对Microsoft 365中的Umbrella云恶意软件不检测Eicar测试文件进行故障排除

目录

简介

本文档介绍如何排除Umbrella Cloud恶意软件在Microsoft 365中无法检测到测试文件的故障。

概述

eicar测试文件内容是行业认可的文本字符串，可用于确认防病毒软件是否可在多个供应商中运行。如果您正在使用此文件确认Cisco Umbrella云恶意软件功能在Microsoft 365平台上运行，您可能会注意到eicar测试文件未显示在“云恶意软件”报表或“扫描的文件”部分中。

分辨率

思科提供高级恶意软件防护(AMP)测试文件，该文件由云恶意软件功能检测，但无法由Microsoft 365内置的恶意软件防护检测。此文件可用于验证Microsoft平台上云恶意软件的正确功能

您可以在Cisco Umbrella文档中找到AMP测试文件(和每个文件)。

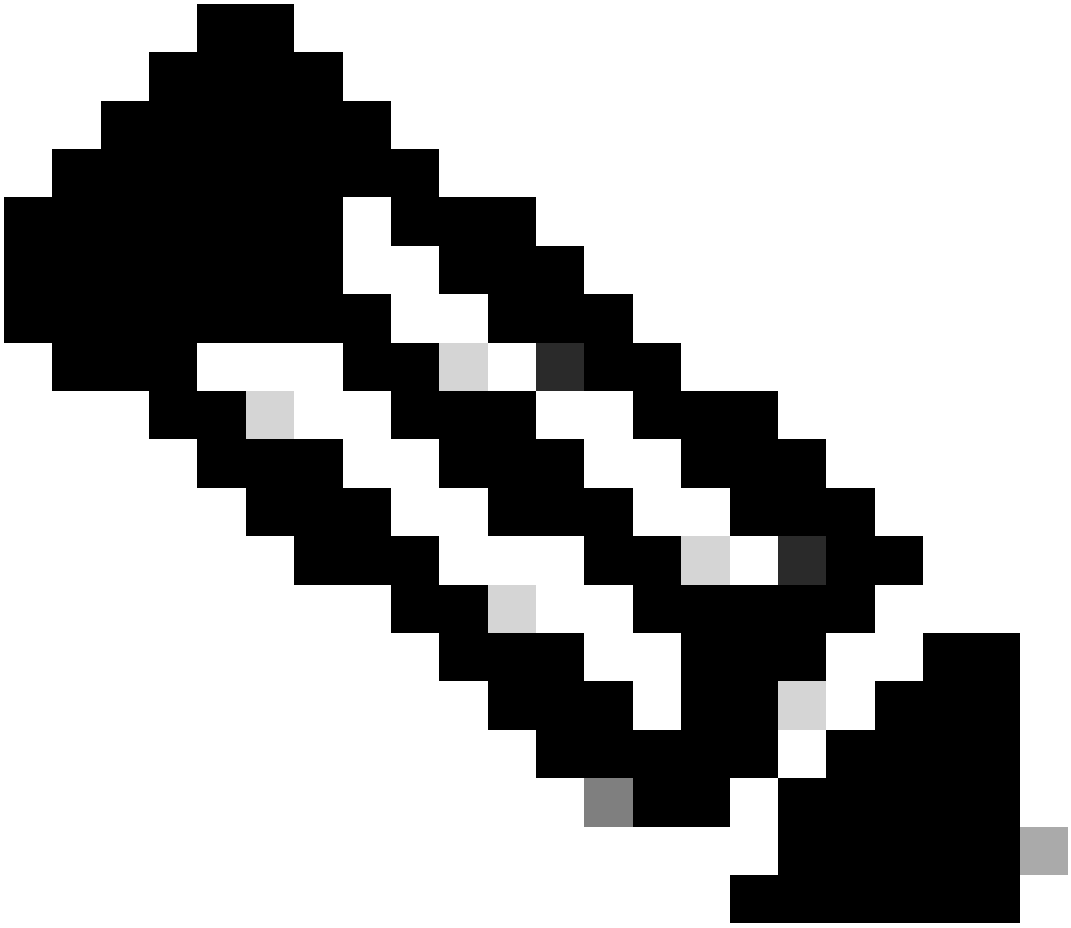
或者，将受密码保护的文件保存到Microsoft会在云恶意软件报告中检测为“可疑”。通过“云恶意软件报告”左下方的“可疑文件”选项，可以切换可疑文件的显示。

原因

Microsoft在其Microsoft订用中包含一层防恶意软件防护。有关此及其配置的详细信息，请参阅Microsoft文档：

- SharePoint Online、OneDrive和Microsoft Teams中的内置病毒防护
- SharePoint、OneDrive和Microsoft Teams的安全附件

Microsoft的防恶意软件层会检测到恶意软件，因此会针对该文件设置恶意软件标志。这可以阻止共享文件，还可以阻止通过云恶意软件用于与Microsoft 365平台集成的API访问文件。



注意：默认情况下，即使Microsoft 365将该文件标记为恶意软件，它仍允许所有者下载该文件。如果此下载通过Cisco Umbrella安全Web网关(SWG)进行（启用HTTPS检查），则此下载在传输期间被阻止并显示在“活动搜索”报告中。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。