



Amber <a47u0905@gmail.com>

(no subject)

Amber <a47u0905@gmail.com>
To: Amber <a47u0905@gmail.com>

Fri, Sep 12, 2025 at 12:19 PM

<https://tw.news.yahoo.com/%E9%80%A3%E5%B7%9D%E6%99%AE%E6%89%8B%E6%A9%9F%E9%83%BD%E4%B8%AD%E6%8B%9B-%E4%B8%AD%E5%9C%8B%E9%A7%AD%E5%AE%A2-%E6%BB%B2%E9%80%8F80%E5%9C%8B%E6%A0%B8%E5%BF%83%E7%B6%B2%E8%B7%AF-fbi%E8%AD%A6%E5%91%8A%E5%9C%8B%E9%98%B2%E5%8D%B1%E6%A9%9F%E5%B7%B2%E7%88%86%E7%99%BC-041800190.html>

連川普手機都中招！中國駭客「滲透80國核心網路」 FBI警告國防危機已爆發

鏡報 2025年9月5日 週五 下午
12:18



美國總統川普、副總統萬斯的手機都被中國駭客集團滲透。圖／翻攝自FB／The White House

美國網路安全暨基礎建設安全局（Cybersecurity and Infrastructure Security Agency，CISA）近日發布緊急警示指出，中國駭客組織「Salt Typhoon」（鹽颱風）自2019年開始針對全球通訊網路及關鍵基礎設施發動資安攻擊，至今已波及至少80個國家、200間企業，就連美國總統川普（Donald Trump）與副總統萬斯（JD Vance）的手機都被滲透，此事也被美國聯邦調查局（FBI）及盟國情報單位列為國防危機。

中國駭客「Salt Typhoon」滲透各國！全球爆國防危機

英國獨立報（The Independent）、美國富比士（Forbes）等外媒近日由美國FBI、CISA、英國國家網路安全中心（NCSC）、德國聯邦情報局（BND）等盟國情報單位聯合發佈的**CISA警示**報導指出：「中華人民共和國支持的網路攻擊行為者正在對全球各地的網路下手，包括但不限於電信、政府、交通運輸、旅宿以及軍事基礎設施網路。」

廣告

這類網路攻擊手法包括入侵核心路由器、管理層級系統，竊取敏感資料、監控通訊、破壞網路完整性等，一名參與調查的高階情報官員直言：「**這不只是網路入侵，而是通訊基礎設施的武器化**」。據了解，FBI早已在今（2025）年4月懸賞1000萬美元（約3055億元新台幣），徵求與鹽颱風相關的任何線索，試圖鎖定駭客及其作戰網絡。

該警示指出，鹽颱風自2019年活躍至今，**已針對80個國家、至少200間公司發動資安攻擊**，堪稱史上最大規模的間諜行動之一。FBI網路部門高級官員布雷特李瑟曼（Brett Leatherman）表示：「北京不分青紅皂白地對私人通訊下手，迫使我們必須與合作夥伴加強協作，在威脅初期就加以識別並反制。」



美國爆國防危機。圖／翻攝自FB／The White House

鹽颱風的滲透手法是什麼？

- 初始入侵

利用已知漏洞滲透網路設備，包括Ivanti Connect Secure (CVE-2024-21887)、Palo Alto PAN-OS (CVE-2024-3400)、Cisco IOS XE (CVE-2023-20198與CVE-2023-20273)。不過，調查發現，鹽颱風的攻擊並未使用「零日攻擊」，即軟體中尚未被開發商發現、修補的安全漏洞；換言之，鹽颱風利用的是已知漏洞的管理鬆懈，而非新技術。

- 長期滲伏核心

鹽颱風入侵後，就能擁有修改存取控制清單、建立高權限帳號，並在異常高端口啟用遠端管理功能，藉此開啟「隱藏服務」，例如在端口裝設監聽功能，使駭客得以隱匿存取權限長達數月甚至數年。

- 情資蒐集與橫向移動

駭客利用SPAN、RSPAN、ERSPAN等技術鏡像網路流量，暗中監控通訊，並竊取管理員憑證，進一步透過開發商互聯網路橫向滲透，再悄悄偽裝成合法流量，藉此把機密資料往外傳。

- 攻擊目的

鹽颱風不以快速獲利為目標，而是持續監控全球人員、通訊及行動，受害範圍包括電信業者、政府系統、交通樞紐、旅宿網路及軍事基礎設施。



美國CISA發佈警示，揭露中國駭客組織的資安攻擊。圖／翻攝自FB／The White House

FBI與盟國如何應對？

該警示公告也被形容為一份「戰鬥計畫」，內容包含：

1. 要求監控可疑模式。
2. 公開自2021年以來的惡意IP、YARA規則、Snort偵測規則等，協助防禦人員辨識惡意工具與特權升級企圖。
3. 全面隔離管理平面、強制多因子驗證、僅允許金鑰登入、同步驅逐駭客，避免部分修補暴露漏洞。
4. 美國國防部10月起將要求新合約供應商符合網路安全成熟度模型認證（CMMC），以降低類似攻擊風險。

一般人可以做什麼來降低被盜風險？

1. 設定電信帳號PIN碼及門號轉出鎖定。
2. 啟用多重要素驗證（MFA），即使用者要通過2種以上的認證機制之後才能得到授權。舉例來說，使用者要輸入PIN碼、插入銀行卡、經指紋比對，通過3種認證方式才能使用銀行帳戶。
3. 開啟SIM卡防盜功能。
4. 監控個人帳號異常活動。

[Quoted text hidden]