瞭解Umbrella中的潛在有害安全類別

目錄

簡介

本檔案介紹Cisco Umbrella中的「潛在有害」安全類別。

必要條件

需求

本文件沒有特定需求。

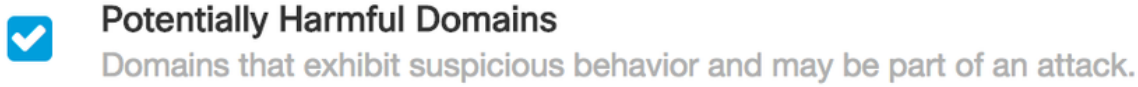
採用元件

本檔案中的資訊是根據Cisco Umbrella。

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。

概觀

Umbrella客戶在安全方面的風險容忍級別不同。根據您從事的工作的行業和型別，主動監控和阻止潛在有害活動是有益的。新的「可能有害的」安全設定可在「其他安全設定」旁邊的Prevent下找到，預設設定為Allow:



115011476788

詳細資料

潛在危害是一個安全類別，其中包含可能為惡意的域。它不同於Umbrella的「惡意軟體」類別，因為Umbrella對這些惡意軟體是否真正具有惡意性的信心較低。另一種說法是，根據我們的研究分析人員，以及我們用於確定整體但並不一定為惡意的演算法，這些域被視為可疑。

此類別的使用取決於您對阻止可能良好的域的風險的容忍度。如果您有一個高度安全的環境，這是一個要阻止的良好類別；如果您的環境更鬆散，您只需允許和監視即可。

如果您不確定您屬於哪一種，可以監控報告中被確認為「潛在危害」的活動。提供此類別可以在流量分類、提高可視性、提供更強保護和改進事件響應方面提供更精細的粒度。 例如，如果您認為某個電腦感染了惡意軟體，則檢視其訪問的潛在有害域可以幫助您更好地評估危害程度。

Umbrella通過權衡多個因素來確定「潛在有害」的內容，這些因素表明儘管域並非明顯惡意的，但可能會造成威脅。例如，有各種型別的DNS隧道服務。其中有些服務屬於良性、惡意和DNS隧道VPN類別，但有些服務則不太清楚，不屬於這些類別中的任何一個。如果隧道的使用情形未知且可疑，則目標可能屬於「潛在危害」類別。

另一個例子來自Umbrella的Spike等級模型。Umbrella的Spike排名模型利用大量DNS請求資料，並使用聲波圖檢測其DNS請求模式中存在峰值點的域。在Spike等級域中達到高位的流量可自動歸類為惡意流量，閾值較低的流量可歸入潛在有害類別。

要報告以下任一類別中的不需要的檢測，請執行以下操作：

- 請通過Talos支援向Cisco Talos提交所有資料分類請求。
- 有關向Cisco Talos提交請求的一般步驟，請參閱如何：提交分類請求。

對於潛在有害類別，Umbrella不會將其重新歸類為安全，除非保證該域絕對合法。

與任何其他安全類別一樣，這兩種類別都可以在報告中進行過濾。

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）。