Testar inspeção de arquivo com Eicar

Contents

Introdução

Overview

Entendendo o processo de detecção do Eicar

Em resumo...

Introdução

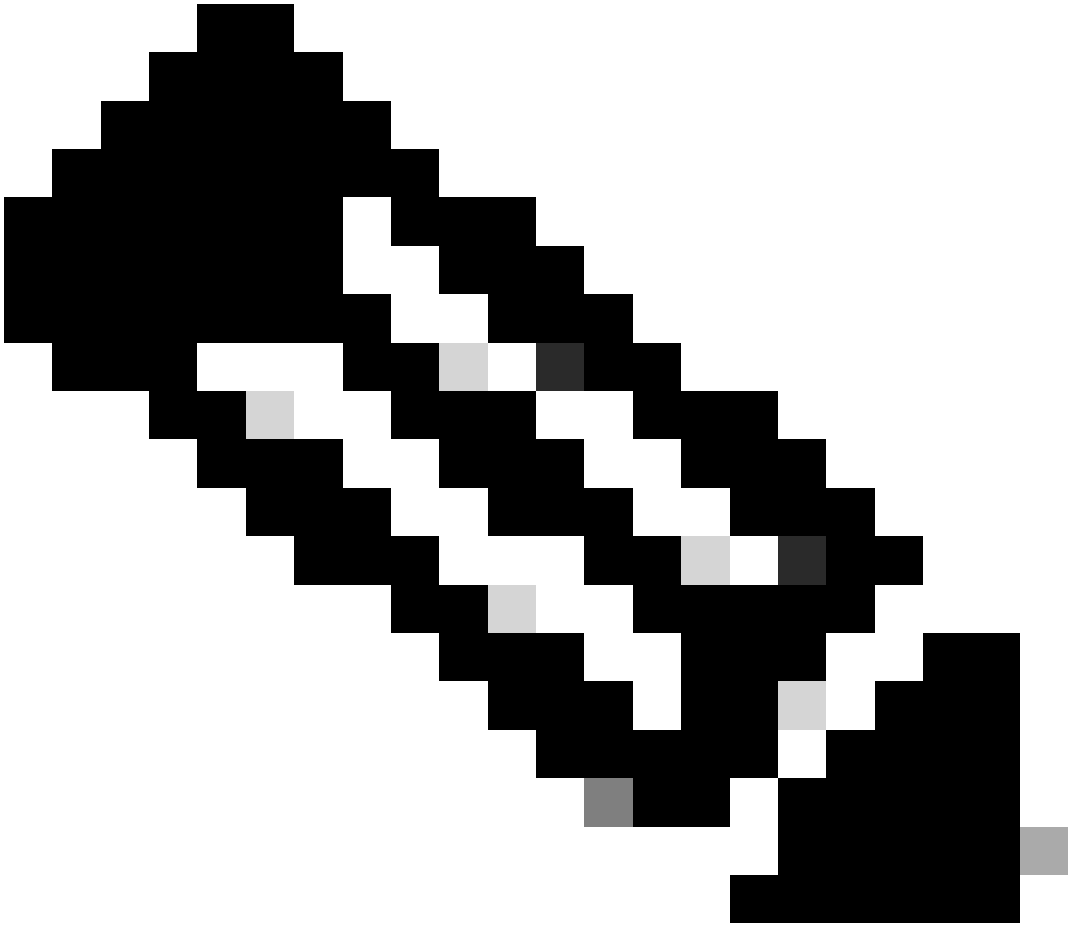
Este documento descreve como testar a inspeção de arquivo com Eicar.

Overview

No momento, ao testar se o recurso de inspeção de arquivo está ou não habilitado usando os arquivos de download de teste eicar.org, você vê um comportamento diferente quando a "descriptografia SSL" está habilitada ou desabilitada. O Umbrella File Inspection só verifica downloads de AV em eicar.org se a descriptografia SSL estiver habilitada.

Entendendo o processo de detecção do Eicar

Para habilitar o bloqueio de eicar.org, habilite a descriptografia SSL.



Note: A Descriptografia SSL é necessária mesmo ao visitar o site por HTTP. Se a Descriptografia SSL não estiver habilitada, o proxy ignorará os domínios que atendem ao tráfego sobre HTTPS.

- O Umbrella Intelligent Proxy decide se deve enviar um domínio para o proxy na camada DNS.
- A solicitação DNS ocorre antes da conexão HTTP/HTTPS, o que significa que quando um domínio está sujeito ao proxy, o tráfego HTTP e HTTPS sempre é intermediado por proxy.
- Quando o tráfego HTTP/HTTPS chega ao nosso Proxy Inteligente, a primeira etapa é fazer um redirecionamento para identificar o usuário.

Esse redirecionamento não é possível sem a descriptografia SSL, o que significa que talvez não seja possível identificar corretamente os usuários em alguns cenários (como usuários móveis).

Para evitar que esses usuários interrompam solicitações HTTPS, o Umbrella não usa domínios de proxy (como eicar.org) que atendam ao tráfego HTTP/HTTPS, a menos que a descriptografia SSL esteja habilitada.

Em resumo...

Para obter a melhor segurança e eficácia do recurso, é altamente recomendável instalar o Cisco Root CA e habilitar a descriptografia SSL. Isso permite que os arquivos de teste eicar.org sejam bloqueados e aumenta o número de domínios que estão sujeitos à inspeção de arquivos por meio de nosso Proxy Inteligente.

Aqui está um resumo do comportamento esperado:

- Descriptografia SSL DESATIVADA
  - Os sites Eicar.org NÃO estão bloqueados em https://www.eicar.org/download/eicar.com. O domínio simplesmente não recebe proxy porque a descriptografia SSL está desabilitada.
  - Nosso próprio site de teste hospedando eicar está bloqueado: http://proxy.opendnstest.com/download/eicar.com
- Descriptografia SSL ATIVADA
  - Eicar bloqueado pela verificação de AV em http://www.eicar.org/download/eicar.com e https://www.eicar.org/download/eicar.com

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.