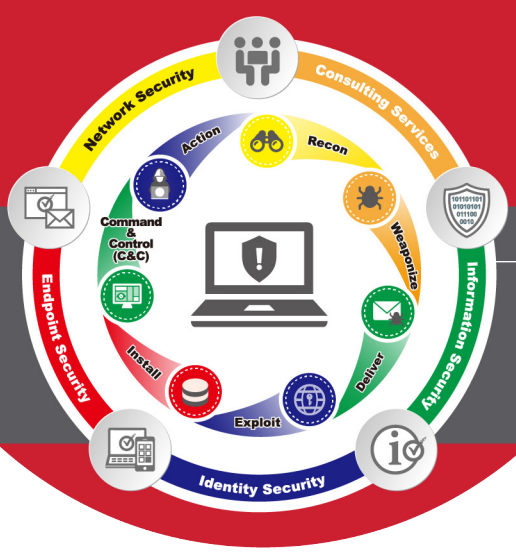


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

運用賽門鐵克端點偵測與回應(EDR)防護技術阻斷長期埋伏的進階持續威脅(APT)與勒索軟體威脅

2025 年 8 月 26 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

為了在受害者環境中長期維持立足點，攻擊者運用持久性／常駐技術--這類方法目的在確保即使系統重新開機、憑證變更或防禦行動發生，仍能維持不中斷的存取權限。透過具有持久性的能力，攻擊者得以延長其存活的時間，進而竊取資料、進行間諜活動，並在網路中橫向移動。

對攻擊者而言，持久性／常駐是貫穿整個入侵過程的基石戰術。對防禦者來說，偵測並清除這些企圖對於防止長期入侵非常重要。 持久性之所以重要，在於它能：

- 實現長期隱蔽存取
- 支援隱蔽的資料收集與間諜活動
- 增加偵測與應對的複雜性
- 促進環境內的橫向移動

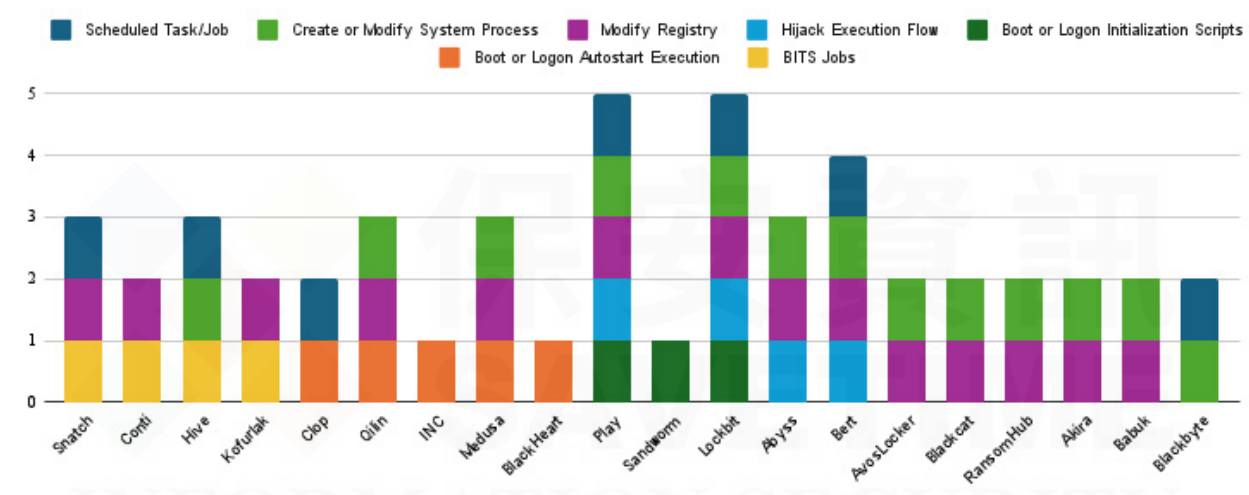
已知常見的持久化技術

根據 MITRE ATT&CK 框架的威脅活動分析顯示，攻擊者反覆採用多種作業系統核心層級的持久化機制。在賽門鐵克客戶環境中，以下技術最為突出：

- 修改登錄檔 (T1112)：攻擊者竄改登錄檔機碼以保存有效酬載，或設定支援執行與持久化的指令。
- 啟動或登入自動執行 (T1547)：惡意二進位檔或腳本被設定在系統啟動或使用者登入時自動執行。
- 排程任務／工作 (T1053)：攻擊者建立排程工作，確保有效酬載在啟動時或指定間隔內重複執行。
- 劫持執行流程 (T1574)：
  - 。DLL 側載：利用合法應用程式載入攻擊者提供的 DLL 檔案。
  - 。DLL 搜尋順序劫持：利用 Windows 搜尋順序漏洞，使惡意 DLL 優先於合法檔案載入。
- 建立服務 (T1543)：建立自訂惡意服務以維持持久性，並混入正常系統運作中。。

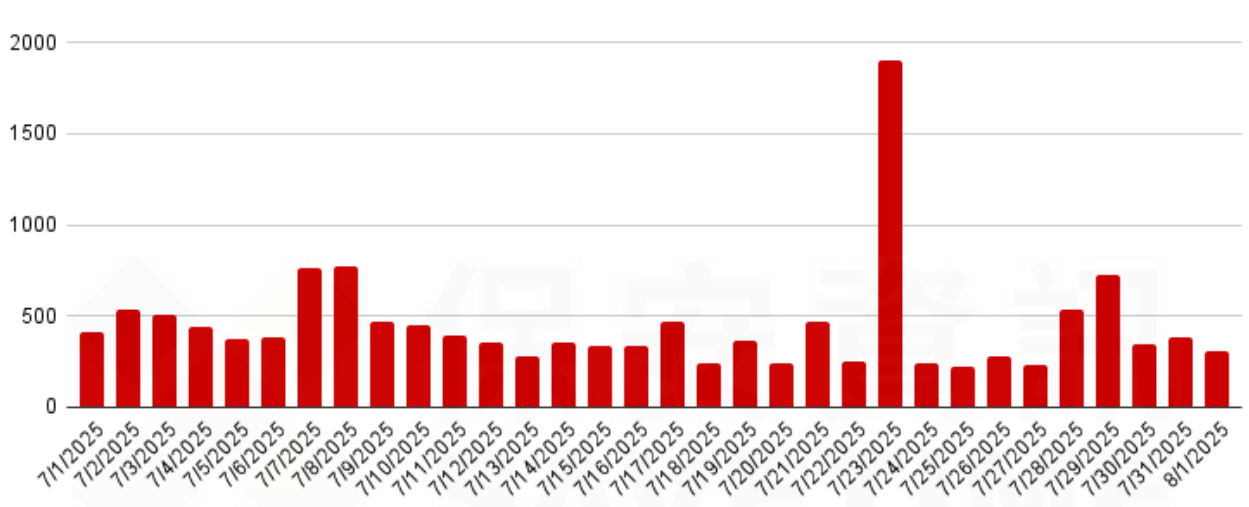
勒索軟體家族與持久性機制

持久性機制並非僅見於進階持續威脅 (APT) 攻擊--勒索軟體經營者同樣高度依賴這些技術。針對多個勒索軟體家族的分析顯示，它們傾向透過修改登錄檔、設定工作排程、劫持動態連結庫 (DLL) 及建立服務等方式來維持控制權。詳見以下概述：

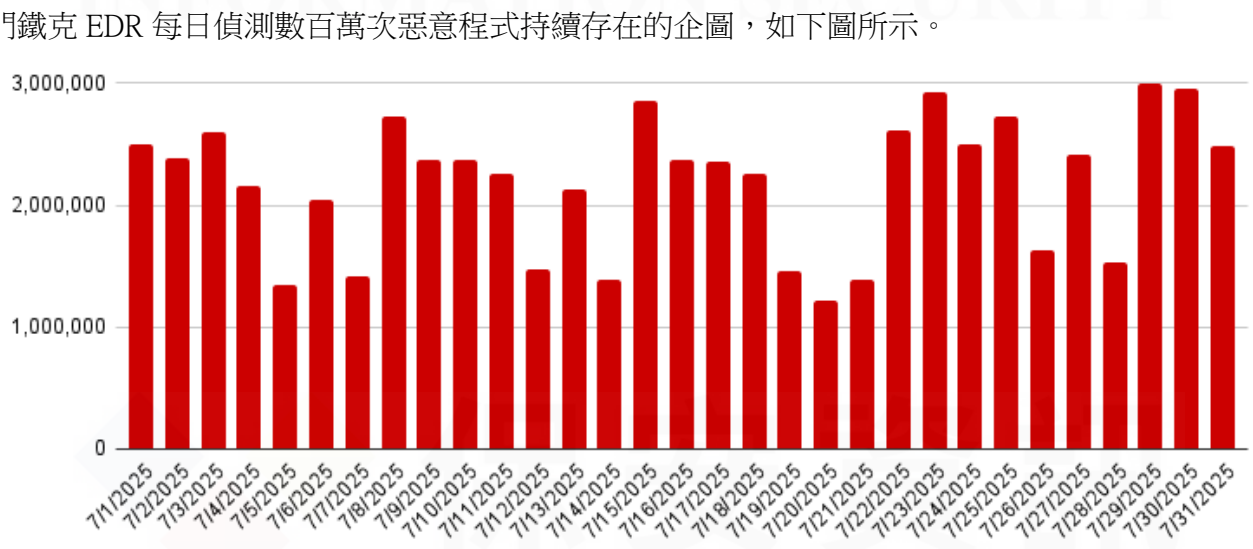


賽門鐵克 EDR 阻斷長期埋伏的持久化機制

賽門鐵克 EDR 阻斷長期埋伏的持久化相關活動，防止攻擊者將自身植入客戶環境。每日遙測資料顯示這些防禦措施的規模，如下所示：



除了封鎖攻擊外，EDR 還能深入洞察惡意程式持續存在的行為模式，賦予防禦者調查可疑活動的能力，將其與攻擊者戰術建立關聯，並在惡意程式擴散造成更嚴重損害前主動應對。賽門鐵克 EDR 每日偵測數百萬次惡意程式持續存在的企圖，如下圖所示。



持久性是攻擊者武器庫中最關鍵的戰術之一。從進階持續威脅 (APT) 組織到勒索軟體經營者，攻擊者皆仰賴登錄檔竄改、工作排程、DLL 劫持及惡意服務來確保長期存取權限。賽門鐵克 EDR 不僅能大規模阻斷此類企圖，更賦予防禦者深入調查與修復的可視性。

阻斷持久性就是瓦解攻擊者的控制權--這正是捍衛企業環境的關鍵決策步驟。

關於賽門鐵克EDR 的原廠官方網站介紹，請點擊此處。

欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

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，而且在全球前兩千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 年起就全心全力專注在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，以及基於比原廠更孰悉用戶使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。