Probar inspección de archivos con Eicar

Contenido

Introducción

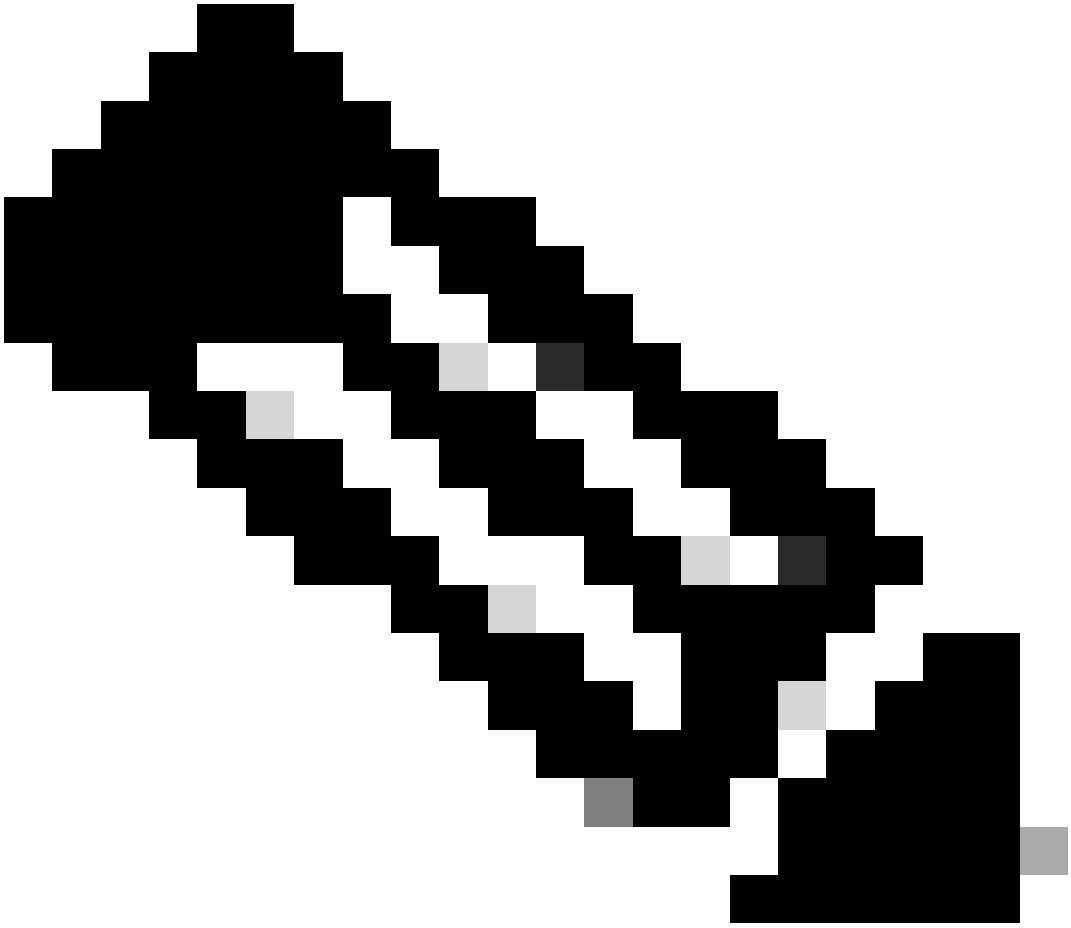
Este documento describe cómo probar la inspección de archivos con Eicar.

Overview

En la actualidad, cuando se prueba si la función de inspección de archivos está habilitada mediante la prueba eicar.org descargar archivos, se ve un comportamiento diferente cuando el "descifrado SSL" está habilitado o deshabilitado. Umbrella File Inspection sólo explora las descargas de AV en eicar.org si el descifrado SSL está activado.

Comprensión del proceso de detección para Eicar

Para habilitar el bloqueo de eicar.org, habilite el descifrado SSL.



Nota: El descifrado SSL es necesario incluso cuando se visita el sitio a través de HTTP. Si no tiene habilitado el descifrado SSL, el proxy omite los dominios que suministran tráfico a través de HTTPS.

- El Umbrella Intelligent Proxy (Proxy inteligente de paraguas) toma la decisión de enviar un dominio al proxy en la capa DNS.
- La solicitud DNS se produce antes de la conexión HTTP/HTTPS, lo que significa que cuando un dominio está sujeto al proxy, el tráfico HTTP y HTTPS siempre se procesa como proxy.
- Cuando el tráfico HTTP/HTTPS llega a nuestro proxy inteligente, el primer paso es realizar una redirección para identificar al usuario.

Esta redirección no es posible sin el descifrado SSL, lo que significa que es posible que no podamos identificar correctamente a los usuarios en algunos escenarios (como los usuarios de roaming).

Para evitar que estos usuarios interrumpan las solicitudes HTTPS, Umbrella no utiliza dominios

proxy (como eicar.org) que ofrezcan tráfico HTTP/HTTPS a menos que se active el descifrado SSL.

En resumen...

Para obtener la mejor seguridad y eficacia de la función, recomendamos encarecidamente instalar la CA raíz de Cisco y habilitar el descifrado SSL. Esto permite bloquear los archivos de prueba de eicar.org y aumenta el número de dominios que están sujetos a la inspección de archivos a través de nuestro proxy inteligente.

A continuación se muestra un resumen del comportamiento esperado:

- Descifrado SSL DESACTIVADO
  - Los sitios Eicar.org NO están bloqueados en https://www.eicar.org/download/eicar.com. El dominio simplemente no está proxy en absoluto porque el descifrado SSL está inhabilitado.
  - Nuestro propio sitio de prueba que aloja eicar está bloqueado: http://proxy.opendnstest.com/download/eicar.com
- Descifrado SSL ACTIVADO
  - Eicar bloqueado por análisis antivirus en http://www.eicar.org/download/eicar.com y https://www.eicar.org/download/eicar.com

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).