Inspection de fichier de test avec Eicar

Table des matières

Introduction

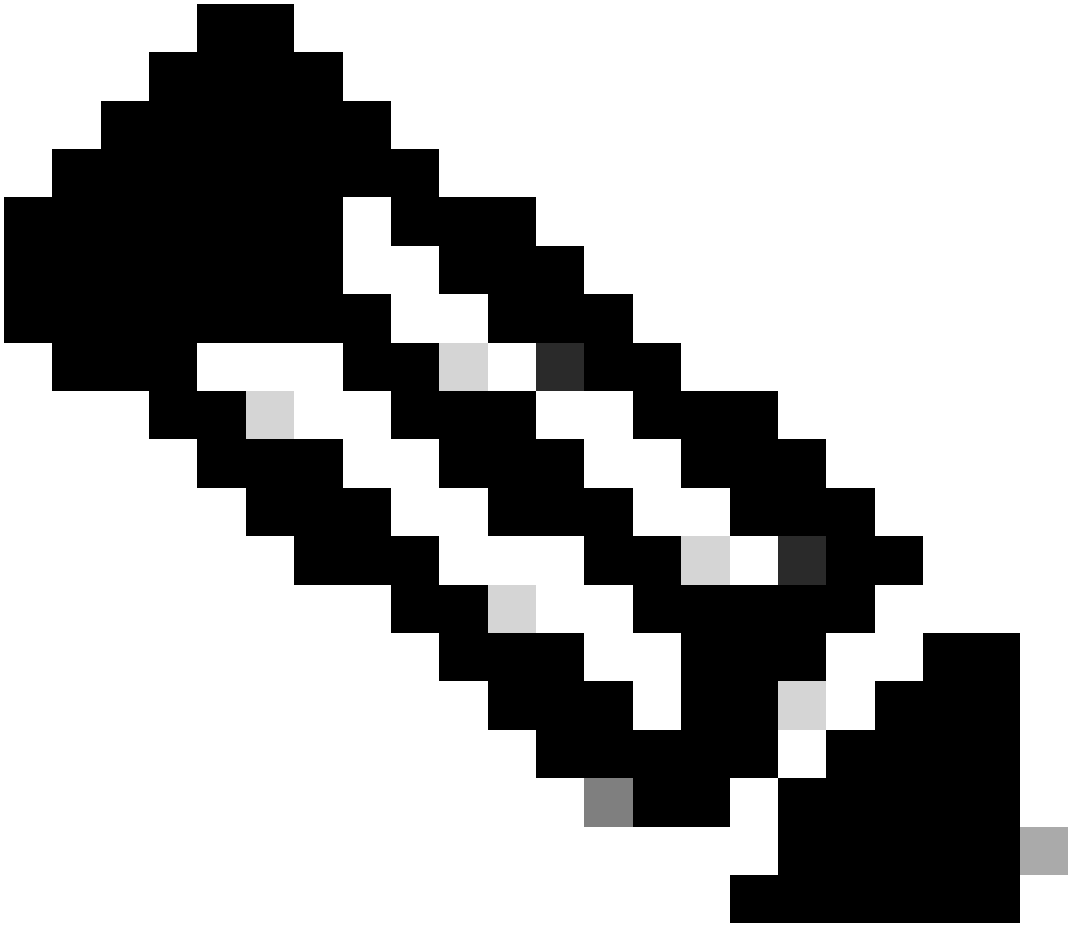
Ce document décrit comment tester l'inspection de fichier avec Eicar.

Aperçu

À l'heure actuelle, lorsque vous testez si la fonction d'inspection des fichiers est activée ou non à l'aide des fichiers de téléchargement de test eicar.org, vous voyez un comportement différent lorsque le « déchiffrement SSL » est activé ou désactivé. Umbrella File Inspection analyse uniquement les téléchargements AV sur eicar.org si le déchiffrement SSL est activé.

Comprendre le processus de détection pour Eicar

Pour activer le blocage de eicar.org, veuillez activer le déchiffrement SSL.



Remarque : Le décodage SSL est requis même lors d'une visite du site via HTTP. Si le décodage SSL n'est pas activé, le proxy contourne les domaines qui traitent le trafic sur HTTPS.

- Le proxy intelligent Umbrella prend la décision d'envoyer ou non un domaine au proxy au niveau de la couche DNS.
- La requête DNS se produit avant la connexion HTTP/HTTPS, ce qui signifie que lorsqu'un domaine est soumis au proxy, le trafic HTTP et HTTPS est toujours mis en proxy.
- Lorsque le trafic HTTP/HTTPS atteint notre proxy intelligent, la première étape consiste à effectuer une redirection pour identifier l'utilisateur.

Cette redirection n'est pas possible sans le déchiffrement SSL, ce qui signifie que nous pourrions être incapables d'identifier correctement les utilisateurs dans certains scénarios (tels que les utilisateurs itinérants).

Pour empêcher ces utilisateurs de casser les requêtes HTTPS, Umbrella n'utilise pas de domaines proxy (comme eicar.org) qui servent à la fois le trafic HTTP/HTTPS, sauf si le

déchiffrement SSL est activé.

En résumé...

Pour obtenir la meilleure sécurité et efficacité de la fonctionnalité, nous vous recommandons fortement d'installer l'autorité de certification racine Cisco et d'activer le déchiffrement SSL. Cela permet de bloquer les fichiers de test eicar.org et d'augmenter le nombre de domaines soumis à l'inspection des fichiers via notre proxy intelligent.

Voici un résumé du comportement attendu :

- Décryptage SSL DÉSACTIVÉ
  - Les sites Eicar.org NE sont PAS bloqués sur https://www.eicar.org/download/eicar.com. Le domaine n'est tout simplement pas du tout mis en proxy car le déchiffrement SSL est désactivé.
  - Notre propre site de test hébergeant eicar sont bloqués : http://proxy.opendnstest.com/download/eicar.com
- Déchiffrement SSL ACTIVÉ
  - Eicar bloqué par l'analyse antivirus sur http://www.eicar.org/download/eicar.com et https://www.eicar.org/download/eicar.com

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.