# Cisco WSA勒索軟體檢測功能和AMP整合驗證

## 目錄

## 問題

詢問思科安全網路裝置(WSA)是否為Triple X勒索軟體提供特定簽名或檢測功能。此問題還包括請求澄清如何驗證高級惡意軟體防護(AMP)與Cisco Talos威脅情報之間的整合是否在WSA平台上正常運行。

## 環境

- Cisco Secure Web Appliance (WSA)
- 進階惡意軟體防護(AMP)整合
- Cisco Talos威脅情報整合
- Web聲譽和URL篩選(WBRS)
- 防惡意軟體掃描引擎(Webroot、McAfee、Sophos)
- Application Visibility and Control (AVC)

## 解析

思科安全網路裝置不依賴於一個專門命名為Triple X勒索軟體的專用簽名。相反，WSA採用全面的多層安全架構，利用各種檢測技術來識別和阻止勒索軟體威脅，包括Triple X勒索軟體變體。

WSA檢測方法

WSA平台使用以下檢測技術保護勒索軟體：

- 模式匹配演算法
- 啟發式分析
- 模擬技術
- 與思科Talos威脅智慧整合的高級惡意軟體防護(AMP)
- Web聲譽和URL篩選(WBRS)
- 多個防惡意軟體掃描引擎，包括Webroot、McAfee和Sophos
- Application Visibility and Control (AVC)

這些檢測功能會持續更新，每隔幾分鐘就會部署新的規則，以確保防禦新興威脅。

## 檢驗AMP和Talos整合

要確認高級惡意軟體防護(AMP)與Cisco Talos威脅情報之間的整合在WSA上是否正常工作，管理員可以檢視以下日誌：

步驟 1:檢視WSA訪問日誌

檢查WSA裝置上的訪問日誌，驗證AMP裁決是否應用於下載的檔案和Web請求。

步驟 2:檢查AMP日誌

檢視AMP日誌，確認正在處理的惡意軟體分析結果和威脅情報資料。

步驟 3:驗證WBRS得分

確保正在填充Web聲譽(WBRS)分數，並且這些分數與日誌中的Web請求相關聯。

如果在日誌中填充並強制執行AMP判定和WBRS分數，這表示AMP和Talos整合正在按預期運行，並提供基於威脅情報的即時決策。

## 原因

這是有關WSA勒索軟體檢測功能的資訊請求，而不是需要故障排除的技術問題。該調查是為了瞭解WSA如何針對特定勒索軟體變體提供保護，以及驗證威脅情報整合是否正常運行。

## 相關內容

- Cisco Secure Web Appliance的功能和優點
- Cisco Talos威脅情報服務
- 思科安全Web裝置資料表
- 思科技術支援與下載

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）。