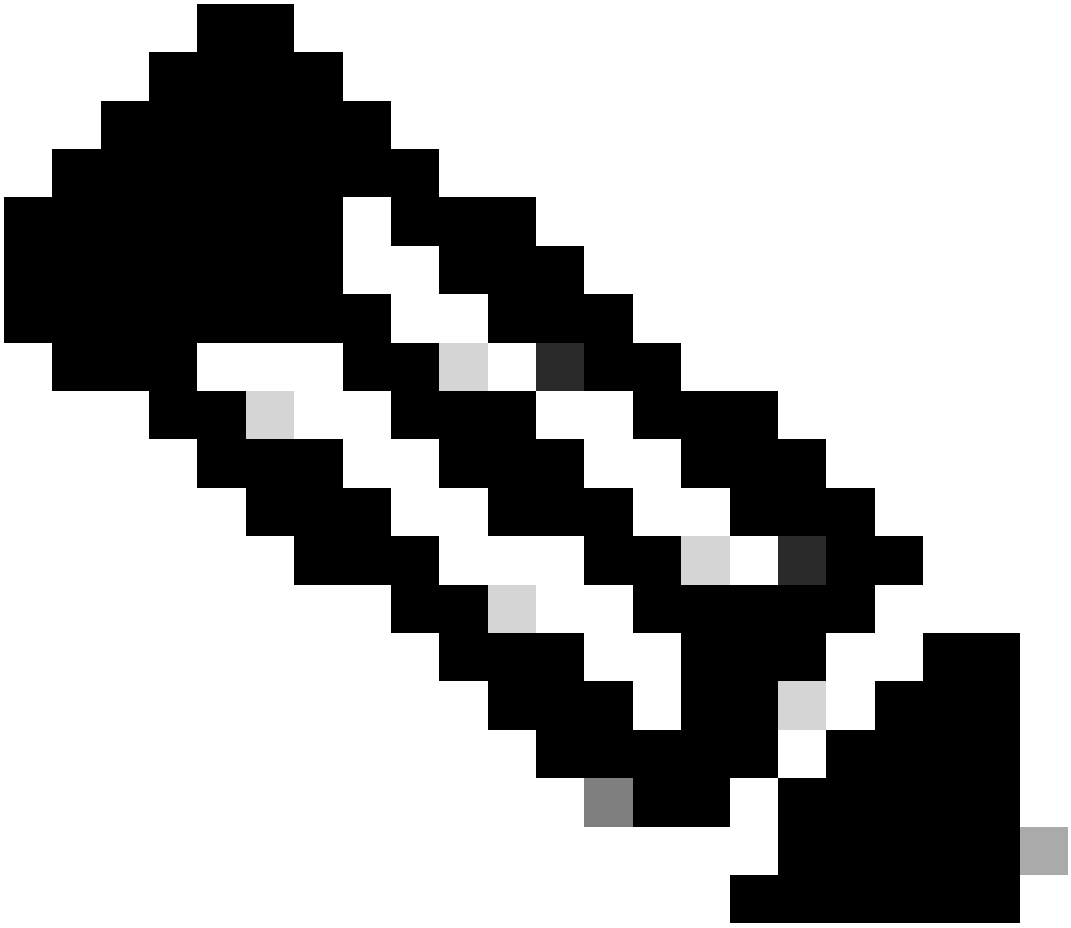
或者，將受密碼保護的檔案儲存到Microsoft會在雲惡意軟體報告中檢測為「可疑」。通過Cloud Malware報告左下角的「Suspect Files」選項，可以切換可疑檔案的顯示。

原因

Microsoft在其Microsoft訂閱中包含一層防惡意軟體防護。您可以在Microsoft文檔中查詢有關此問題及其配置的詳細資訊：

- SharePoint Online、OneDrive和Microsoft Teams中的內建病毒防護
- SharePoint、OneDrive和Microsoft Teams的安全附件

Microsoft的反惡意軟體層會檢測eicar，從而針對該檔案設定惡意軟體標誌。這可以阻止共用檔案，還可以阻止通過Cloud Malware用於與Microsoft 365平台整合的API訪問該檔案。



附註：預設情況下，即使Microsoft 365將該檔案標籤為惡意軟體，它仍允許所有者下載該檔案。如果此下載通過Cisco Umbrella安全Web網關(SWG)（啟用HTTPS檢查）進行，則此下載在傳輸過程中被阻止並顯示在「活動搜尋」報告中。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。