Solución de problemas de Umbrella Cloud Malware que no detecta archivos de prueba Eicar en Microsoft 365

Contenido

Introducción

Este documento describe cómo resolver problemas de Malware de Umbrella Cloud que no detecta archivos de prueba eicar en Microsoft 365.

Overview

El contenido del archivo de prueba eicar es una cadena de texto reconocida en el sector que se puede utilizar para confirmar que el software antivirus funciona en muchos proveedores. Si utiliza este archivo para confirmar que la función Cisco Umbrella Cloud Malware está funcionando en la plataforma Microsoft 365, es posible que observe que los archivos de prueba eicar no se muestran en los informes de malware en la nube o en la sección Archivos analizados.

Resolución

Cisco proporciona un archivo de prueba de protección frente a malware avanzado (AMP), que es un archivo que detecta la función de malware en la nube, pero no la protección frente a malware integrada en Microsoft 365. Este archivo se puede utilizar para comprobar la funcionalidad correcta del malware en la nube en la plataforma de Microsoft

Puede encontrar los archivos de prueba de AMP (y los archivos Eicar) en la documentación de Cisco Umbrella.

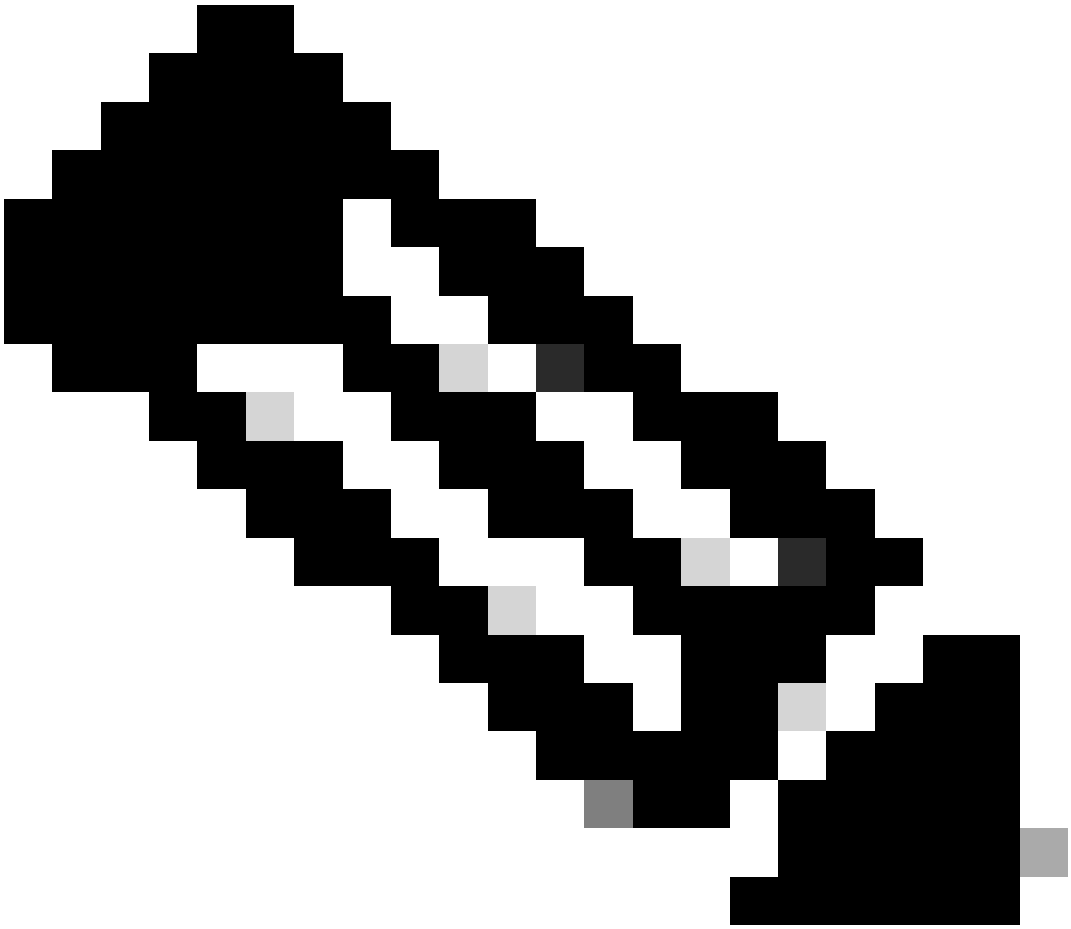
Como alternativa, al guardar un archivo protegido mediante contraseña en Microsoft, se detecta que es "sospechoso" en los informes de malware en la nube. La visualización de archivos sospechosos se puede alternar mediante la opción "Archivos sospechosos" en la parte inferior izquierda de los informes de malware en la nube.

Causa

Microsoft incluye una capa de protección antimalware en sus suscripciones de Microsoft. Puede encontrar más información sobre esto y su configuración en la documentación de Microsoft:

- Protección antivirus integrada en SharePoint Online, OneDrive y Microsoft Teams
- Archivos adjuntos seguros para SharePoint, OneDrive y Microsoft Teams

La capa anti-malware de Microsoft detecta eicar y, como resultado, establece la bandera de malware contra el archivo. Esto, entre otras cosas, evita que el archivo se comparta y también impide el acceso a él a través de la API que Cloud Malware utiliza para integrarse con la plataforma Microsoft 365.



Nota: De forma predeterminada, aunque Microsoft 365 marque el archivo como malware, el propietario podrá descargarlo. Si la descarga se realiza mediante Cisco Umbrella Secure Web Gateway (SWG) (con la inspección HTTPS activada), la descarga se bloquea durante la transferencia y aparece en el informe de búsqueda de actividad.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).