如何從面向終端的AMP門戶在Threat Grid中提交檔案？

目錄

簡介

本文檔介紹從面向終端的高級惡意軟體防護(AMP)終端門戶向Threat Grid(TG)雲提交樣本的過程。

作者：Yeraldin Sánchez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- 思科終端進階惡意軟體防護
- TG雲端

採用元件

本檔案中的資訊是根據思科終端進階惡意軟體防護主控台版本5.4.20190709。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

以下為本檔案所述情境的要求：

- 訪問面向終端的思科AMP入口網站
- 檔案大小不超過20MB
- 每天提交少於100次

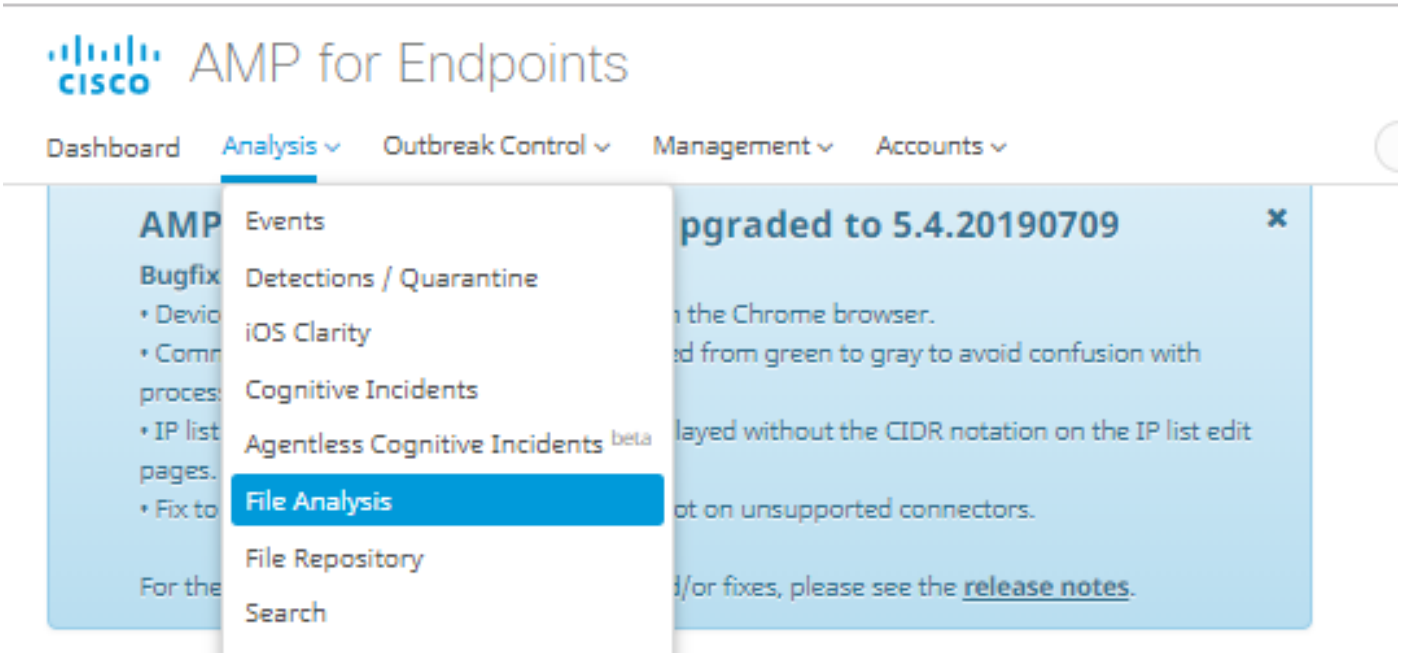
檔案分析限制：

- 檔名限製為59個Unicode字元。
- 檔案不能小於16位元組或大於20 MB
- 支援的檔案型別：**.exe、.dll、.jar、.swf、.pdf、.rtf、.doc(x)、.xls(x)、.ppt(x)、.zip、.vbn和.sep**

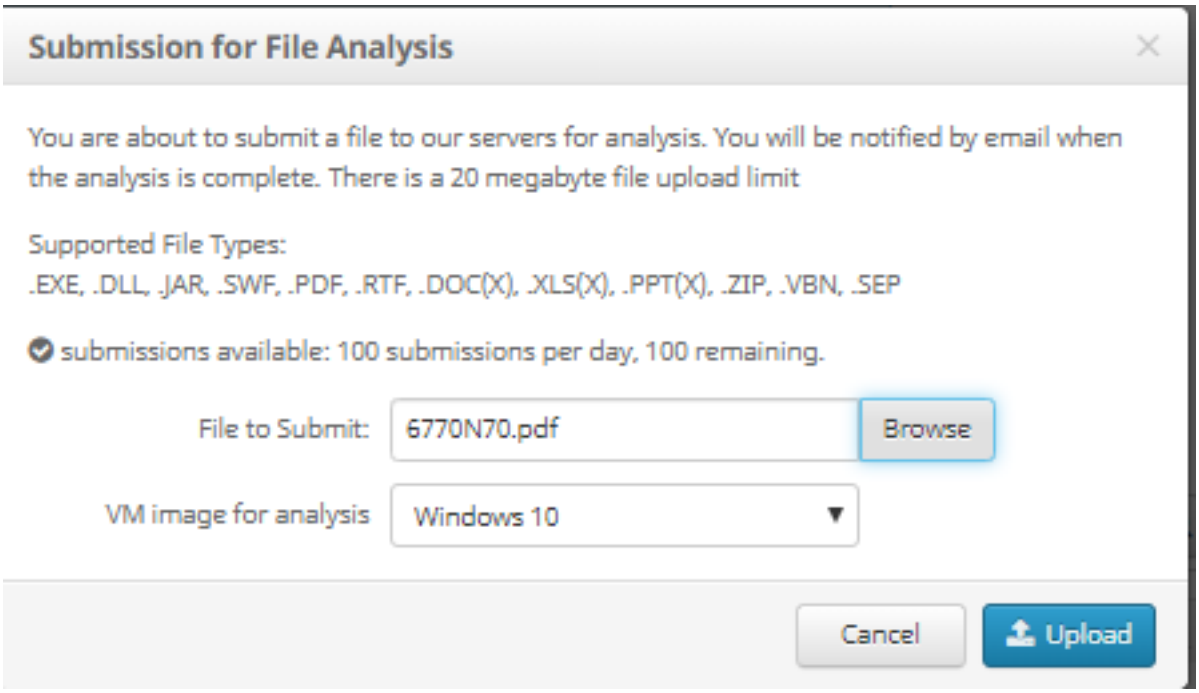
如何從面向終端的AMP門戶在Threat Grid中提交檔案？

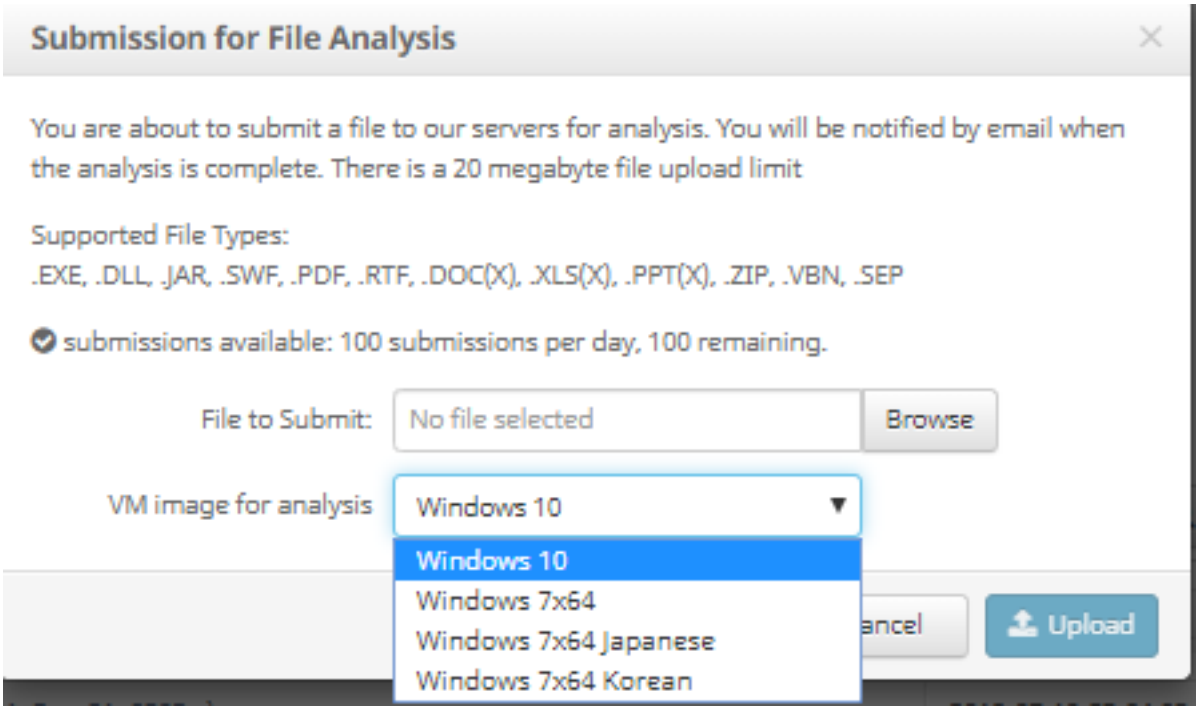
以下為從AMP門戶向TG雲提交示例時應遵循的步驟。

步驟1。在AMP入口上，導覽至**Analysis > File Analysis**，如下圖所示。



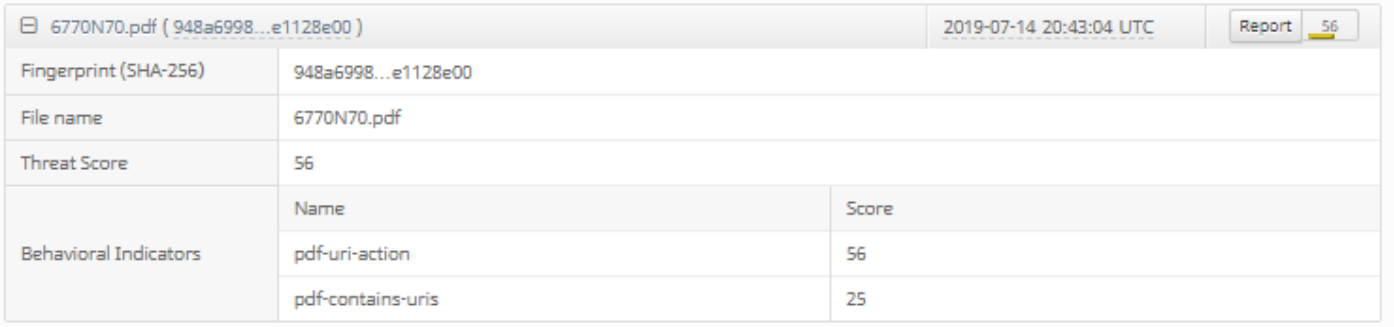
步驟2.選擇要傳送進行分析的檔案和Windows映像版本，如下圖所示。

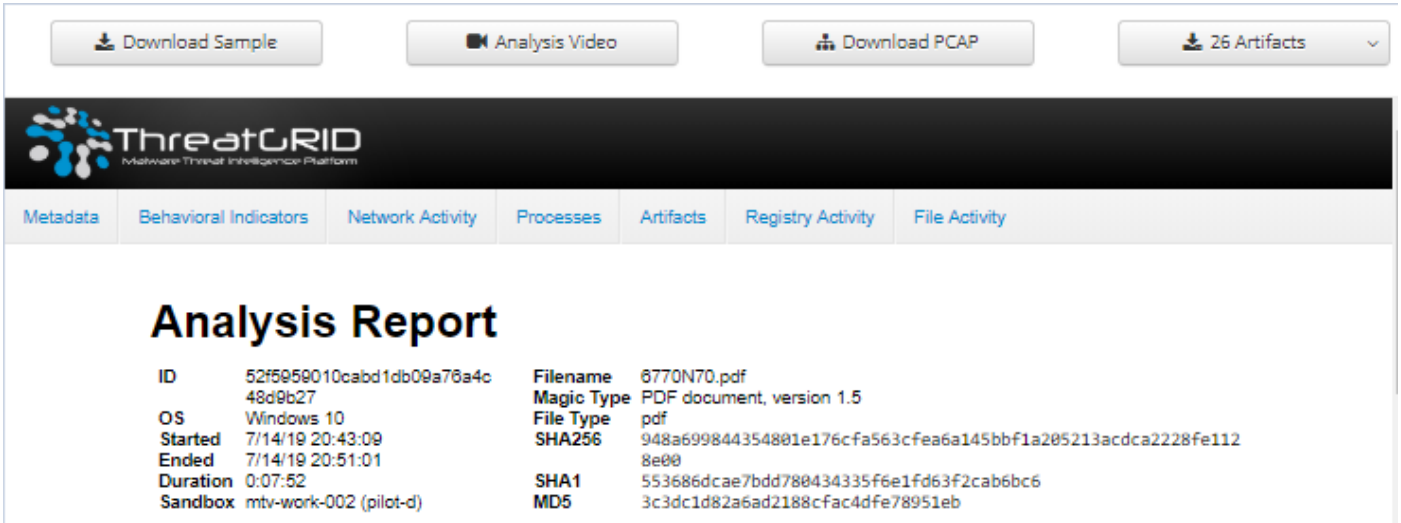




步驟3.在上傳示例後，分析大約需要30到60分鐘才能完成，具體取決於系統負載。在此過程完成後，將向您的電子郵件傳送電子郵件通知。

步驟4.檔案分析準備就緒後，按一下**Report**按鈕可獲得有關威脅評分的詳細資訊，如下圖所示。





若要瞭解更多資訊，可以查詢用於檔案分析的其他選項：

下載範例：此選項可讓您下載該示例。

分析影片：此選項提供在分析中獲得的示例影片。

下載PCAP:此選項提供網路連線分析。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

> **警告**：從「檔案分析」下載的檔案通常是即時惡意軟體，必須謹慎處理。

> **附註**：特定檔案的分析分為幾個部分。某些部分不能適用於所有檔案型別。

相關資訊

- 面向終端的思科AMP — 使用手冊
- 技術支援與文件 - Cisco Systems