Microsoft 365でEicarテストファイルを検出しない包括クラウドマルウェアのトラブルシューティング

内容

はじめに

このドキュメントでは、Microsoft 365でEicarテストファイルを検出しないUmbrella Cloud Malwareをトラブルシューティングする方法について説明します。

概要

eicarテストファイルの内容は業界公認のテキスト文字列で、ウイルス対策ソフトウェアが多くのベンダーで機能していることを確認するために使用できます。 このファイルを使用してMicrosoft 365プラットフォームでCisco Umbrellaクラウドマルウェア機能が機能していることを確認した場合、Eicarテストファイルがクラウドマルウェアレポートまたは「スキャンファイル」セクションに表示されないことがあります。

解決方法

シスコでは、高度なマルウェア防御(AMP)テストファイルを提供しています。このファイルは、クラウドマルウェア機能によって検出されますが、Microsoft 365に組み込まれたマルウェア防御では検出されません。このファイルは、Microsoftプラットフォーム上のクラウドマルウェアの正しい機能を確認するために使用できます

AMPテストファイル（およびeicarファイル）は、Cisco Umbrellaドキュメントにあります。

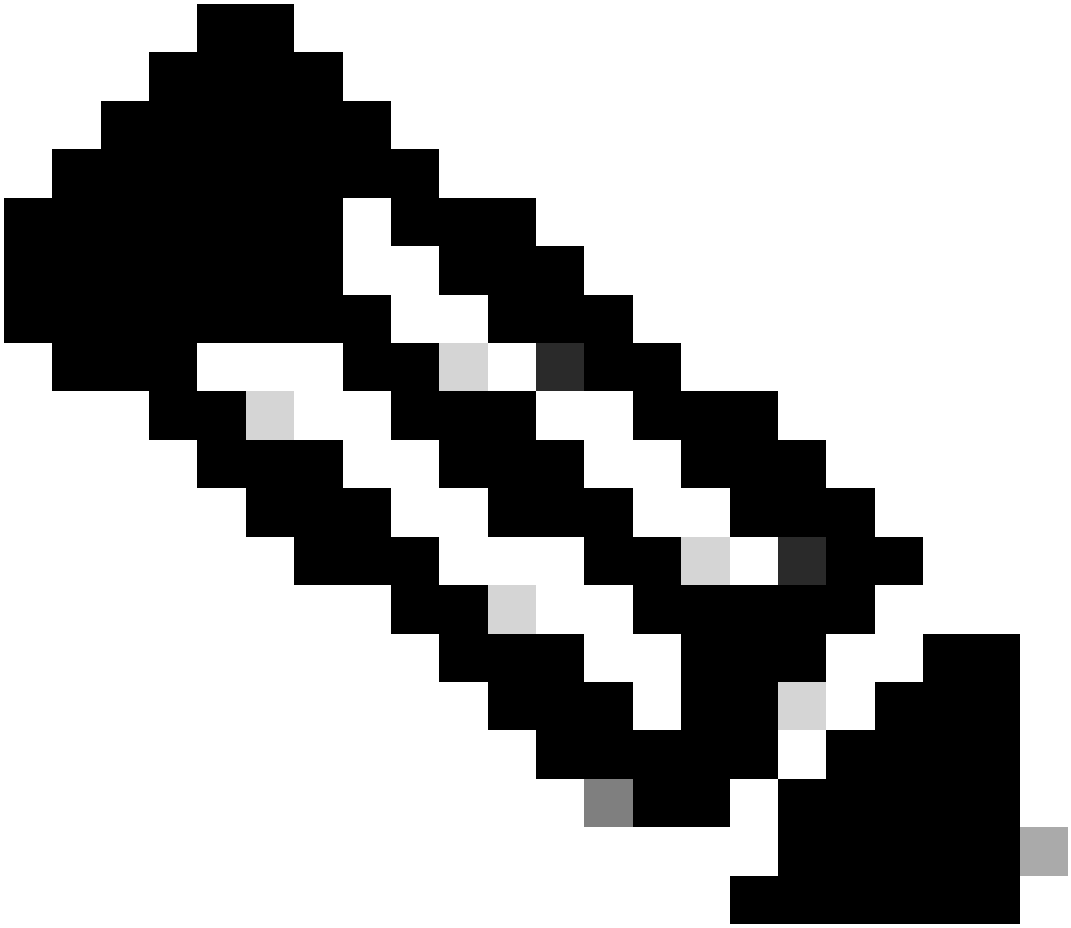
また、パスワードで保護されたファイルをMicrosoftに保存すると、クラウドマルウェアのレポートで「不審」と判断されます。疑わしいファイルの表示は、クラウドマルウェアレポートの左下にある「疑わしいファイル」オプションで切り替えることができます。

原因

Microsoftは、Microsoftサブスクリプションにマルウェア対策保護のレイヤを含めています。この設定の詳細については、次のMicrosoftのドキュメントを参照してください。

- SharePoint Online、OneDrive、およびMicrosoft Teamsに組み込みのウイルス対策
- SharePoint、OneDrive、およびMicrosoft Teamsの安全な添付ファイル

Microsoftのマルウェア対策層はeicarを検出し、その結果、ファイルに対してマルウェアフラグを設定します。これは特に、ファイルが共有されるのを防ぎ、クラウドマルウェアがMicrosoft 365プラットフォームと統合するために使用するAPI経由でのファイルへのアクセスも防ぎます。



注：デフォルトでは、ファイルにマルウェアのフラグがMicrosoft 365によって付けられている場合でも、所有者はファイルをダウンロードできます。このダウンロードがCisco Umbrella Secure Web Gateway(SWG)（HTTPSインスペクションが有効な状態）を介して行われると、このダウンロードは転送中にブロックされ、アクティビティ検索レポートに表示されます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。