[外部] — 使用高級惡意軟體防護(AMP)進行虛假檢測、爆發和事件響應

目錄

簡介

我們始終致力於改進和擴展高級惡意軟體防護(AMP)技術的威脅情報，但是，如果您的AMP解決方案未觸發警報或錯誤觸發警報，則您可以採取一些操作來防止對環境造成任何進一步的影響。本檔案為這些行動事項提供了指南。

說明

立即行動

如果您認為AMP解決方案無法保護您的網路免受威脅，請立即採取以下措施：

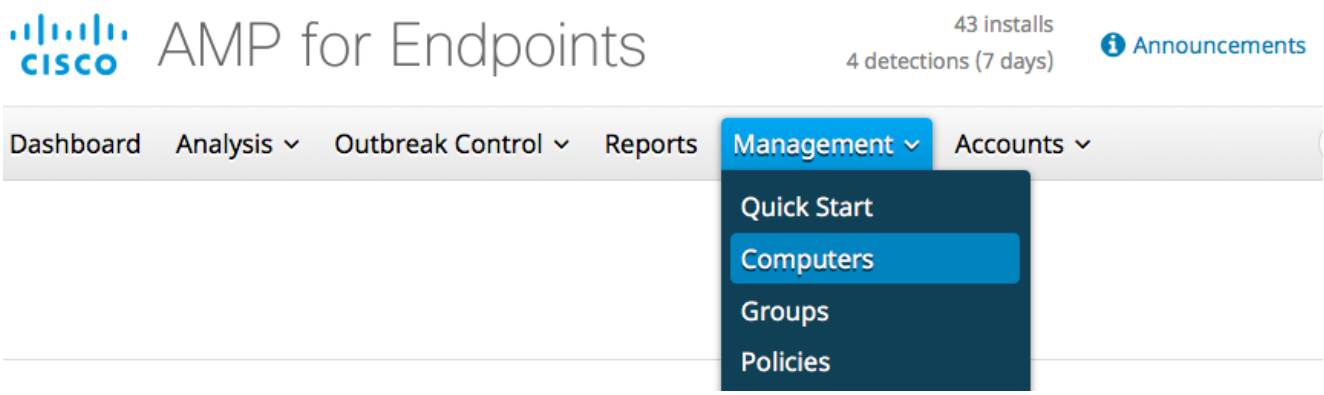
1. 將可疑電腦與網路的其餘部分隔離。這可能包括關閉電腦，或者從物理上斷開電腦與網路的連線。
2. 寫下感染的重要資訊，例如電腦受到感染的時間，可疑電腦上的使用者活動等。

   警告：不要擦除或重新映像電腦。它可消除在取證調查或故障排除過程中發現違規軟體或檔案的機會。

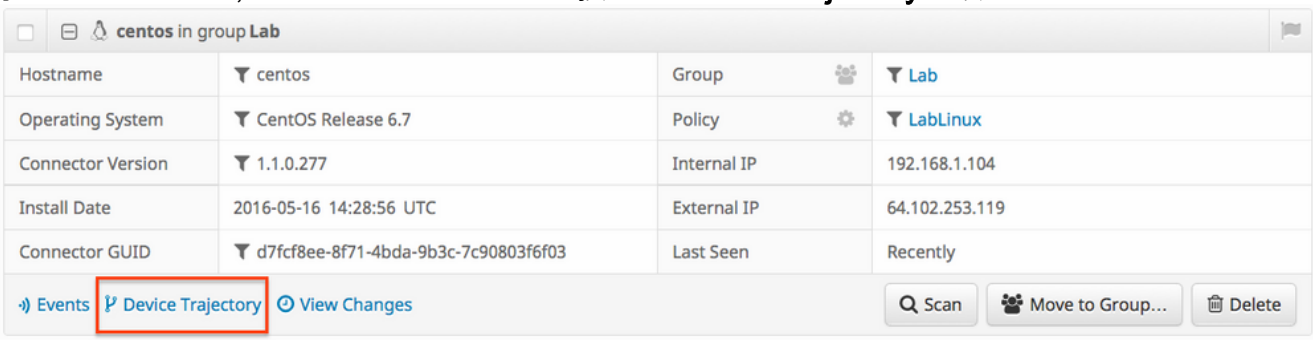
分析

1. 使用**Device Trajectory**功能開始您自己的調查。Device Trajectory能夠儲存大約9百萬個最新的檔案事件。面向終端的AMP裝置軌跡在跟蹤導致感染的檔案或進程時非常有用。

   在控制面板中，導航到**管理>電腦**。



找到可疑的電腦，並展開該電腦的記錄。按一下**Device Trajectory**選項。



2. 如果發現任何可疑檔案或雜湊，請將其新增到自定義檢測清單中。面向終端的AMP可以使用自定義檢測清單將檔案或雜湊視為惡意檔案。這是提供停止間隔覆蓋以防止進一步影響的好方法。

思科分析

1. 提交任何可疑樣本以進行動態分析。您可以手動從儀表板中的**分析>檔案分析**中提交這些樣本。面向終端的AMP包含動態分析功能，可生成來自Threat Grid的檔案行為報告。如果我們的研究團隊需要進行其他分析，則這也有利於將檔案提供給思科。

2. 如果您懷疑網路中存在*false-positive*或*false-*檢測，建議您對AMP產品使用自定義黑名單或白名單功能。當您聯絡思科技術協助中心(TAC)時，請提供以下資訊進行分析：檔案的SHA256雜湊。如果可能，提供檔案的副本。有關檔案的資訊，例如檔案的來源以及檔案需要位於環境中的原因。解釋您為什麼認為此錯誤為正或負結果。
3. 如果您需要緩解威脅或執行環境分類方面的幫助，您需要聯絡Cisco Talos事件響應(CTIR)團隊，該團隊專門負責制定行動計畫、研究受感染機器並利用高級工具或功能來緩解活動病毒爆發。
   附註：思科技術協助中心(TAC)不提供此類專案的協助。可在此處聯絡CTIR。這是一項收費服務，起價為60,000美元，除非您的組織有思科提供的事件響應服務定金。參與後，他們將提供有關其服務的其他資訊，並針對您的事件建立案例。我們還建議與您的思科客戶經理進行進一步溝通，以便他們能夠提供有關這一過程的更多指導。

相關文章

- WindowsFireAMP
- FireAMP