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

斷開攻擊鏈-- xSenseNet 阻斷腳本優先攻擊

2026 年 3 月 1 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

「經典」的惡意軟體攻擊模式--雙擊 EXE 檔案導致系統崩潰--至今仍時有發生，但已非主流手法。當前攻擊日益傾向採用非 PE 格式載體 (Non-PE stagers) 作為起點，透過腳本與命令列指令建立執行環境，隨後才傳遞最終有效載荷。

此階段化層之所以有效，在於其依賴 Windows 本有的原生元件且能快速適應。威脅攻擊者可透過 wscript.exe、powershell.exe 及 mshta.exe 串接 JavaScript、VBScript、PowerShell、批次指令檔等程式，隨後替換為當下最不易被偵測的載入器、竊取程式或遠端存取工具 (RAT)--無需更動初始誘餌。

正因如此，早期阻斷階段化工具至關重要：此舉能剝奪攻擊者的靈活性，在有效載荷選擇階段前便切斷攻擊鏈。

實例分析：2025 年末至 2026 年初觀察到的劇本密集型 (「非 PE」) 攻擊鏈

- 遭入侵網站 > 偽造「人工驗證」驗證碼 > ClickFix(使用者複製/貼上指令) > PowerShell > AMSI 繞過腳本 > VBS > XWorm
- Discord 連結 > ZIP > LNK > 批次檔 (.bat) > AI 生成的 PowerShell >繞過UAC > PowerShell 後門
- 遭入侵網站 > 偽造驗證碼 > ClickFix(使用者複製指令)> mshta.exe > JScript > 簽署版 Microsoft App-V 腳本 > PowerShell > Amatera 竊取程式
- 電子郵件 > 7Z/RAR > WSF(Windows 腳本檔案)> PowerShell > 圖片下載(Archive.org)>資訊隱藏技術> .NET 加載程式 > Agent Tesla
- 電子郵件 > PDF > 網址重導向 > 登錄頁面 > ClickFix(使用者複製指令)> PowerShell > VBS > 批次檔 > QuasarRAT
- 電子郵件 > 網址 > VBS > wscript.exe > PowerShell(編碼)> 分散化純文字載荷 (.txt) > 記憶體內 .NET載入器 > Remcos RAT
- 電子郵件 > JavaScript 載入器 > 混淆型批次處理 > PowerShell > 解碼 PNG 嵌入加密資料區塊 > 記憶體內 .NET 組件 > XWorm
- 電子郵件 > ZIP/7z > 混淆 VBScript > wscript.exe > PowerShell > 雲端託管 Shellcode (Google Drive / OneDrive) > GuLoader > Remcos / Agent Tesla
- 電子郵件 > JavaScript載入器 (JSGuLdr) > wscript.exe > COM 執行 > PowerShell > msiexec.exe > 記憶體載入 > Phantom Stealer
- 電子郵件 > DOCX (遠端範本注入) > RTF (CVE-2017-11882) > VBS > Remcos
- 電子郵件 > JS / VBS > PowerShell > AsyncRAT

核心關鍵很簡單：PE 載荷往往要到第四或第五階段才會顯現。若僅聚焦於「最終可執行檔」，等於在攻擊鏈最後期才做出反應。

xSenseNet問世：深度學習對抗腳本型威脅：

為應對這種檔案輕量化、腳本主導的趨勢，賽門鐵克開發了 xSenseNe--一款專為非 PE 檔案類型及腳本驅動式分階段行為設計的深度學習惡意軟體掃描器。

不同於主要依賴僵化規則或狹隘特徵檔的方案，xSenseNet 旨在含括現代腳本的複雜現實：高度混淆、分階段解碼、離地攻擊執行模式，以及快速更迭換代活動。

xSenseNet 支援：

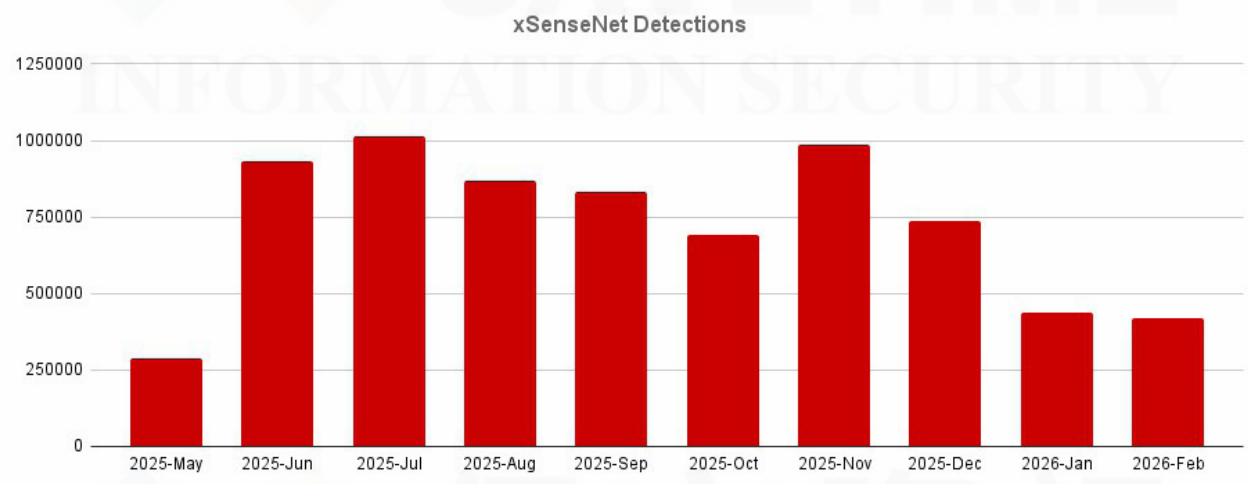
- 獨立腳本： js、vbs、ps1、vbe、bat、cmd
- 腳本容器：含 VBA 的文件、含 JavaScript 的 PDF、含命令列的 LNK 檔案，以及類似「容器化執行」格式

xSenseNet 透過整合多重訊號生成全面風險評分，能識別雖無「明顯」惡意軟體特徵、卻仍具備惡意階段化數學特徵的隱蔽階段化程式。

數據洞察：實戰影響力：

全球遙測數據顯示，以腳本為先的「非執行檔型態」(Non-PE) 活動已呈現高度流行與持久性。自 2025 年 4 月以來，xSenseNet 已攔截 6,745,948 次非 PE 威脅，偵測量在 2025 年持續居高不下，並於年中及年末兩波重大攻擊浪潮中達到高峰。

地理分佈數據證實此為全球性問題：攔截事件遍及世界各地，其中北美與歐洲等高風險區域的攔截密度尤為顯著。



結論很明確：只要能阻止階段中的載體活動，就能終止攻擊。xSenseNet 針對此現實需求而生，將分階段部署於賽門鐵克產品組合中，並於 2025 年初完成最終整合。此技術專注於非執行檔威脅的深度學習，具備廣泛部署能力，並在真實遙測數據中通過大規模驗證。其重要性在於：僅針對最終有效載荷的強效防護已不足夠；威脅行為者會慣性轉向當前最不易被偵測的載入器、竊取程式或遠端存取木馬。透過在更早階段--即主機尚未被剖析、持久化機制尚未建立、有效載荷尚未替換之前--中斷攻擊鏈，xSenseNet 能有效限制攻擊者的靈活性，從源頭阻止攻擊行動進入執行階段。

原廠網址：https://www.broadcom.com/support/security-center/protection-bulletin/breaking-the-chain-xsensenet-stops-script-first-attacks

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**。