Controllo file di test con Eicar

Sommario

[Introduzione](#)

[Panoramica](#)

[Informazioni sul processo di rilevamento per Eicar](#)

[Riepilogo...](#)

Introduzione

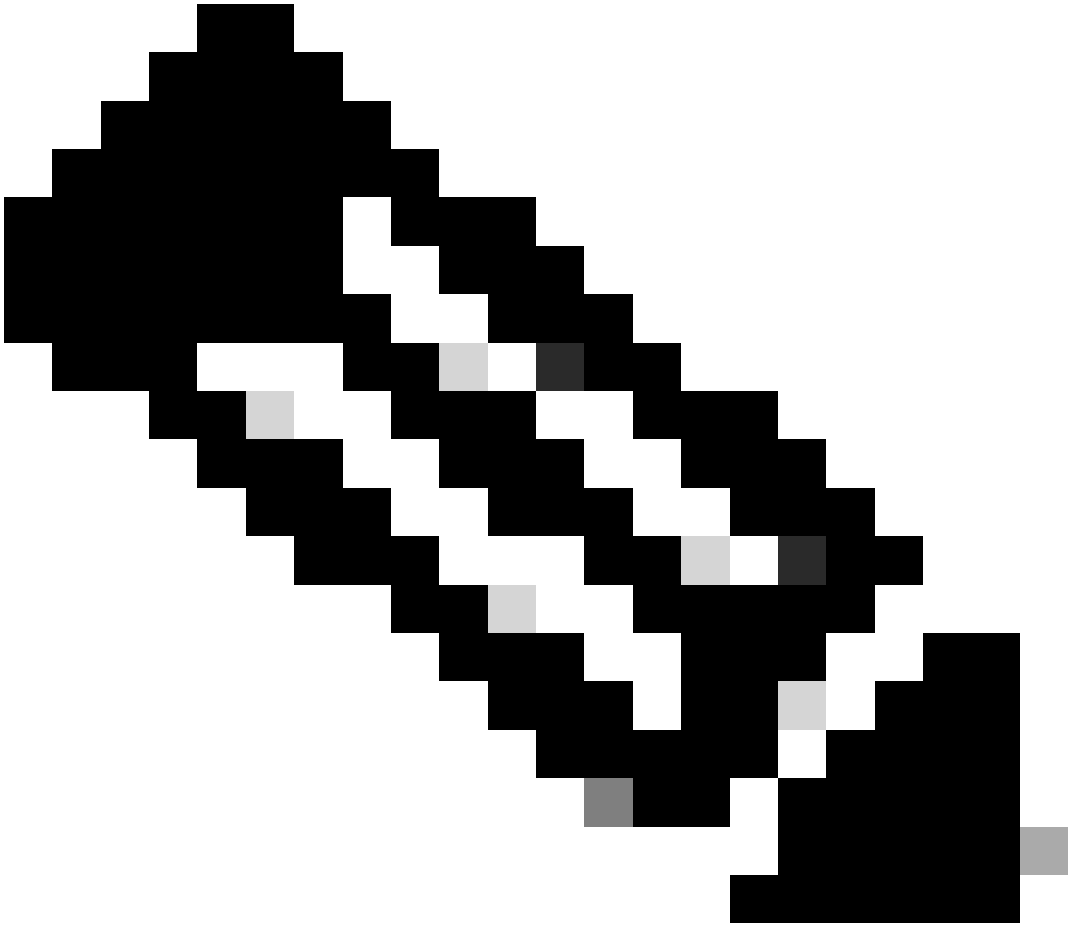
Questo documento descrive come testare l'ispezione dei file con Eicar.

Panoramica

Al momento, quando si verifica se la funzione di ispezione dei file è attivata o meno utilizzando i file di download dei test eicar.org, si riscontra un comportamento diverso quando la "decrittografia SSL" è attivata o disattivata. Solo Umbrella File Inspection esegue la scansione dei download su eicar.org se la decrittografia SSL è abilitata.

Informazioni sul processo di rilevamento per Eicar

Per abilitare il blocco di eicar.org, abilitare la decrittografia SSL.



Nota: La decrittografia SSL è necessaria anche quando si visita il sito tramite HTTP. Se la decrittografia SSL non è abilitata, il proxy ignora i domini che gestiscono il traffico su HTTPS.

- Il proxy intelligente Umbrella decide se inviare un dominio al proxy a livello DNS.
- La richiesta DNS si verifica prima della connessione HTTP/HTTPS, ovvero quando un dominio è soggetto al proxy, il traffico HTTP e HTTPS viene sempre trasmesso tramite proxy.
- Quando il traffico HTTP/HTTPS raggiunge il nostro proxy intelligente, il primo passo è effettuare un reindirizzamento per identificare l'utente.

Questo reindirizzamento non è possibile senza la decrittografia SSL, il che significa che potrebbe non essere possibile identificare correttamente gli utenti in alcuni scenari (ad esempio Utenti mobili).

Per impedire a questi utenti di interrompere le richieste HTTPS, Umbrella non utilizza domini proxy (come eicar.org) che servono sia il traffico HTTP che HTTPS, a meno che non sia abilitata la

decrittografia SSL.

Riepilogo...

Per ottenere la massima sicurezza ed efficacia dalla funzione, si consiglia di installare la Cisco Root CA e abilitare la decrittografia SSL. In questo modo, è possibile bloccare i file di test eicar.org e aumentare il numero di domini soggetti a ispezione dei file tramite il proxy intelligente.

Di seguito è riportato un riepilogo del comportamento previsto:

- Decrittografia SSL OFF
  - Eicar.org i siti NON sono bloccati all'indirizzo https://www.eicar.org/download/eicar.com. Il dominio non viene inserito nel proxy perché la decrittografia SSL è disabilitata.
  - Il nostro sito di test che ospita l'eicar è bloccato: http://proxy.opendnstest.com/download/eicar.com
- Decrittografia SSL ATTIVATA
  - Eicar bloccata dalla scansione AV sia su http://www.eicar.org/download/eicar.com che su https://www.eicar.org/download/eicar.com

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).