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

有效應對防禦規避的攻擊手法，Carbon Black EDR (端點偵測與回應)神通廣大

2025 年 7 月 22 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

現代網路安全解決方案是利用先進、多層次的技術來對抗不斷演變的威脅。然而，攻擊方會不斷改良其技術以混入企業環境，利用看似合法的行為來逃避偵測。2025 年 6 月，VMware Carbon Black EDR(端點偵測與回應) 偵測到採用防禦規避的網路攻擊行動激增，讓客戶能夠迅速回應並降低威脅。本公告重點介紹所觀察到的趨勢和駭客所使用的技倆，以及 Carbon Black 如何協助瓦解這些趨勢和技倆。

Carbon Black EDR(端點偵測與回應)

Carbon Black EDR(端點偵測與回應) 透過雲端原生平台提供進階的端點偵測與回應功能，該平台整合行為分析與端點活動的可視性。它使用單一輕量級代理程式和統一主控台簡化防護和回應。

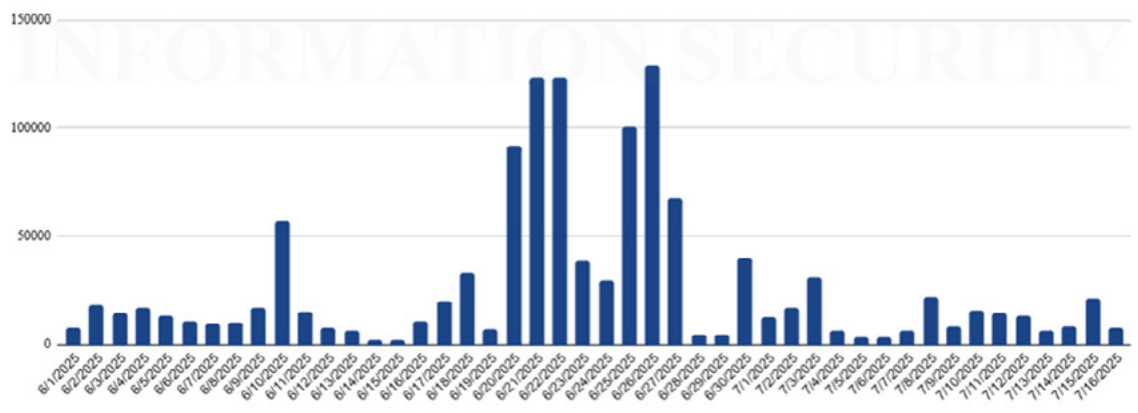
主要功能包括

- 阻止已知和未知的惡意軟體、勒索軟體和就地取材 (LotL) 攻擊
- 運用檔案信譽、啟發式技術、機器學習和行為模型
- 提供開箱即用的防禦政策與客製化選項
- 提供攻擊鏈的完整可見性，以便進行快速調查
- 啟用遠端 shell 存取功能以進行即時回應
- 利用監視清單(Watchlists)進行持續的威脅攔截與警示

偵測到的趨勢

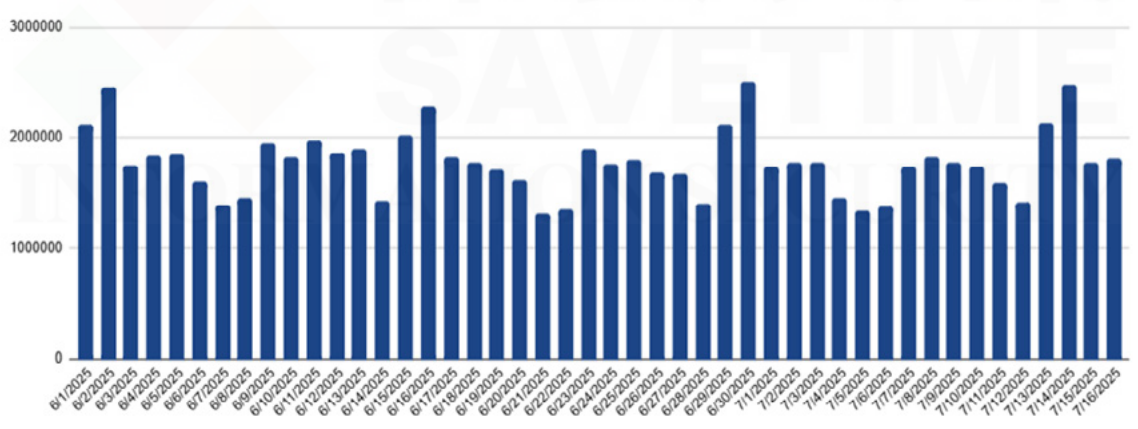
兩組不同的資料集顯示 Carbon Black 在 6 月和 7 月初對防禦規避活動的涵蓋情況。在 2025 年 6 月 18 日至 26 日期間，警報數量激增，最高峰時每天超過 120,000 次。這些警報代表即時偵測到主動規避嘗試，例如：DLL 側載和就地取材 (LOLBin) 工具的濫用。。

防禦規避嘗試的警示



在這段期間內，監視清單 (Watchlists) 每天標記 150 萬至 250 萬個潛在的防禦規避行為。這些警示是由主動的威脅獵捕 (threat hunting) 查詢所產生，且有助發現可能會避開自動化偵測的隱匿行為。

監視清單(Watchlists)顯示的防禦規避的警報



觀察到的常見防禦規避技術

威脅發動者利用各種 MITRE ATT&CK 對應的攻擊手法來避免被偵測並維持持久性。其中許多手法被 Carbon Black EDR(端點偵測與回應) 透過即時警示和持續的監視清單 (Watchlists) 查詢偵測到。以下是觀察到一些最普遍的攻擊手法。

- DLL 側載 (T1574.001)：攻擊者濫用合法的可執行檔來載入惡意的 DLL。這通常是透過搜尋順序劫持或將可信任的應用程式與攻擊者製作的 DLL 綁定在一起來達成。此技術常用於持久性、提權及防禦規避。
- 不尋常的 DLL 執行 (T1218.011、T1218.010)：rundll32.exe 和 regsvr32.exe 等公用程式被用來從意外路徑載入 DLL 或使用非標準擴充檔，通常會偽裝成合法的系統行為，以繞過啟發式偵測。
- 常用的合法工具 (LOLBins) 被改名 (T1036.003)：內建的 Windows 工具 (例如：powershell.exe、cmd.exe) 被改名，以掩蓋其真正目的。這些被改名的二進位檔隨後被用於隱蔽執行、橫向移動、提權和遠端指令執行，同時根據檔案名稱或雜湊值逃避偵測。
- 系統二進位代理執行 (T1218)：攻擊者利用可信任的 Windows 二進位檔 (例如：mshta.exe、regsvr32.exe) 來執行惡意的有效負載，並採用代理執行策略。此技術常用於繞過應用程式控制及安全政策。
- 篡改安全工具 (T1562.001、T1112)：攻擊者使用多種手法以削弱資安防護機制，包括終止 AV／EDR 程序、修改或刪除登錄檔機碼，以及停用更新機制以防止部署新憑證或修補程式。

Carbon Black 偵測到多個威脅組織和惡意軟體家族採用這些防禦規避手法。

勒索軟體家族

- LockBit
- BlackBasta
- Hive
- BlackCat
- Kofurlak
- RansomHub

木馬／後門程式家族

- Emotet
- IcedID
- Pikabot
- ShadowPad
- Mocha Manakin（基於 NodeJS）

多層次防禦技術

Carbon Black EDR 多層次防禦技術結合即時行為分析與透過監視清單 (Watchlists) 進行的持續威脅攔截，可針對進階的防禦規避技術提供可視性與可操作性。6 月份警報的急劇增加突顯威脅發動者的敏捷性，以及持續監控和主動偵測的必要性。隨著威脅份子的演變，組織必須持續利用 Carbon Black EDR 等工具，不僅是為了防護，也是為了洞察、回應和調適。

欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的郵件威脅偵測和回應(ETDR)功能，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**。