解決面向終端的AMP中的誤報檔案分析問題

目錄

簡介

本文描述如何在面向終端的高級惡意軟體防護(AMP)中收集誤報檔案分析。

作者：Jesus Javier Martinez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- AMP控制檯控制面板
- 具有管理員許可權的帳戶

採用元件

本檔案中的資訊是根據適用於終端的Cisco AMP版本6.X.X及更新版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

面向終端的AMP可能針對特定檔案/進程/安全雜湊演算法(SHA)256生成過多警報。如果您懷疑網路中存在任何誤報檢測，您可以聯絡思科技術支援中心(TAC)，診斷團隊會繼續做更深入的檔案分析

。當您聯絡思科TAC時，您需要提供以下資訊：

·檔案SHA 256雜湊
·檔案示例複製
·從AMP控制檯捕獲警報事件
·從AMP控制檯捕獲事件詳細資訊
·有關檔案的資訊（檔案來自何處，以及為何需要存在於環境中）
·解釋為什麼您認為檔案/進程可能是誤報

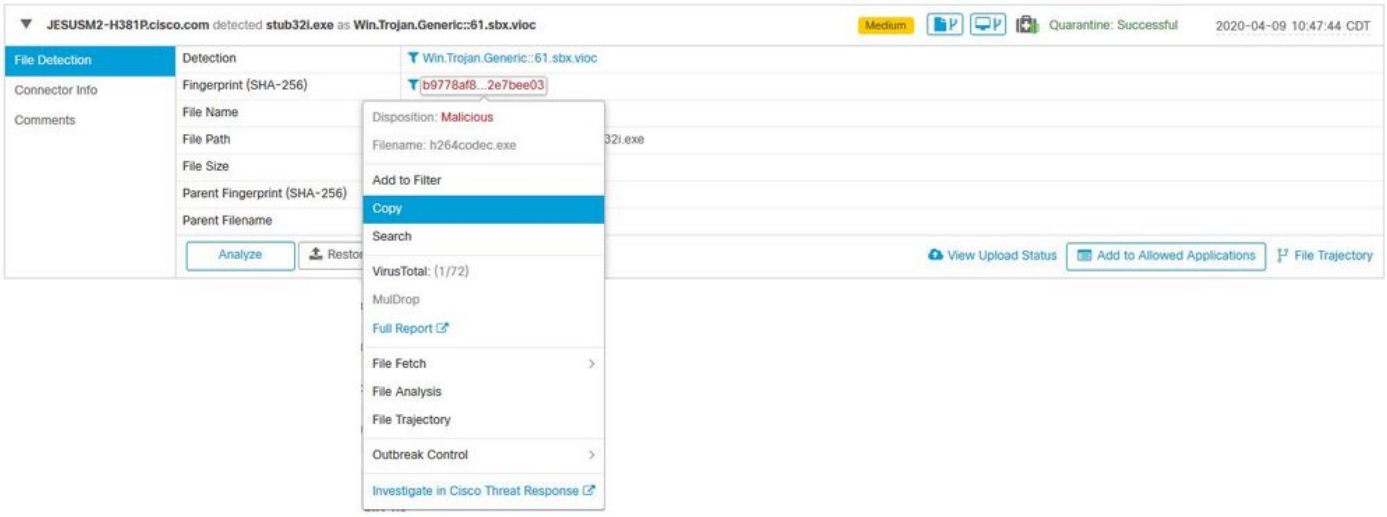
對面向終端的AMP中的誤報檔案分析進行故障排除

本節提供的資訊可用於獲取使用Cisco TAC開啟誤報票證所需的全部詳細資訊。

檔案SHA 256雜湊

步驟1。若要獲取SHA 256雜湊，請導覽至**AMP Console > Dashboard > Events。**

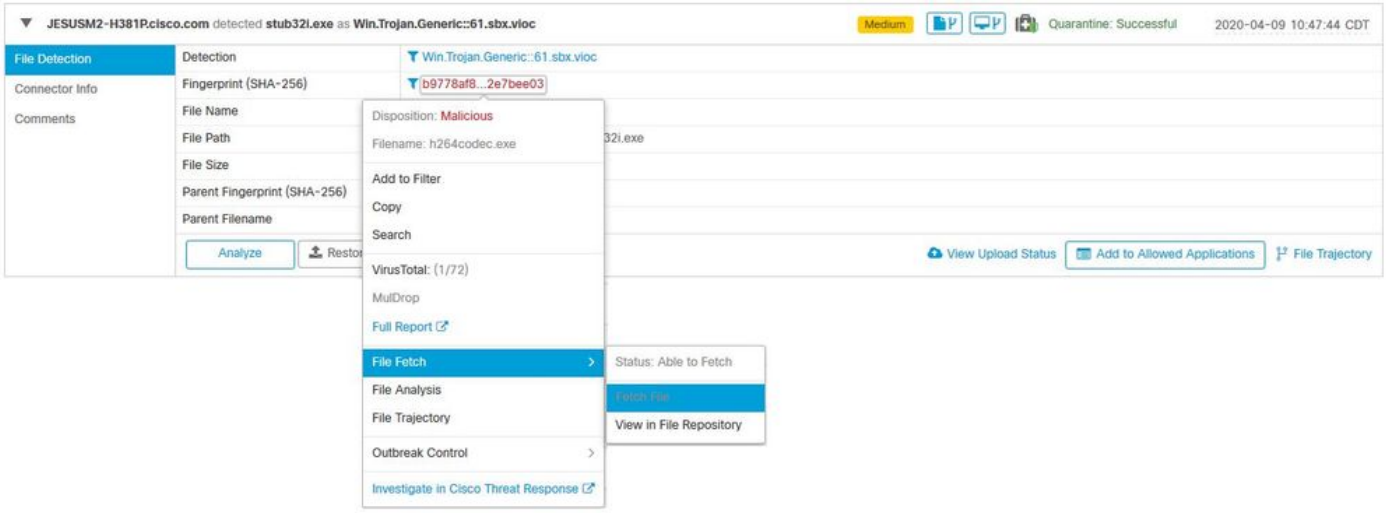
步驟2.選擇**Alert Event**，按一下**SHA256**，然後選擇**Copy**，如下圖所示。



檔案示例副本

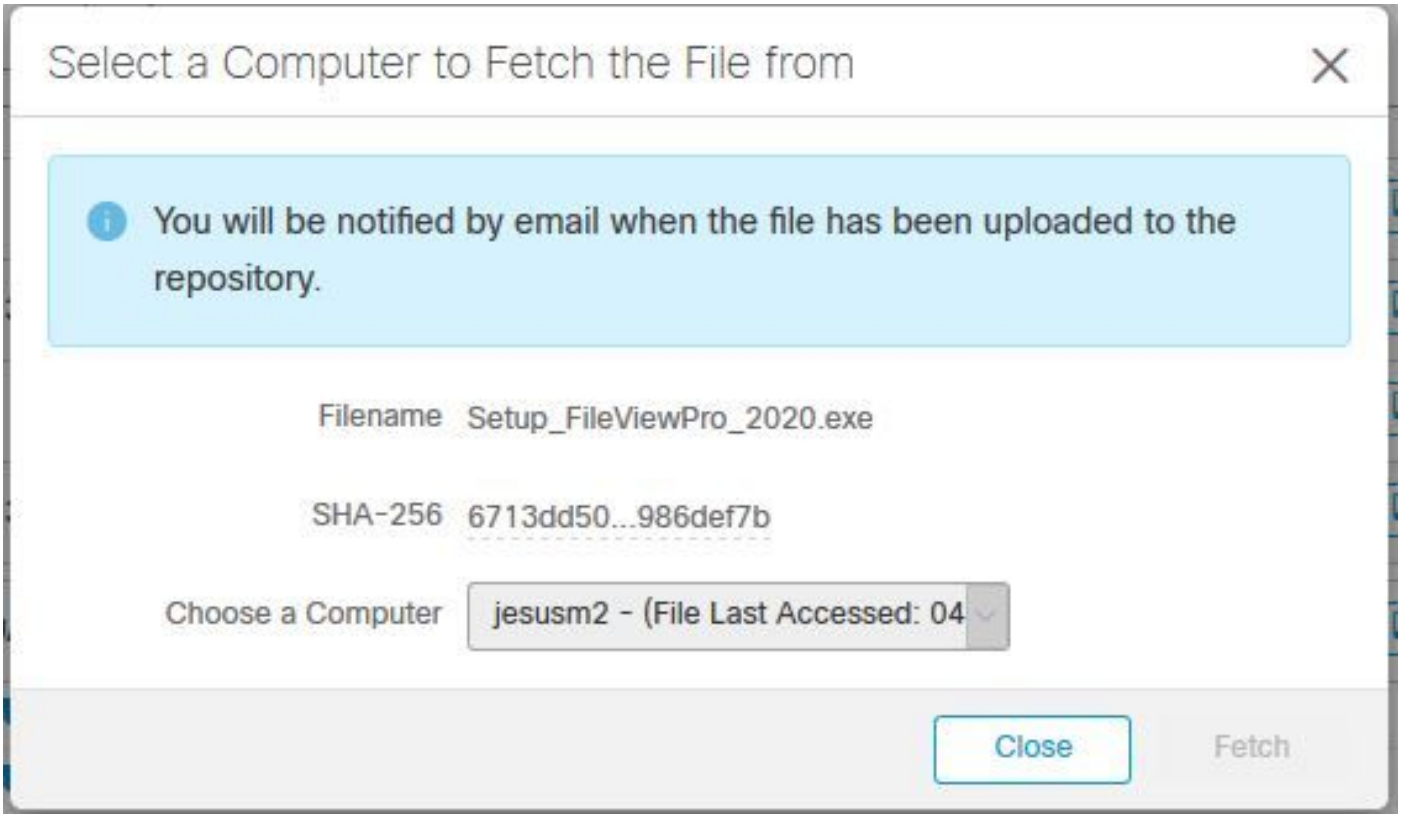
步驟1。您可以從AMP控制檯獲取檔案示例，導航到**AMP控制檯>**控制**板>**事件**。**

步驟2.選擇**Alert Event**，按一下**SHA256**，然後導覽至**File Fetch> File Fetch**，如下圖所示。

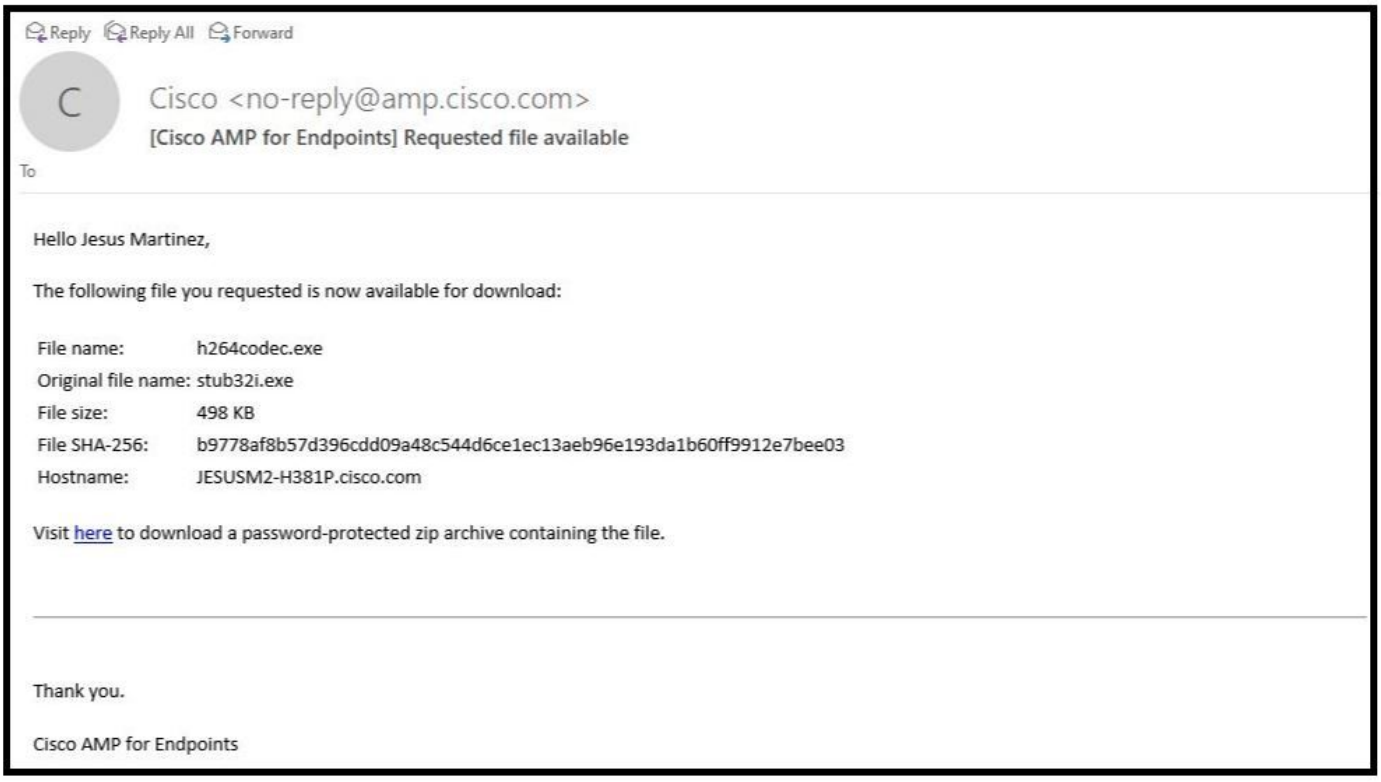


步驟3.選擇偵測到檔案的裝置，然後按一下**Fetch**，如下圖所示(裝置必須開啟),如圖所示。

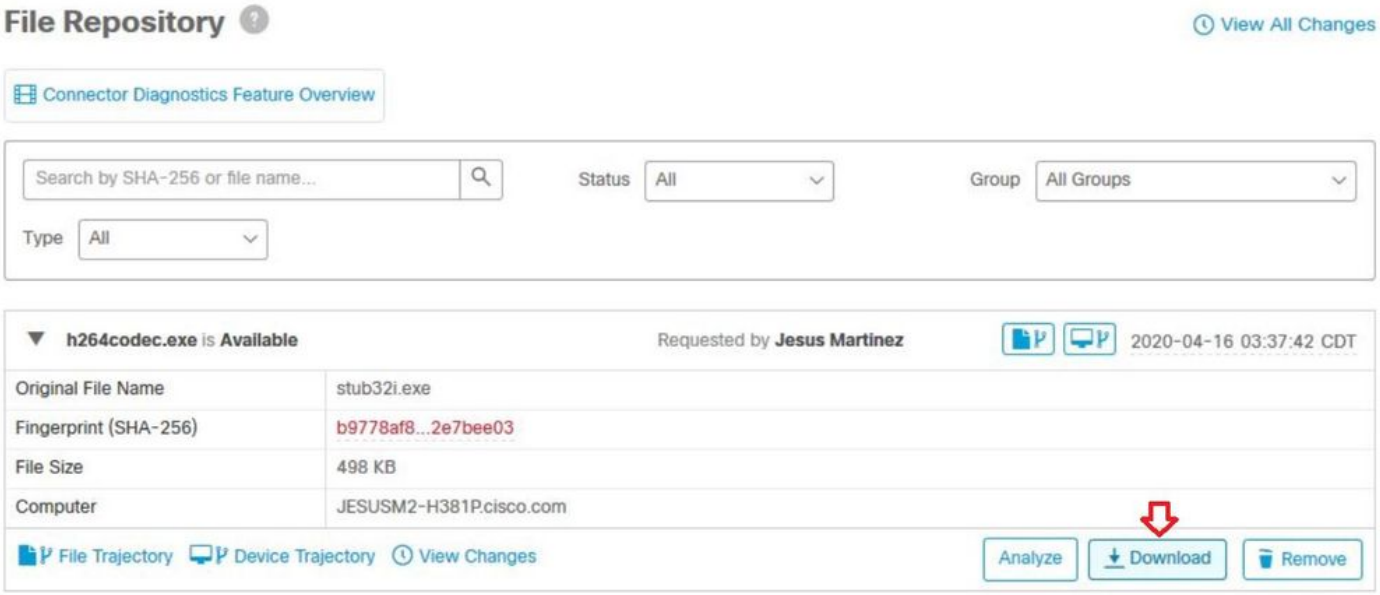
步驟4.您會收到如下圖所示的訊息。



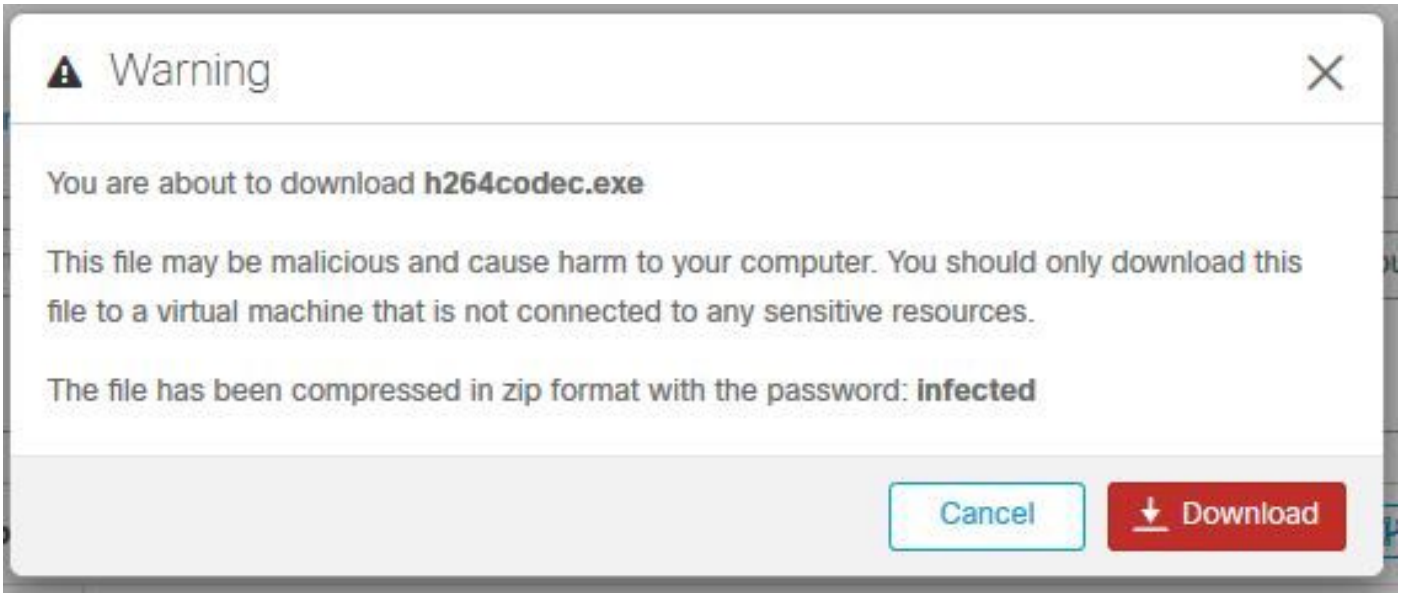
幾分鐘後，檔案可供下載時，您會收到電子郵件通知，如下圖所示。



步驟5.導覽至**AMP Console > Analysis > File Repository**，然後選擇檔案並按一下**Download**，如下圖所示。



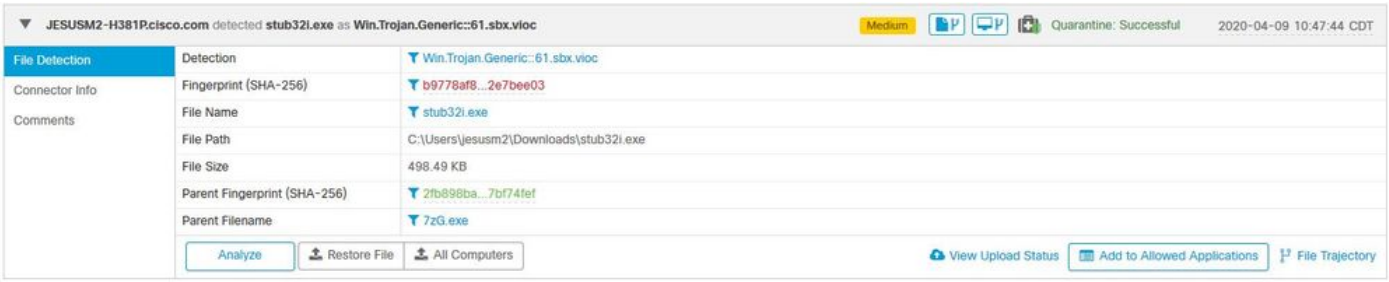
步驟6.出現通知框，按一下**Download**，如下圖所示，並將檔案下載到ZIP檔案中。



從AMP控制檯捕獲警報事件

步驟1.導航到**AMP控制檯>控制面板>事件。**

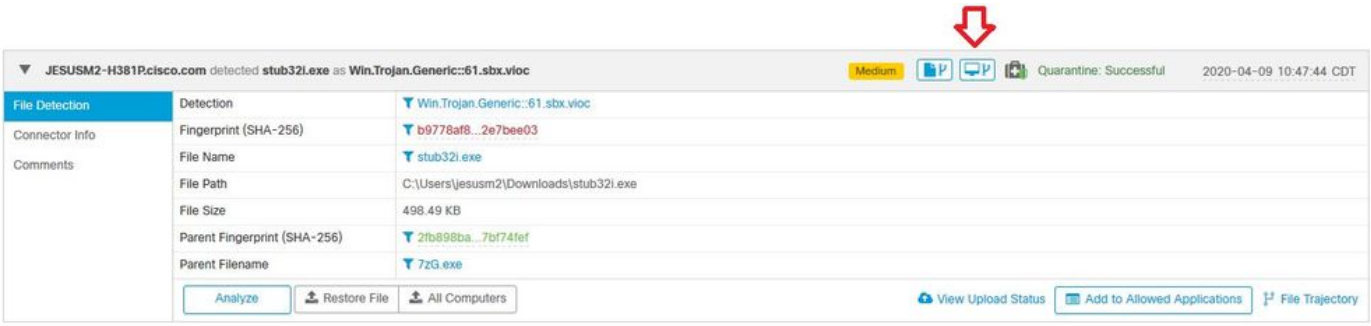
步驟2.選擇**Alert Event**，然後進行捕獲，如下圖所示。



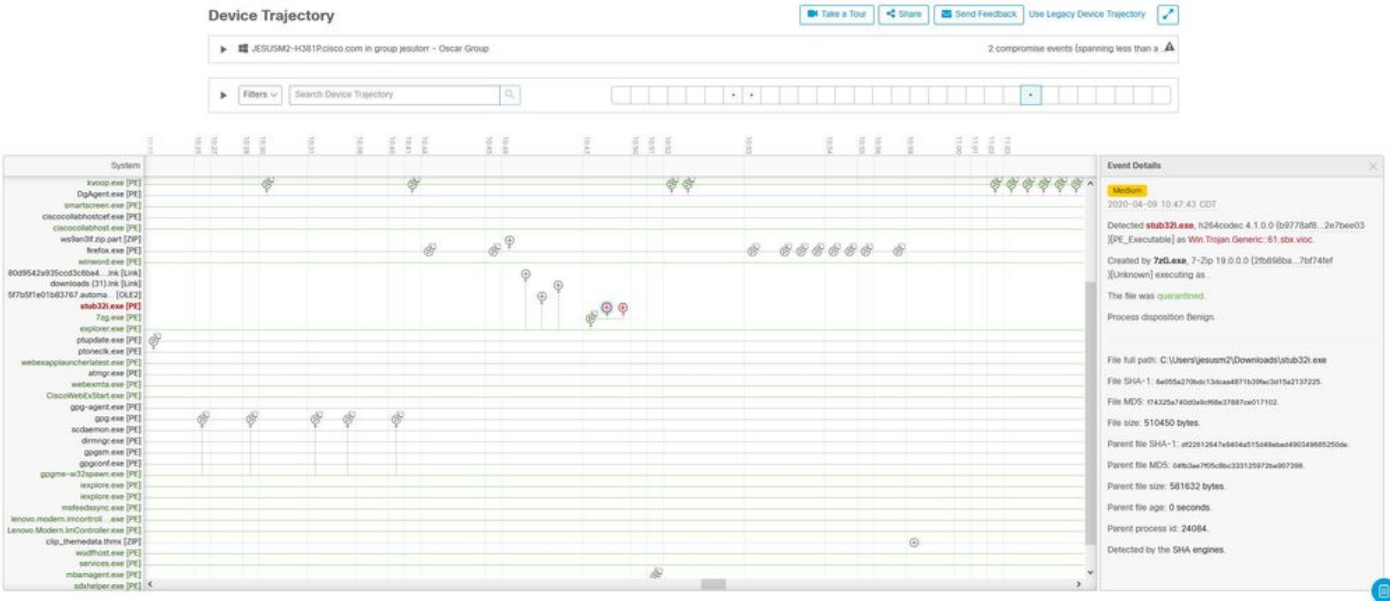
從AMP控制檯捕獲事件詳細資訊

步驟1.導航到**AMP控制檯>控制面板>事件。**

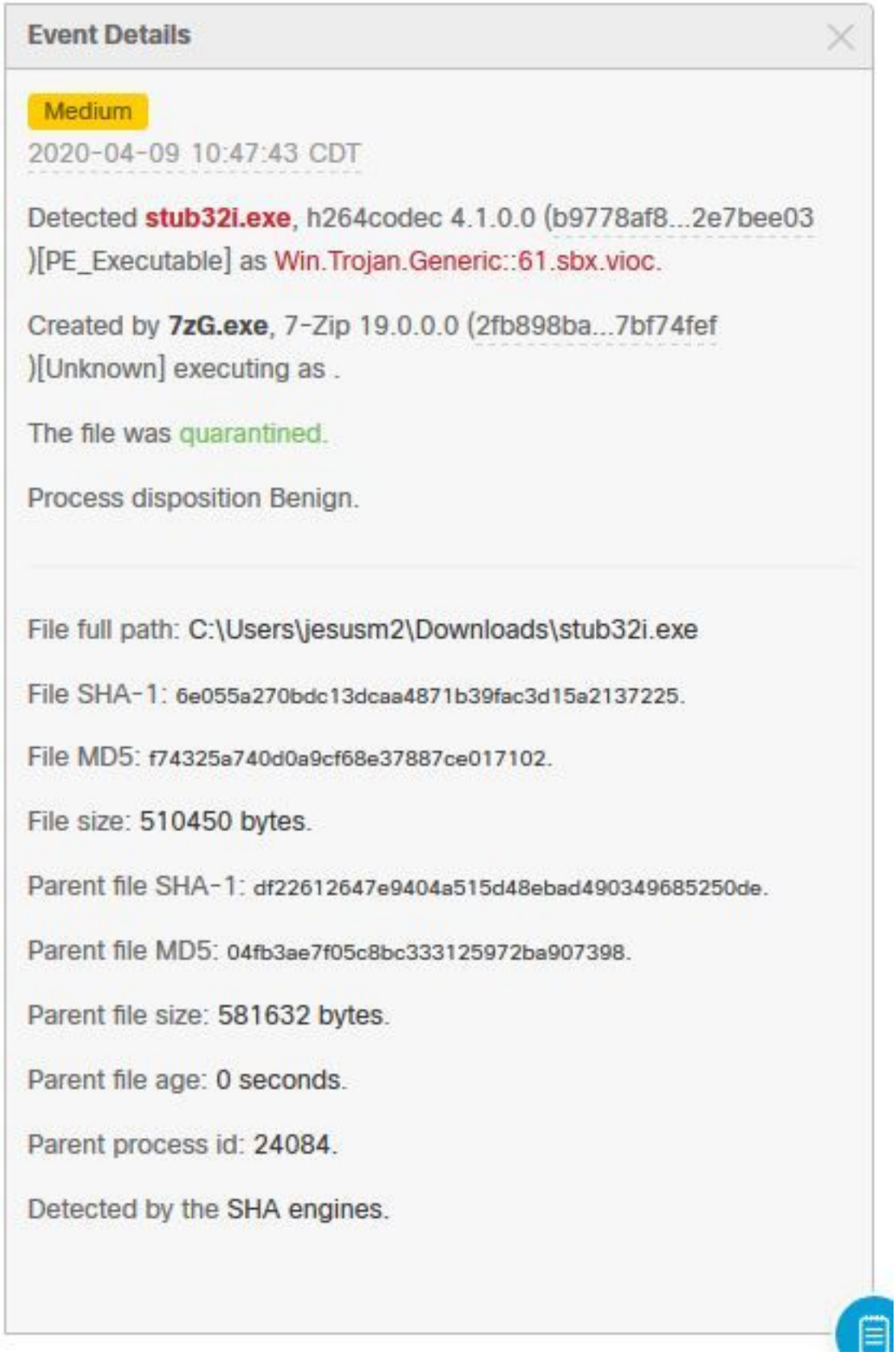
步驟2.選擇Alert Event（警報事件）並按一下**Device Trajectory**選項，如下圖所示。



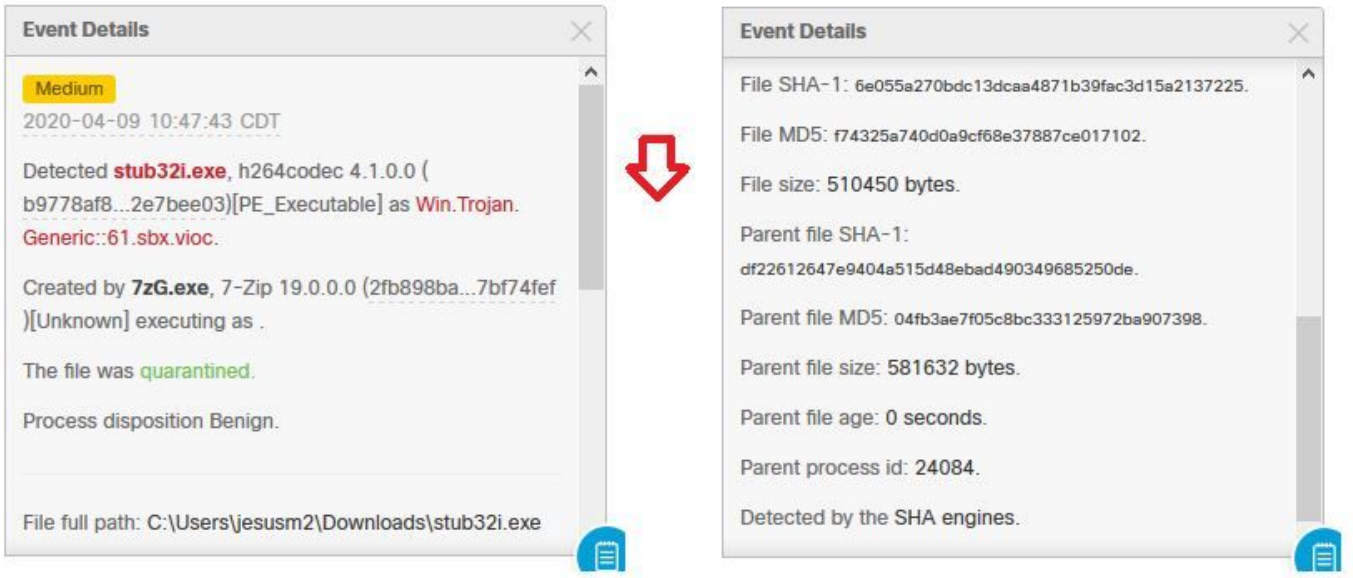
它重定向至**裝置軌跡**詳細資訊，如下圖所示。



步驟3.捕獲**Event Details**框，如下圖所示。



步驟4.如有必要，請向下滾動並擷取一些捕獲，獲得所有**Events Details**資訊，如下圖所示。



有關檔案的資訊

- 有關檔案來源的資訊。
- 如果檔案來自網站，請共用Web URL。
- 共用一些檔案說明並解釋檔案功能。

說明

- 為什麼您認為檔案過程可能是誤報？
- 分享您信任檔案的原因。

提供資訊

- 收集所有詳細資訊後，將請求的所有資訊上傳到https://cway.cisco.com/csc/。
- 確保引用服務請求編號。

結論

思科始終致力於改進和擴展面向終端的AMP的威脅情報技術，但是，如果您的面向終端的AMP解決方案錯誤地觸發了警報，則您可以採取一些措施以防止對您的環境造成任何進一步的影響。本文提供原則，以取得與Cisco TAC就誤報問題建立案例所需的所有詳細資訊。根據診斷團隊檔案分析，檔案處置可以更改以停止AMP控制檯上觸發的警報事件，或者Cisco TAC可以提供正確的修復程式，讓運行檔案/進程時不會在您的環境中出現問題。