Dépanner les programmes malveillants Umbrella Cloud ne détectant pas les fichiers de test Eicar dans Microsoft 365

Table des matières

Introduction

Ce document décrit comment dépanner Umbrella Cloud Malware ne détectant pas les fichiers de test eicar dans Microsoft 365.

Aperçu

Le contenu du fichier de test eicar est une chaîne de texte reconnue par l'industrie qui peut être utilisée pour confirmer que le logiciel antivirus fonctionne sur de nombreux fournisseurs. Si vous utilisez ce fichier pour confirmer que la fonctionnalité Cisco Umbrella Cloud Malware fonctionne sur votre plate-forme Microsoft 365, vous remarquerez peut-être que les fichiers de test eicar ne sont pas affichés dans vos rapports de programme malveillant cloud ou dans la section Fichiers analysés.

Résolution

Cisco fournit un fichier de test AMP (Advanced Malware Protection), qui est un fichier détecté par la fonctionnalité de programme malveillant sur le cloud, mais pas par la protection contre les programmes malveillants intégrée à Microsoft 365. Ce fichier peut être utilisé pour vérifier le bon fonctionnement du programme malveillant sur le cloud sur la plate-forme Microsoft

Vous trouverez les fichiers de test AMP (et les fichiers eicar) dans la documentation Cisco Umbrella.

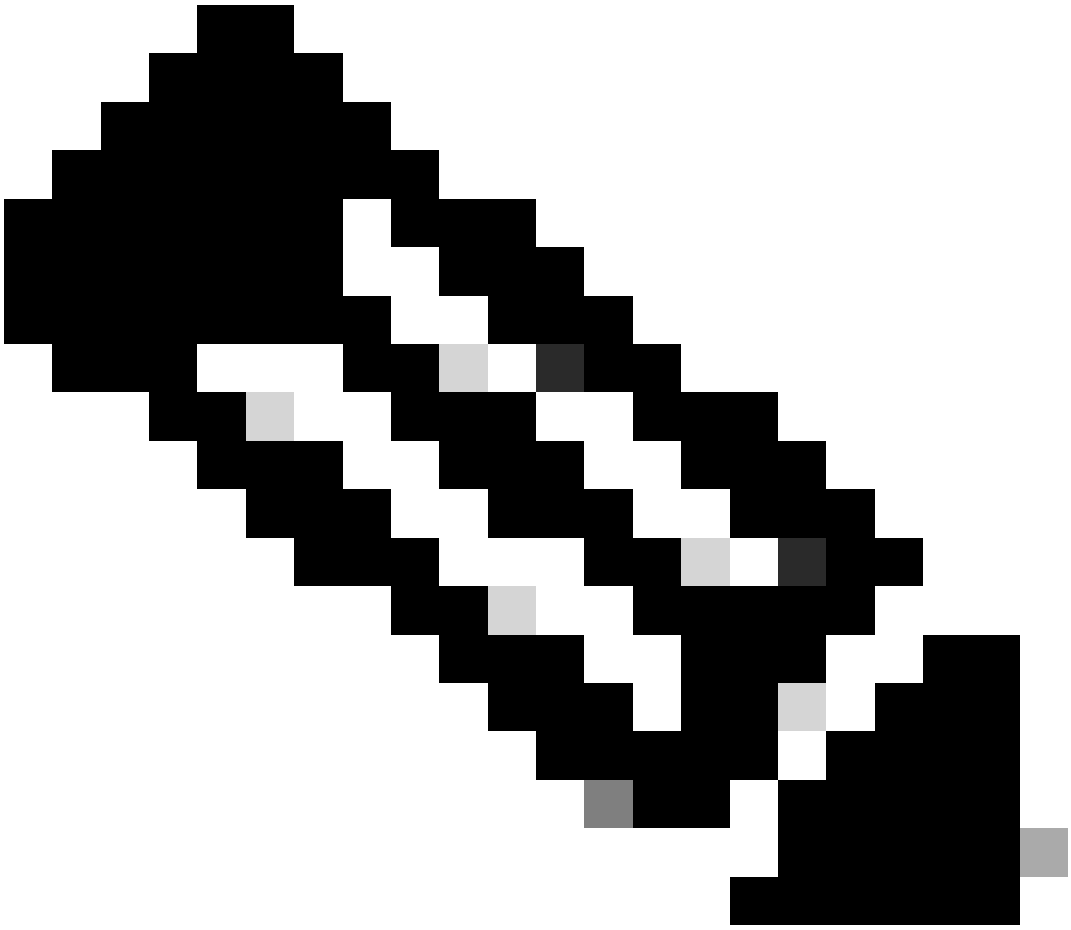
Par ailleurs, l'enregistrement d'un fichier protégé par mot de passe dans Microsoft est détecté comme « suspect » dans les rapports sur les programmes malveillants dans le cloud. L'affichage des fichiers suspects peut être basculé via l'option « Fichiers suspects » en bas à gauche du rapport sur les programmes malveillants dans le cloud.

Motif

Microsoft inclut une couche de protection contre les programmes malveillants dans ses abonnements Microsoft. Vous trouverez plus d'informations sur cette configuration dans la documentation Microsoft :

- Protection antivirus intégrée dans SharePoint Online, OneDrive et Microsoft Teams
- Pièces jointes sécurisées pour SharePoint, OneDrive et Microsoft Teams

La couche anti-programme malveillant de Microsoft détecte Eicar et, par conséquent, définit l'indicateur de programme malveillant par rapport au fichier. Ceci, entre autres choses, empêche le fichier d'être partagé et empêche également l'accès à celui-ci via l'API que le Cloud Malware utilise pour intégrer à la plate-forme Microsoft 365.



Remarque : Par défaut, même si le fichier est marqué par Microsoft 365 comme un programme malveillant, il permet toujours au propriétaire de télécharger le fichier. Si ce téléchargement a lieu via Cisco Umbrella Secure Web Gateway (SWG) (avec l'inspection HTTPS activée), ce téléchargement est bloqué pendant le transfert et apparaît dans le rapport de recherche d'activité.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.