Fehlerbehebung: Umbrella Cloud-Malware erkennt keine EICAR-Testdateien in Microsoft 365

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei Umbrella Cloud-Malware beschrieben, die eicar-Testdateien in Microsoft 365 nicht erkennt.

Überblick

Der Inhalt der EICAR-Testdatei ist eine in der Branche anerkannte Textzeichenfolge, die verwendet werden kann, um zu bestätigen, dass die Antivirus-Software von vielen Herstellern verwendet wird. Wenn Sie diese Datei verwenden, um zu bestätigen, dass die Cisco Umbrella Cloud Malware-Funktion auf Ihrer Microsoft 365-Plattform funktioniert, stellen Sie möglicherweise fest, dass die EICAR-Testdateien nicht in Ihren Cloud-Malware-Berichten oder im Abschnitt Gescannte Dateien angezeigt werden.

Auflösung

Cisco stellt eine Advanced Malware Protection (AMP)-Testdatei bereit. Dabei handelt es sich um eine Datei, die von der Cloud-Malware-Funktion erkannt wird, jedoch nicht von der in Microsoft 365 integrierten Malware-Schutzfunktion. Diese Datei kann verwendet werden, um die ordnungsgemäße Funktion von Cloud-Malware auf der Microsoft-Plattform zu überprüfen.

Sie finden die AMP-Testdateien (und eicar-Dateien) in der Cisco Umbrella-Dokumentation.

Alternativ wird das Speichern einer kennwortgeschützten Datei bei Microsoft im Rahmen der Cloud-Malware-Berichterstattung als "verdächtig" erkannt. Verdächtige Dateien können über die Option "Verdächtige Dateien" unten links im Cloud-Malware-Bericht angezeigt werden.

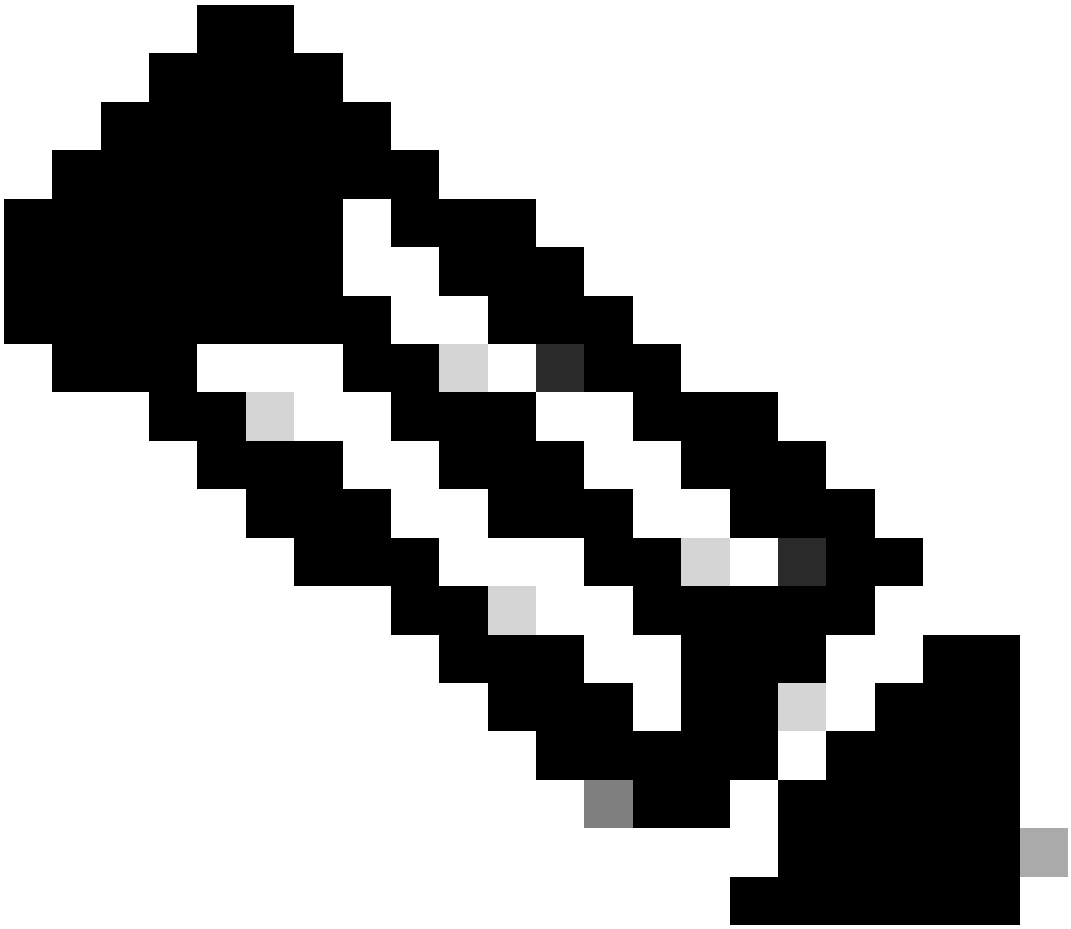
Ursache

Microsoft bietet in seinen Microsoft-Abonnements eine Ebene für Malware-Schutz. Weitere

Informationen hierzu und zur entsprechenden Konfiguration finden Sie in der Microsoft-Dokumentation:

- Integrierter Virenschutz in SharePoint Online, OneDrive und Microsoft Teams
- Sichere Anhänge für SharePoint, OneDrive und Microsoft Teams

Die Anti-Malware-Ebene von Microsoft erkennt eicar und setzt daher die Malware-Markierung für die Datei. Dies verhindert unter anderem die gemeinsame Nutzung der Datei und den Zugriff darauf über die API, die Cloud-Malware für die Integration in die Microsoft 365-Plattform verwendet.



Anmerkung: Obwohl die Datei von Microsoft 365 standardmäßig als Malware markiert wird, kann der Besitzer die Datei immer noch herunterladen. Wenn dieser Download über Cisco Umbrella Secure Web Gateway (SWG) erfolgt (bei aktivierter HTTPS-Überprüfung), wird dieser Download während der Übertragung blockiert und im Bericht "Activity Search" (Aktivitätssuche) angezeigt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.