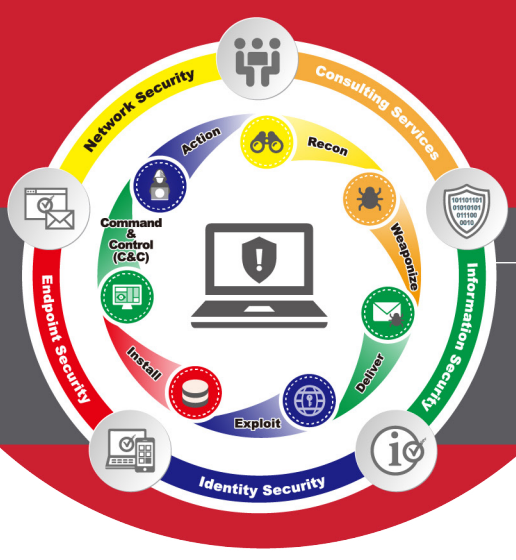


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

Carbon Black Endpoint Standard有效阻擋勒索軟體

2025 年 3 月 18 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

現今檯面上數百家爭鳴之勒索軟體家族是一個蓬勃發展的威脅生態。不單單只是對檔案加密之外，源於相同勒索軟體家族的後繼新變種也各出奇招，出現越來越多的新變種並整合無檔案的威脅技術。數十年來，駭客勒索軟體隨著時間推進與新技術發展而變得越來越複雜，因此對網路安全專家造成嚴峻的挑戰。在 2025 年 1 月，我們發現勒索軟體攻擊激增，但 Carbon Black Endpoint Standard 成功阻擋這些攻擊。在所有情況下，客戶都能避免檔案被加密。

Carbon Black Endpoint Standard

Carbon Black Endpoint Standard 透過整合代理程式的統一平台提供端點防護，並運用行為分析來強化偵測、預防及對應網路攻擊。Carbon Black Endpoint Standard 透過單一代理程式和主控台簡化端點安全功能，提供更快、更有效的修復功能，並提供端點上執行程序的高能見度和詳細的情境脈絡。

- 阻止已知和未知的惡意軟體、勒索軟體和外來攻擊
- 採用多重防護層，包括檔案信譽和啟發式、機器學習和行為模型
- 開箱即用且能依環境自訂的防禦政策
- 整個攻擊鏈的可見性，以便調查
- 可遠端 shell 進入端點以立即採取行動
- 單一代理程式與主控台的雲端原生平台

熱門的勒索軟體家族

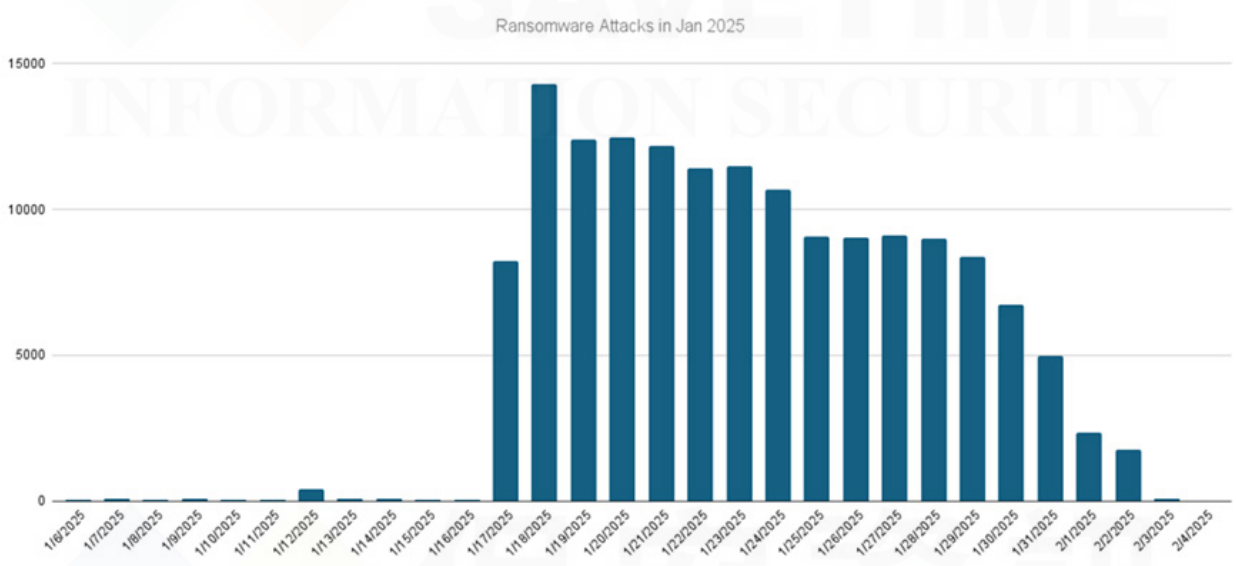
以下勒索軟體家族是涉入 2025 年 1 月網路攻擊的主要威脅者。

- **Cactus**：是採用雙重勒索手法的勒索軟體體，會加密受害者的資料，如果受害者拒絕支付贖金，還會洩露資料。它通常利用虛擬私人網路 (VPN) 軟體的漏洞來取得初始存取權。一旦完成加密和檔案滲出，惡意軟體就會在使用者的電腦上張貼勒索 (贖金支付) 通知。
- **RansomHub**：使用多種演算法組合來加密使用者資料，然後要脅贖金以還原檔案。如果受害者拒絕支付，攻擊者會威脅要出售或公佈竊取的資訊。它還具有透過網路傳播的能力。與其他勒索軟體一樣，它會刪除磁碟區陰影複本並停用 Windows 自動啟動修復功能，以確保資料無法輕易還原。
- **Blacksuit**：利用多種初始存取媒介，包括網路釣魚活動、RDP 漏洞利用。它會加密和滲出受害者的資料，並洩露那些不乖乖就範付贖金的受害者資料。惡意軟體的功能包括停止與虛擬機器環境相關的程序、停止特定的 Windows 服務，以及刪除受攻擊系統的磁碟區陰影複本。

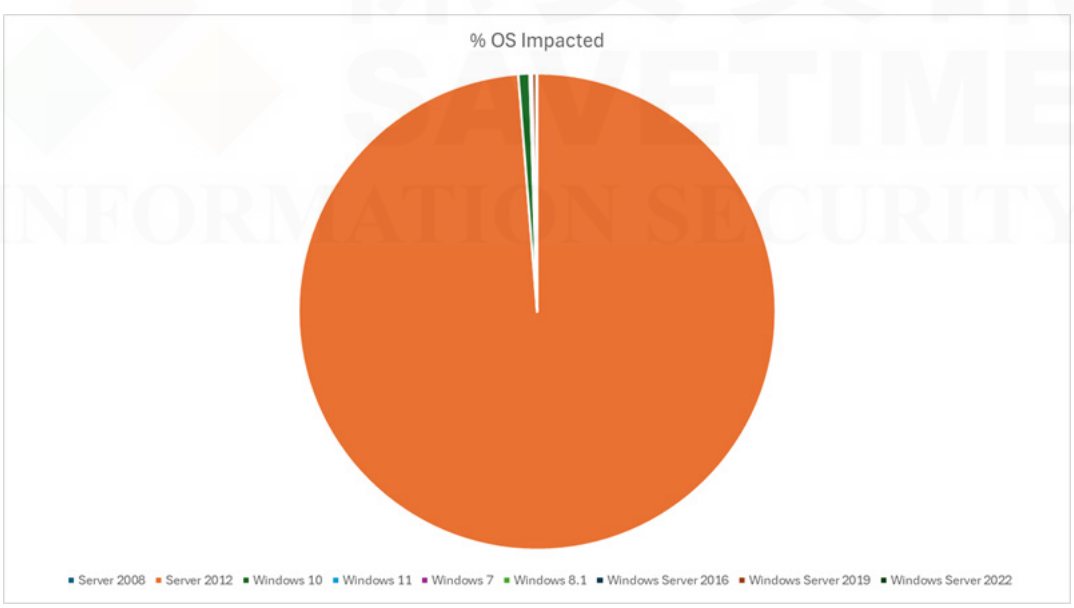
拆解其攻擊鏈發現其在加密檔案之前，有許多前置的變動系統設定的作業：

- 使用 vssadmin.exe／wmic.exe 刪除陰影複本
- 使用 bcdedit.exe 竄改開機設定以停用復原功能
- 使用排程任務來持續執行和提升權限
- 使用 msiexec.exe 透過軟體 GUID 卸載常見的防毒軟體

下圖為 2025 年 1 月的資料，顯示 Carbon Black Endpoint Standard 所阻擋的勒索軟體攻擊。



下圖顯示勒索軟體所針對的作業系統版本。98% 的攻擊以 Win Server 2012 為目標。



欲了解更多關於 Carbon Black Endpoint 的資訊，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**。