使用Eicar進行測試檔案檢查

目錄

簡介

概觀

瞭解Eicar的檢測流程

總結中……

簡介

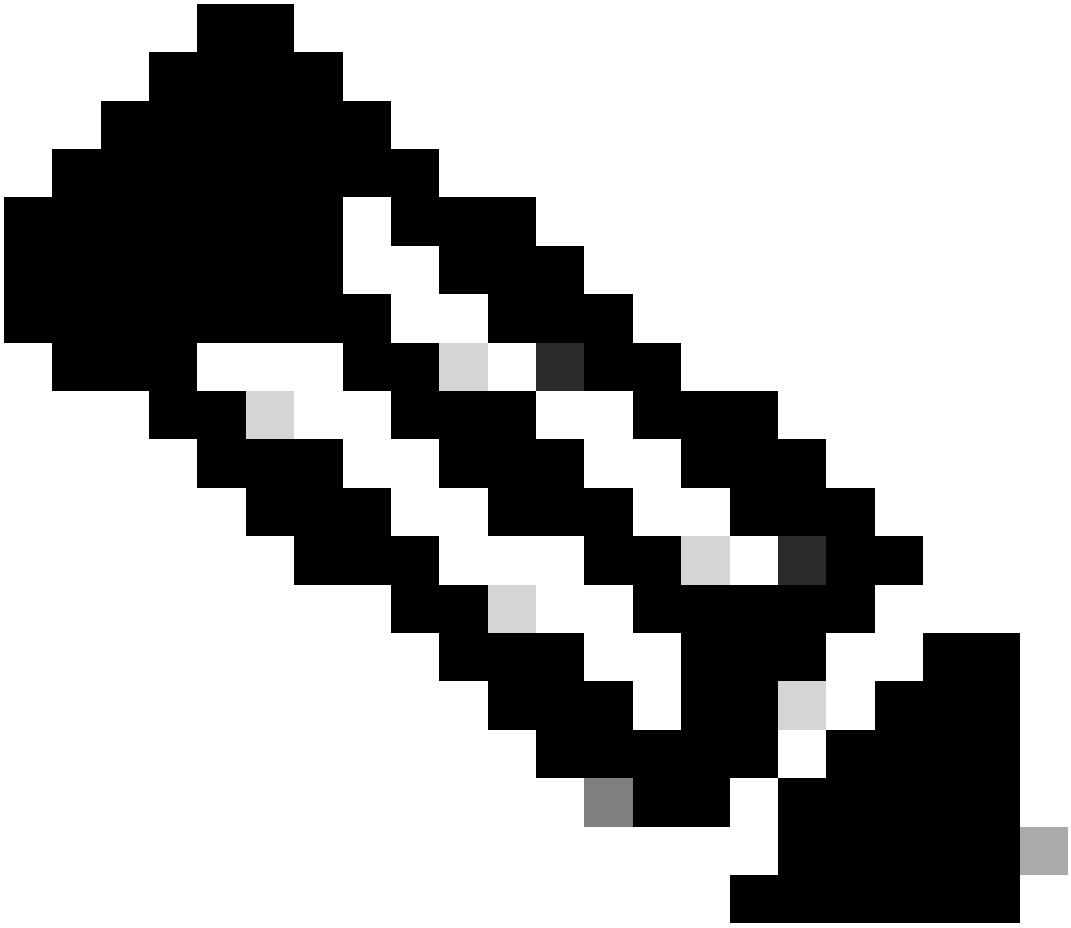
本文說明如何使用Eicar測試檔案檢查。

概觀

目前，使用eicar.org測試下載檔案測試是否啟用檔案檢查功能時，啟用或禁用「SSL解密」時，您會看到不同的行為。如果啟用SSL解密，則僅可在eicar.org下載Umbrella File Inspection AV掃描檔案。

瞭解Eicar的檢測流程

要啟用eicar.org的阻止，請啟用SSL解密。



附註：即使通過HTTP訪問站點，也需要SSL解密。如果您未啟用SSL解密，則代理會繞過透過HTTPS提供流量的網域。

- Umbrella智慧代理決定是否在DNS層將域傳送到Proxy。
- DNS請求發生在HTTP/HTTPS連線之前，這表示當域受代理作用時，HTTP和HTTPS流量總是被代理。
- 當HTTP/HTTPS流量到達我們的智慧代理時，第一步是進行重定向以識別使用者。

沒有SSL解密，則無法進行此重新導向，這表示在某些情景（例如漫遊使用者）中，我們可能無法正確識別使用者。

為防止這些使用者中斷HTTPS請求，除非啟用SSL解密，否則Umbrella不使用同時為HTTP/HTTPS流量提供服務的代理域(如eicar.org)。

總結中.....

為了從該功能獲得最佳安全性和有效性，我們強烈建議安裝思科根CA並啟用SSL解密。這允許

eicar.org測試檔案被阻止，並增加了通過智慧代理進行檔案檢查的域數。

以下是預期行為的摘要：

- SSL解密關閉
  - Eicar.org站點在https://www.eicar.org/download/eicar.com上未被阻止。因為SSL解密被禁用，所以根本就沒有代理域。
  - 我們自己的測試站點託管電子郵件被阻止：http://proxy.opendnstest.com/download/eicar.com
- SSL解密開啟
  - Eicar在http://www.eicar.org/download/eicar.com和https://www.eicar.org/download/eicar.com上被AV掃描阻止

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。