Carbon Black -- 阻斷基於 PowerShell 的攻擊

2025 年 11 月 25 日發布

PowerShell 是一款強大的殼層命令列與腳本語言，內建於 Windows 系統中。此工具在攻擊者間廣泛流傳，協助其執行惡意活動，例如：資訊偵測、惡意軟體投放、勒索軟體部署及資料竊取。

為何 PowerShell 如此顯眼

- 常見於組織中，用於自動化系統管理
- 採用無檔案方式，直接在記憶體中執行命令與腳本
- 攻擊者利用 PowerShell 來：
  - 混淆惡意命令並執行
  - 遠端下載並執行有效載荷或任意程式碼／二進位檔
  - 蒐集並變更系統設定
  - 利用PowerSploit、Empire等框架濫用PowerShell功能，以停用Windows安全工具、協助程序注入、編碼/混淆惡意活動等

常見的 PowerShell 技術觀察

以下 MITRE ATT&CK PowerShell 技術最為顯著：

- 破壞系統復原 (T1490)：勒索軟體攻擊者運用 PowerShell 命令刪除系統的陰影複製，以阻擋復原機制
- 加密資料並造成影響 (T1486)：透過 PowerShell 腳本執行資料加密
- 破壞防禦機制：停用或修改工具程式 (T1562.001)：透過無檔案命令停用 AMSI
- 命令與腳本解譯器 (T1059)：攻擊者利用的無檔案活動
- 伺服器軟體元件：網頁殼層 (T1059.003)：利用反向網頁殼層協助攻擊者連線至遠端機器

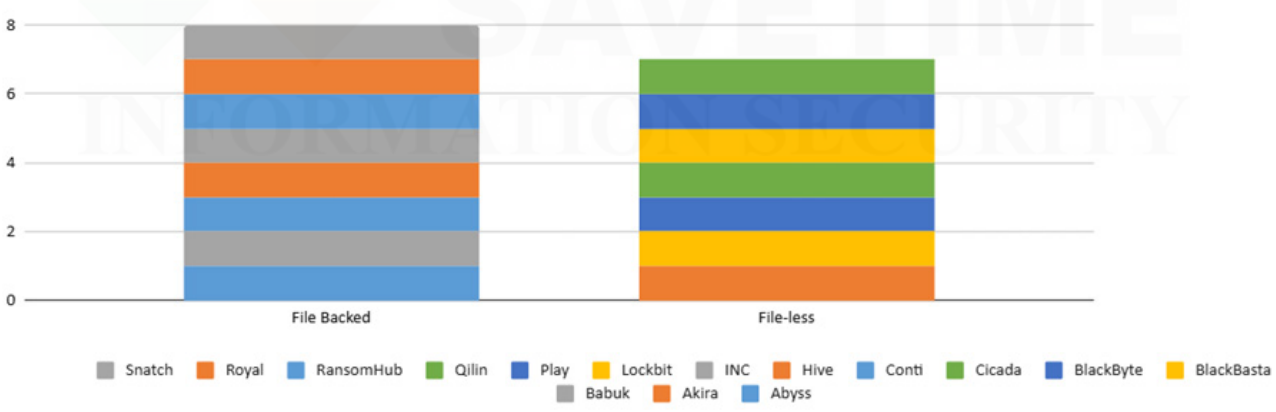
Carbon Black EDR

Carbon Black EDR 透過整合式平台提供端點防護，集中管理代理程式並運用行為分析技術，強化對網路攻擊的偵測、防禦與應對能力。藉由單一代理程式與控制台簡化端點安全功能，Carbon Black EDR 能深入掌握端點上運行的程序狀態與背景資訊，實現更快速、更有效的修復措施。

- 採用多重防護層，包含檔案信譽評分與啟發式分析、機器學習及行為模型
- 預設防護策略並可自訂環境需求客製調整
- 全面掌握攻擊鏈動態，簡化事件調查流程
- 提供遠端用戶端連入殼層功能，可即時採取應變措施
- 雲原生平台，單一代理程式與控制台整合

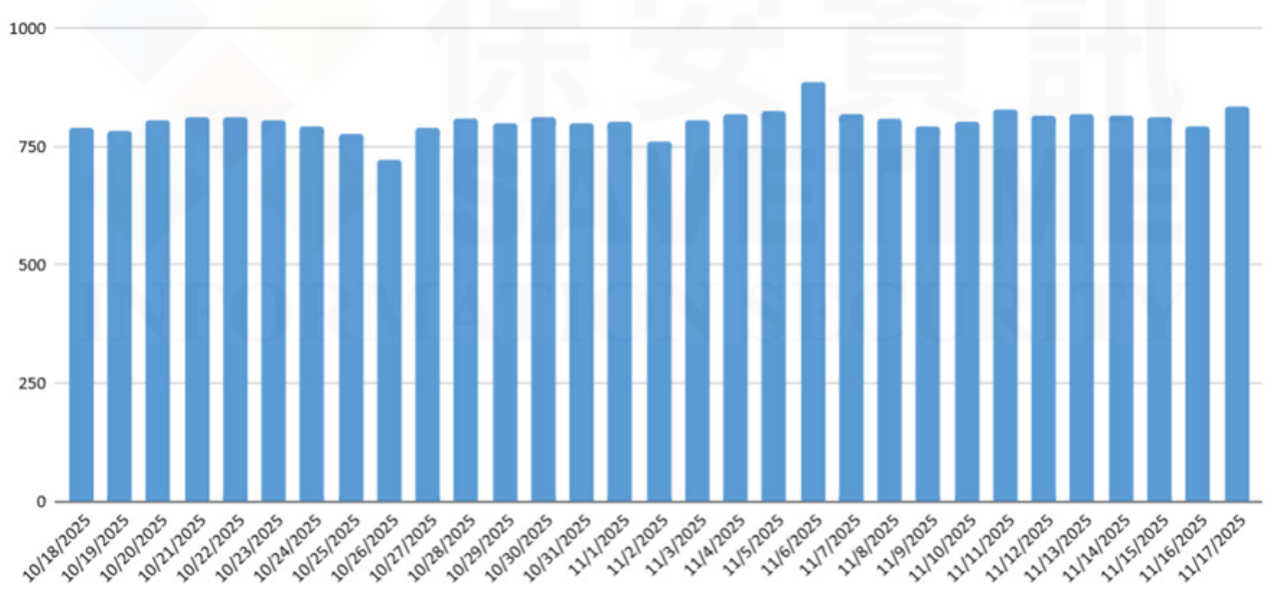
Carbon Black 亦提供「觀察清單」作為威脅狩獵查詢，該功能會定期在 EDR 儀表板上運行，以在偵測到可疑活動時發出警示。

勒索軟體攻擊者利用 PowerShell 作為攻擊載體



碳黑防護趨勢

碳黑防護抵禦PowerShell無檔案與有檔案攻擊



欲深入瞭解更多 Carbon Black Endpoint，請點擊此處。

欲深入瞭解更多 Carbon Black Endpoint Detection & Response (EDR)，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**。