



保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

SEP提供行動裝置的中間人 (MITM) 攻擊防護

2023年4月24日發布

[點擊此處可獲取--最完整的賽門鐵克解決方案資訊](#)

中間人 (MITM) 攻擊是近期熱門的網路攻擊模式之一，通訊雙方之間的通訊被攔截並可能被竄改，同時使其看起來好像正在進行正常的訊息交換。MITM 攻擊通常主要在竊取資訊，但也可能有其他意圖，例如：監視受害者、破壞通訊或破壞資料。

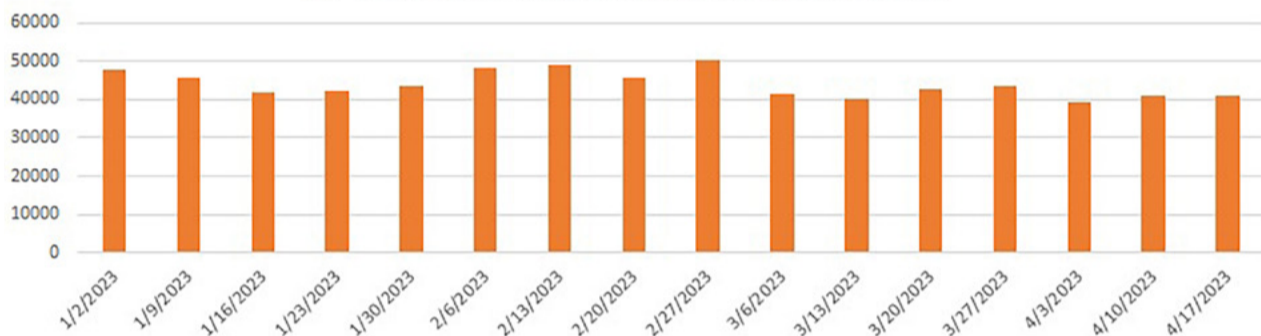
隨著越來越多的人使用行動裝置進行銀行、購物和存取敏感資料等線上活動，行動裝置上的 SSL MITM 攻擊變得越來越猖獗。公共 Wi-Fi 網路的廣泛使用更是助長這些攻擊，這些網路通常不安全且容易被攔截，駭客經常利用未經修補被廣泛運用於保護傳輸安全的 SSL/TLS 網路加密協議進行攻擊。

簡而言之，行動裝置上的 SSL 中間人 (MITM) 攻擊的工作原理如下：

- * 攻擊者設置一個假的 Wi-Fi 熱點或一個惡意模仿合法熱點的熱點
- * 受害者連接到假熱點並開始瀏覽網際網路或存取線上服務
- * 當受害者存取安全網站時，攻擊者攔截 SSL/TLS 流量並與受害者行動裝置建立假的 SSL/TLS 連接
- * 攻擊者充當受害者設備和伺服器之間的代理，攔截和解密加密流量
- * 攻擊者現在可以讀取和修改受害者裝置和伺服器之間的流量
- * 攻擊者可以竊取敏感訊息，例如登錄憑證、信用卡號或個人資料
- * 攻擊者可以竄改流量並將惡意程式碼或惡意軟體注入通訊流，進一步駭入受害者的裝置

下圖顯示今年以來 SEP 行動裝置版本所攔截到 SSL 中間人 (MITM) 攻擊的走勢。

SEP 行動裝置版本所攔截到的 SSL 中間人 (MITM) 攻擊統計



SEP 行動裝置版本透過以下防護技術有效防護中間人 (MITM) 攻擊：

- 主動蜜罐誘捕技術徹底分析端到端的網路連接以確保通訊安全
- 當 SEP 行動裝置版本檢測到 MITM 網路攻擊時，會同時發生兩件事：
 - 我們的自動網路保護回應啟動，包括從行動裝置透過安全的 VPN 連線或阻止行動裝置存取敏感的公司資源（電子郵件、營運類應用程式）等機制
 - 資安管理員和終端使用者都會收到有關威脅的警報，警報包括攻擊中涉及的證書和網路事件的詳細資訊

賽門鐵克的端點安全企業版 (SESE) / 端點安全完整版 (SESC) 內含防護 IOS / Android 的最先進防護技術，[請點擊此處](#)瀏覽更完整的資訊。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom, 美國股市代號 AVGO, 全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED), 特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系, 讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性, 有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者, 致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝, 同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案, 近三年 Symantec 很少出現在由公關機制產生的頭版文章中, 而且在全球前兩大企業的市佔率及營收成長均遠遠高於併入博通之前, 增長幅度也領先其他競爭對手, 是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證, 也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司, 組合國際電腦 (CA Technologies) 以及雲端運算及「硬體虛擬化」的領導廠商--VMware, 也是博通軟體事業部的成員)。2021 年八月, 因應國外發動的針對性攻擊日益嚴重, 美國網路安全暨基礎架構安全管理署 (CISA) 宣布聯合民間科技公司, 發展全國性聯合防禦計畫 JCDC (Joint Cyber Defense Collaborative), 而博通賽門鐵克是首輪被徵招的一線廠商, 如就地緣政治考量, Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商, 被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務, 特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上, 以及基於比原廠更熟悉用戶環境的優勢能提供更快速有效的技術支援回應, 深獲許多中大型企業與組織的信賴, 長期合作的意願與滿意度極高。保安資訊連絡電話: 0800-381-500。

業界公認 保安資訊--賽門鐵克解決方案專家
 We Keep IT Safe, Secure & Save you Time, Cost

服務電話: 0800-381500 | +886 4 23815000 | <http://www.savetime.com.tw>