Risoluzione dei problemi relativi al malware Umbrella Cloud che non rileva i file di test Eicar in Microsoft 365

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al malware Umbrella Cloud che non rileva i file di test EICAR in Microsoft 365.

Panoramica

Il contenuto del file di test eicar è una stringa di testo riconosciuta dal settore che può essere utilizzata per verificare il funzionamento del software antivirus in molti fornitori. Se si utilizza questo file per verificare che la funzionalità Cisco Umbrella Cloud Malware funzioni sulla piattaforma Microsoft 365, è possibile notare che i file di test eicar non sono visualizzati nei report Cloud Malware o nella sezione File digitalizzati.

Risoluzione

Cisco fornisce un file di test Advanced Malware Protection (AMP), che è un file rilevato dalla funzionalità Cloud Malware ma non dalla protezione malware integrata in Microsoft 365. Questo file può essere utilizzato per verificare la corretta funzionalità di Cloud Malware sulla piattaforma Microsoft

I file di test AMP (e i file eicar) sono disponibili nella documentazione di Cisco Umbrella.

In alternativa, il salvataggio di un file protetto da password in Microsoft viene rilevato come "Suspicious" (Sospetto) all'interno del report Cloud Malware (Malware cloud). La visualizzazione dei file sospetti può essere attivata o disattivata tramite l'opzione "Suspect Files" in basso a sinistra del Cloud Malware Reporting.

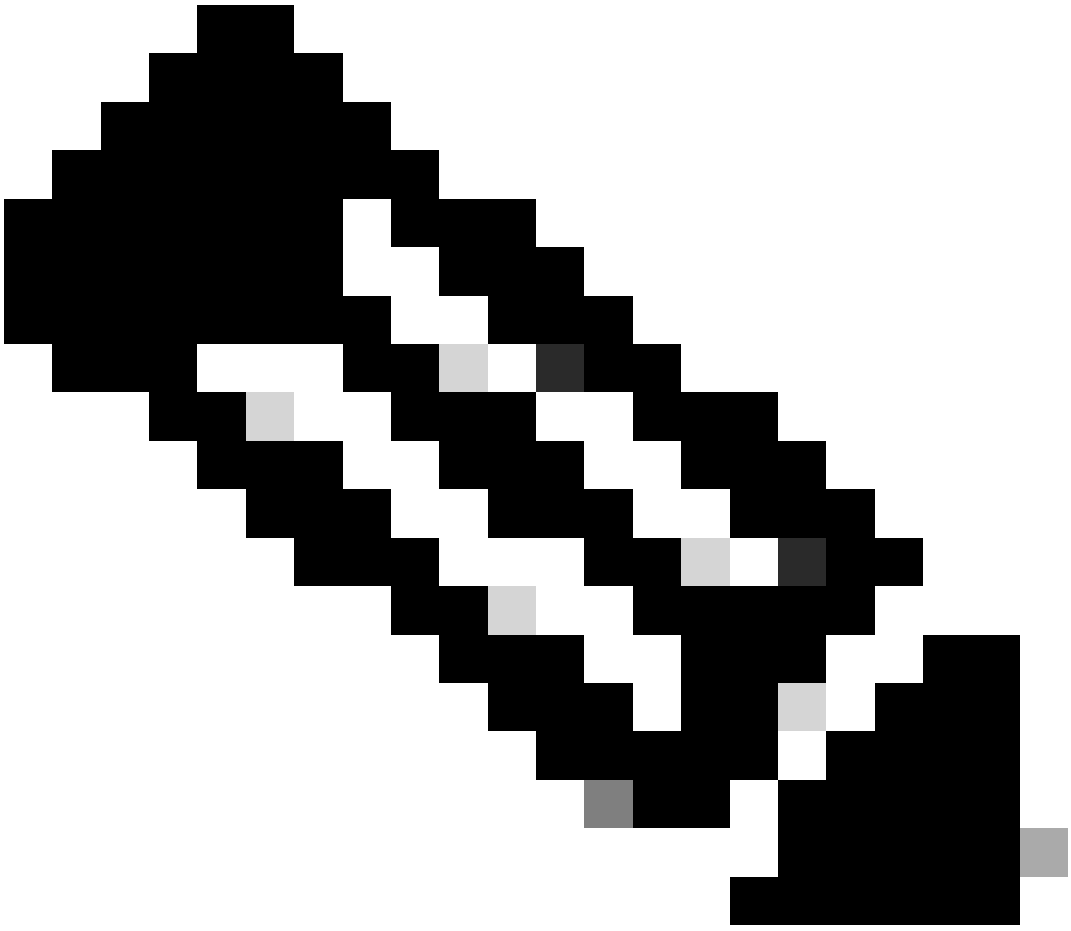
Causa

Microsoft include un livello di protezione antimalware nelle sottoscrizioni Microsoft. Per ulteriori

informazioni su questo argomento e sulla relativa configurazione, vedere la documentazione di Microsoft:

- Protezione antivirus incorporata in SharePoint Online, OneDrive e Microsoft Teams
- Allegati sicuri per SharePoint, OneDrive e team Microsoft

Il livello antimalware di Microsoft rileva l'eicar e, di conseguenza, imposta il flag antimalware sul file. Questo, tra le altre cose, impedisce la condivisione del file e anche l'accesso ad esso attraverso l'API che Cloud Malware utilizza per integrarsi con la piattaforma Microsoft 365.



Nota: Per impostazione predefinita, anche se il file è contrassegnato da Microsoft 365 come malware, consente comunque al proprietario di scaricare il file. Se il download viene eseguito tramite Cisco Umbrella Secure Web Gateway (SWG) (con l'ispezione HTTPS abilitata), il download viene bloccato durante il trasferimento e visualizzato nel report di ricerca attività.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).