Problemen oplossen Umbrella Cloud Malware niet detecteren Eicar Test Files in Microsoft 365

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen met Umbrella Cloud-malware die geen eicar-testbestanden detecteert in Microsoft 365.

Overzicht

De inhoud van het testbestand van eicar is een door de industrie erkende tekstreeks die kan worden gebruikt om te bevestigen dat antivirussoftware in veel leveranciers functioneert. Als u dit bestand gebruikt om te bevestigen dat de functie Cisco Umbrella Cloud Malware werkt op uw Microsoft 365-platform, kunt u merken dat de testbestanden van eicar niet worden weergegeven in uw rapporten over cloudmalware of in de sectie Gescande bestanden.

resolutie

Cisco biedt een AMP-testbestand (Advanced Malware Protection), een bestand dat wordt gedetecteerd door de Cloud Malware-functie, maar niet door de malware-beveiliging die is ingebouwd in Microsoft 365. Dit bestand kan worden gebruikt om de juiste functionaliteit van Cloud Malware op het Microsoft-platform te verifiëren

U kunt de AMP-testbestanden (en eicar-bestanden) vinden in de Cisco Umbrella-documentatie.

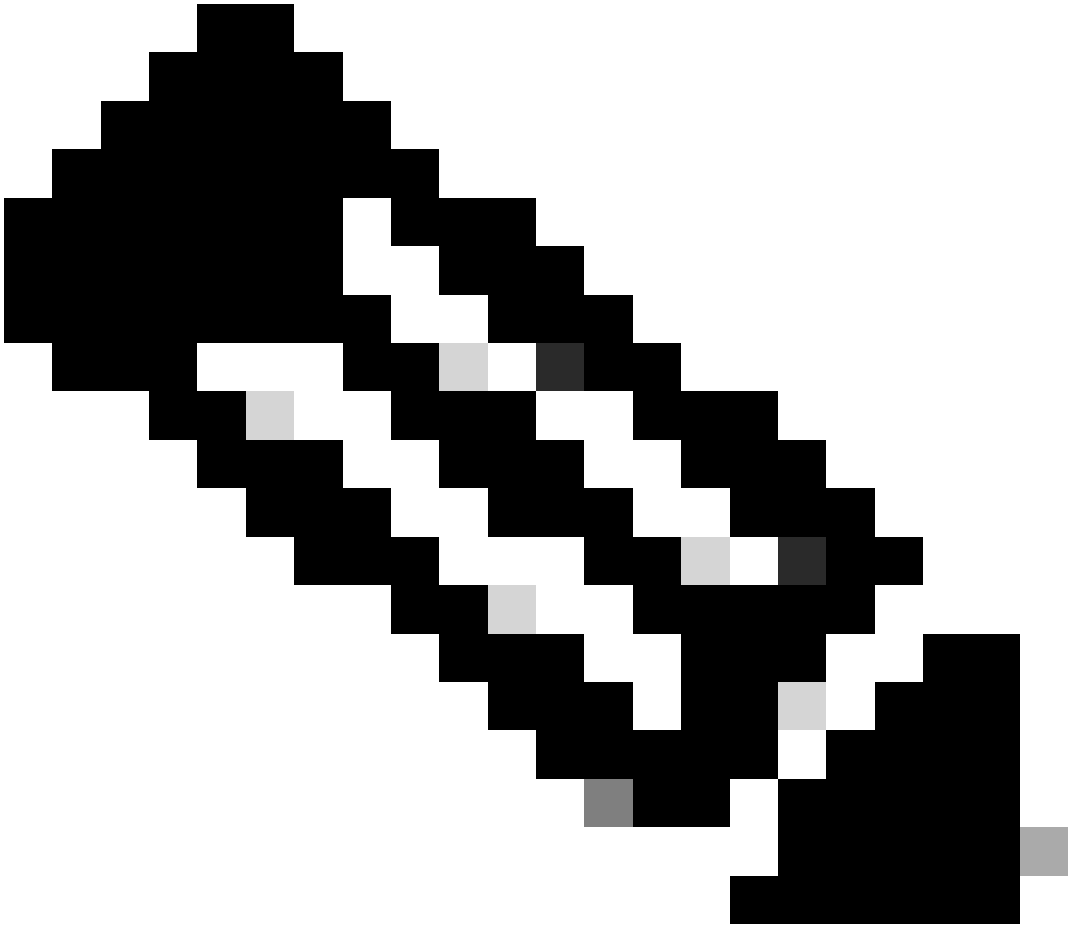
Als alternatief wordt het opslaan van een bestand met wachtwoordbeveiliging naar Microsoft gedetecteerd als "Verdacht" in de rapportage van cloudmalware. De weergave van verdachte bestanden kan worden omgeschakeld via de optie "Verdachte bestanden" linksonder in de rapportage over cloud-malware.

Oorzaak

Microsoft neemt een laag van anti-malware bescherming in hun Microsoft-abonnementen. Meer informatie hierover en de configuratie ervan vindt u in de Microsoft-documentatie:

- Ingebouwde virusbescherming in SharePoint Online, OneDrive en Microsoft Teams
- Veilige bijlagen voor SharePoint, OneDrive en Microsoft Teams

De anti-malwarelaag van Microsoft detecteert eicar en stelt daarom de malware-vlag in tegen het bestand. Dit voorkomt onder andere dat het bestand wordt gedeeld en voorkomt ook toegang tot het via de API die Cloud Malware gebruikt om te integreren met het Microsoft 365-platform.



Opmerking: Hoewel het bestand standaard door Microsoft 365 is gemarkeerd als malware, kan de eigenaar het bestand nog steeds downloaden. Als deze download plaatsvindt via Cisco Umbrella Secure Web Gateway (SWG) (met HTTPS-inspectie ingeschakeld), wordt deze download tijdens de overdracht geblokkeerd en weergegeven in het rapport Activiteit zoeken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.