瓦解鹽颱風的「就地取材」間諜活動

2025 年 12 月 16 日發布

近期威脅態勢由「鹽颱風」(亦被追蹤為 GhostEmperor 或 Earth Estries) 主導，此為精巧的國家級資助攻擊行為，鎖定全球電信與關鍵基礎設施。不同於愛好廣為宣傳的勒索軟體集團，鹽颱風優先採用隱蔽策略，其深入潛伏於網路內部以攔截敏感通訊。它主要規避手段是「就地取材」(LOTL) ，利用標準管理工具偽裝成合法 IT 活動。賽門鐵克自適應防護提供關鍵防禦層，能讓安全團隊阻斷 Salt Typhoon 依賴的特定異常行為，同時不影響業務運作。

威脅：鹽颱風 (GhostEmperor)

背景與動機：鹽颱風是與中國有關聯的進階持續性威脅 (APT) ，其行動規模於 2025 年底顯著擴大。繼 2025 年 8 月與 10月美國聯邦調查局 (FBI) 及網路安全與基礎設施安全局 (CISA) 發布警告後，確認該組織已入侵 80 多國的主要電信供應商。其戰略間諜活動目標：入侵合法監聽系統，監控高價值政治與政府目標。

攻擊手法 (TTP)：鹽颱風擅長隱蔽行動。初始入侵後 (常透過思科路由器等邊緣設備漏洞)，便利用系統內現有工具橫向擴散至Windows環境。主要技術手法包括：

- 透過 netsh 介面埠代理進行流量通道傳輸「濫用 netsh.exe (netsh 介面埠代理) 路由 C2 流量 [MITRE T1090]」。
- 橫向移動利用 wmic.exe 與 rundll32.exe，透過執行遠端機器指令部署「GhostSpider」後門程式或「Demodex」rootkit [MITRE T1047]。
- 服務濫用／持久化機制：Salt Typhoon 會建立惡意 Windows 服務以維持持久性，常偽裝成合法系統更新程式 [MITRE T1543]。

為何重要：Salt Typhoon 依賴 LOTL 二進位檔的特性，使其能躲避傳統防毒軟體的偵測。標準安全政策無法直接封鎖 netsh.exe 或 wmic.exe，因為 IT 管理員需要這些工具進行日常網路管理。這種「雙重用途」的兩難困境，恰恰為 Salt Typhoon 創造完美的隱蔽空間，使其能在數月間不被察覺地運作。

自適應防護如何緩解此威脅

賽門鐵克自適應防護 (SES Complete 功能之一) 能有效對抗 Salt Typhoon，因其著重行為脈絡分析而非靜態檔案信譽評估。自適應防護會分析特定環境中工具使用的「誰、什麼、何處」元素，以當下情境為偵測要素，建立專屬熱力圖以區分正常管理作業與異常濫用行為。干預關鍵點 Salt Typhoon 透過非常規方式運用標準工具發動攻擊。自適應防護能在執行前或存取階段偵測此類偏離常規的行為。

情境：

- 攻擊：Salt Typhoon 攻陷伺服器並嘗試執行 netsh interface portproxy 指令，以建立隱藏的 C2 通訊通道。
- 分析：自適應防護機制評估此特定命令列與父進程。其識別到 netsh.exe 雖屬常見程式，但建立埠代理的特定行為在您環境中的此特定伺服器上呈現零發生率。
- 行動：若政策設定為「拒絕」，該指令將立即遭阻擋。攻擊者建立立足點的企圖失敗，而合法IT流量 (使用標準 netsh 指令) 則不受干擾地持續運作。

通用行為規則面對「鹽颱風」這類進階持續性威脅時往往失效，因其會產生過多誤判。問題在於：若採用全球性規則封鎖「WMI程序建立」，將導致多數企業IT管理軟體癱瘓。自適應防護機制會自動為貴組織客製化規則集。它能辨識貴公司的Exchange伺服器高度依賴WMI (高發生率) ，但人力資源工作站從不使用 (零發生率) 。透過僅在異常行為發生時實施「拒絕」策略，您能有效封堵 Salt Typhoon 的橫向移動路徑，同時確保業務連續性不受影響。

安全團隊的指引與後續步驟

為強化防禦機制以抵禦 Salt Typhoon 當前的攻擊行動，我們建議您在 Symantec Endpoint Security 控制台中採取以下措施：

1. **稽核「雙用途」工具普及率**：開啟自適應防護熱力圖，特別檢視 netsh.exe、wmic.exe、rundll32.exe 及 sc.exe 的普及程度。
2. **對零發生機率的行為強制執行「拒絕」**：識別透過 Netsh 建立代理程式或透過 WMI 遠端建立程序而標記為「零盛行率」的行為。立即將這些行為切換為拒絕。此舉將移除 Salt Typhoon 依賴的隱蔽通訊與移動工具。
3. **調查低發生率異常值**：審查任何由 rundll32.exe 建立網路連線的「低發生率」案例。此為載入 GhostSpider 後門的常見技術、戰術與程序 (TTP) 。若這些案例未與已知商業應用程式相關聯，應立即調查其作為潛在入侵指標的可能性。
4. **針對中高發生率行為設定例外規則**：若某高風險行為 (例如：PowerShell下載檔案) 顯示中度或高度發生率，切勿無限期放任其存在。請運用例外工具為合法業務模式定義特定允許條件 (例如：僅允許團隊使用的特定 IT 管理員腳本或路徑) 。監控發生率：未來數週至數月內持續追蹤剩餘通用行為的發生率。由於合法流量已由例外規則處理，通用行為計數應降至零。鎖定規則：當殘餘發生率歸零時，將主規則設為拒絕。
5. **修補邊緣設備**：在自適應防護確保 Windows 端點安全之際，務必確保所有邊緣設備 (路由器、VPN) 針對已知 CVE (例如： CVE-2023-20198) 進行修補，以防止初始入侵。

透過運用自適應防護機制鎖定鹽颱風濫用的特定行為，您將迫使攻擊者放棄其隱蔽的 LOTL 戰術，使其更容易被偵測並扼殺於萌芽狀態。

欲了解啟用賽門鐵克端點安全完整版 (SESC) 上的「自適應防護」透過管理受信任應用程式所執行的潛在風險行為來減少攻擊面，請點擊此處。

原廠網址：https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-neutralizing-salt-typhoon-s-living-off-the-land-espionage