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

Scattered Spider--企業持續面臨的高風險威脅

2025 年 8 月 13 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

Scattered Spider 又稱 UNC3944 和 Octo Tempest，是一個以財務為動機的網路犯罪集團，對機構組織構成重大且持續的威脅。該網路犯罪集團在 2023 年 9 月因對知名的大型飯店與遊戲產業機構發動多起引人側目的攻擊事件後，在國際上聲名大噪。在這些事件中，他們利用社交工程技倆入侵 IT 系統，造成營運癱瘓，並據報竊取近 6TB 的資料。

此威脅發動者以其先進的社交工手法而聞名，通常會冒充 IT 服務台人員，誘騙員工洩露憑證或批准遠端存取。這樣他們就可以使用推送炸彈和 SIM 卡交換等技術繞過多因素驗證 (MFA)。一旦進入網路，他們就會展現「就地取材」(LOTL) 技術的強大能力--濫用合法的管理工具而不被發現。他們的作業通常會進行勒索軟體之部署，而且越來越專注於 VMware ESXi 環境。其結果是造成大規模的作業中斷、資料竊取，以及包括零售、運輸和金融等部門的財務損失。

Scattered Spider 涉入的著名資安事件：

- 2023 年 9 月：一家酒店集團面臨運作中斷，影響酒店鑰匙卡和角子機。另一家公司發生涉及客戶資訊的資料外洩事件。該網路犯罪集團冒充服務台人員取得存取權限。據報導，一名受害業者支付約 1,500 萬美元的贖金；另一名受害者則蒙受超過 1 億美元的損失。
- 2023 年 9 月至 10 月：攻擊者使用竊取的憑證入侵客戶支援系統，竊取所有支援用戶的姓名和電子郵件地址，並進一步進行後續攻擊。
- 2023－2024 年第 2 季：一系列憑證網路釣魚攻擊針對 Microsoft Entra ID 和 AWS 等雲端基礎架構。
- 2024 年中：超過 160 個未啟用多重驗證 (MFA) 的組織其雲端資料遭攻擊者透過竊取的憑證存取。該組織被追蹤為 UNC5537 (與 Scattered Spider 相關聯)，專注於勒索。
- 2025 年 6 月至 7 月：該組織將範圍擴大至多家航空公司和一家零售業者。社交工程和服務台冒充再次被用來入侵身份服務和中斷營運。

拆解 Scattered Spider 攻擊鏈 V.S. 自適應防護技術如何拆雷

攻擊通常從有目標式的社交工程電話開始，打到 IT 服務台，假冒員工要求重設密碼和繞過 MFA 保護。一旦進入，Scattered Spider 會遵循一套結構化的攻擊鏈，展現出對企業環境的透徹了解。

- 階段 1 -- 入侵初期 (Initial Access)／身份濫用：使用服務台冒充、MFA 推送炸彈和 SIM 卡交換來取得最高存取權限。雖然 Adaptive Protection 不會直接介入此階段，但是維持良好的帳號安全習慣仍是非常重要。
- 階段 2 -- 持續潛伏(Persistence)／就地取攻擊 (LOTL)：AnyDesk、TeamViewer、Teleport.sh、ScreenConnect 和 Splashtop 等工具被重新使用，以保持持久性並逃避偵測。自適應防護會強制執行拒絕模式政策，在通常不使用這些工具的環境中自動封鎖這些工具。例如：AnyDesk 或 Teleport 可在特定環境的學習期結束後自動封鎖。
- 階段 3 -- 發現 (Discovery) 以及橫向移動 (Lateral Movement)：透過 Mimikatz、PowerShell scripting、PsExec、WMIC 和 AWS CLI 濫用收集憑證的情況都很常見。Adaptive Protection 包括 36 種以上的 PowerShell 行為規則--涵蓋 LSASS 記憶體讀取、程序注入、Base64 編碼混淆、PE 建立等。就連 WMI 和 PsExec 濫用也受到嚴格控制。
- 階段 4 -- 防禦逃脫 (Defense Evasion) 與核心驅動程式濫用：該群組嘗試透過終止安全進程或安裝惡意 DRM 來停用端點防護。該組織試圖透過終止安全進程或安裝如 STONESTOP 等惡意驅動程式來停用端點防護。自適應防護可以阻止未授權的驅動程式安裝或試圖終止受保護服務的嘗試。
- 階段 5 -- 滲出 (Exfiltration) 與衝擊(Impact)：資料透過 Rclone 或 AWS CLI 等工具外洩。如果未經日常操作的驗證，自適應防護會阻止未經信任的雲端上傳工具，例如：MegaSync、Ngrok 和 Rclone。

Symantec Adaptive Protection(賽門鐵克自適應防護技術)：專門為複雜威脅的行為保護技術

Scattered Spider 會利用不斷轉變的公用程式、兩用工具和惡意軟體，因此需要能夠在行為層級進行自適應的防護。賽門鐵克自適應防護正是如此--根據攻擊者的行為，而不只是他們使用的工具，來封鎖惡意活動。

舉例來說，Adaptive Protection 會偵測並阻擋 Scattered Spider 作業中部署的惡意軟體家族常見的相關行為。VIDAR Stealer 常常濫用 PowerShell 來啟動 Rundll32 或 WScript、執行 base64 混淆指令，並在已知的持久化／常駐路徑中建立登錄項目。這些行為，以及不受信任的程序中嘗試產生系統層級元件的情況，都會立即被標記並停止。

同樣地，RattyRAT 會透過 PowerShell 修改註冊表機碼來建立持久性而聞名。自適應防護可防止這些與常見持久性技術相關的關鍵位置的註冊表被變更。DragonForceransomware 會嘗試存取 LSASS 記憶體以盜取憑證、修改服務相關的註冊表項，並使用 PowerShell 和 Rundll32 啟動惡意例程，在這種情況下，所有這些行為都會被主動偵測並阻截。Adaptive Protection 還會監控進行持久性相關的註冊表 run 機碼之修改--這是 DragonForce 攻擊中觀察到的另一種策略。

同時，AveMaria (也稱為 WarZone) 經常濫用腳本引擎和 HTML 主機，以逃避防禦並啟動惡意有效酬載。它使用 mshta.exe 來啟動 PowerShell 或命令列程序，並建立對外 HTTP 連線以進行遠端命令和控制。Adaptive Protection 可偵測這些嘗試，包括透過 HTML 應用 (例如：HTA)、.NET 安裝程式或 WScript 啟動 PowerShell 的情況，並在入侵前阻斷攻擊鏈。

自適應防護焦點

- 追蹤的行為：目前有 496 個且跨 69 個應用程式
- 對應：78 項 MITRE ATT&CK 技術
- 受保護的端點：全球超過 290 萬個
- 以拒絕模式封鎖：平均每次部署超過 345 個行為。

賽門鐵克 Adaptive Protection 著重於工具的行為方式，而非僅僅是識別工具，因此可以在不中斷合法業務運作的情況下，同時緩解已知和新型的威脅。想要立即啟用 Adaptive Protection？請參閱此頁面的逐步指南。

Adaptive Protection 現已整合至地端自建的 Symantec Endpoint Protection Manager(SEPM) 管理主控台。透過內建的熱圖視覺化介面，安全團隊可以監控行為的普遍性，並及時採取有根據的決策行動。

請參閱此頁面，了解如何在組織中透過賽門鐵克 Adaptive Protection 最大化降低攻擊面的詳細資訊！對這個功能有興趣的客戶，歡迎與保安資訊聯繫相關導入細節及技術支援。

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**。