Troubleshooting de Umbrella Cloud Malware Não Detectando Arquivos de Teste Eicar no Microsoft 365

Contents

Introdução

Este documento descreve como solucionar problemas de malware do Umbrella Cloud não detectando arquivos de teste eicar no Microsoft 365.

Overview

O conteúdo do arquivo de teste eicar é uma cadeia de texto reconhecida pelo setor que pode ser usada para confirmar se o software antivírus está funcionando em vários fornecedores. Se você estiver usando esse arquivo para confirmar se o recurso Cisco Umbrella Cloud Malware está funcionando em sua plataforma Microsoft 365, observe que os arquivos de teste eicar não são mostrados em seus relatórios de malware na nuvem ou na seção Arquivos verificados.

Resolução

A Cisco fornece um arquivo de teste AMP (Advanced Malware Protection, Proteção avançada contra malware), que é um arquivo detectado pelo recurso Cloud Malware, mas não pela proteção contra malware incorporada ao Microsoft 365. Esse arquivo pode ser usado para verificar a funcionalidade correta do Cloud Malware na plataforma da Microsoft

Você pode encontrar os arquivos de teste da AMP (e os arquivos eicar) na documentação do Cisco Umbrella.

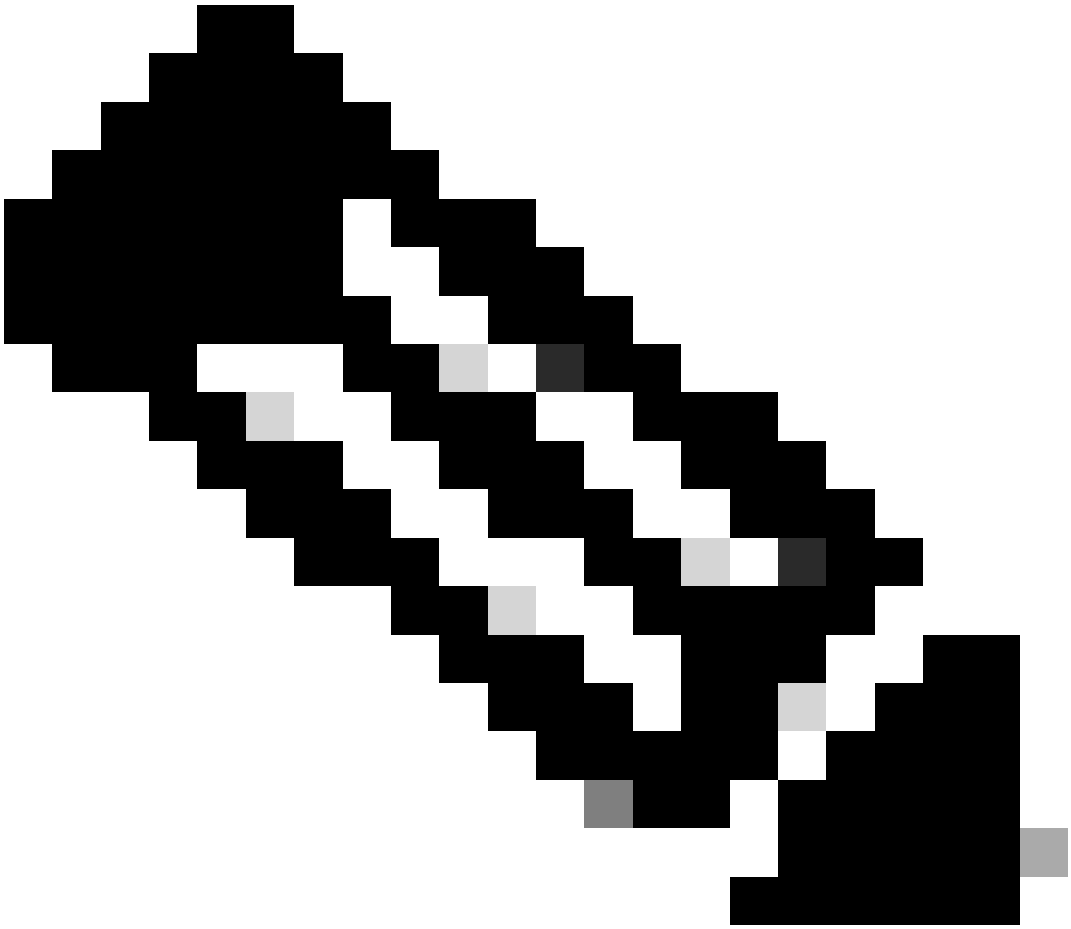
Como alternativa, salvar um arquivo protegido por senha na Microsoft é detectado como "Suspeito" no relatório de malware na nuvem. A exibição de arquivos suspeitos pode ser alternada por meio da opção "Arquivos suspeitos" na parte inferior esquerda do relatório de malware na nuvem.

Causa

A Microsoft inclui uma camada de proteção antimalware em suas assinaturas da Microsoft. Você pode encontrar mais informações sobre isso e sua configuração na documentação da Microsoft:

- Proteção integrada contra vírus no SharePoint Online, OneDrive e Equipes da Microsoft
- Anexos Seguros para Equipes do SharePoint, OneDrive e Microsoft

A camada antimalware da Microsoft detecta eicar e, como resultado, define a bandeira do malware em relação ao arquivo. Isso, entre outras coisas, impede que o arquivo seja compartilhado e também impede o acesso a ele através da API que o malware na nuvem usa para integrar com a plataforma Microsoft 365.



Note: Por padrão, mesmo que o arquivo seja sinalizado pelo Microsoft 365 como malware, ele ainda permite que o proprietário baixe o arquivo. Se esse download ocorrer via Cisco Umbrella Secure Web Gateway (SWG) (com inspeção HTTPS ativada), esse download será bloqueado durante a transferência e será exibido no relatório de pesquisa de atividades.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.