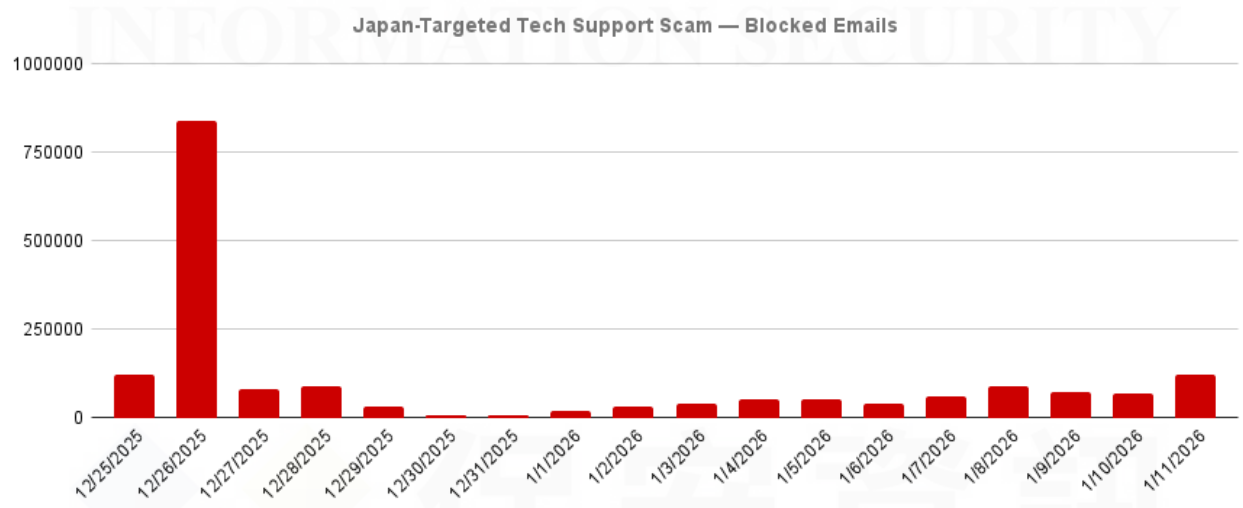
Azure 託管技術支援詐騙活動鎖定日本

2026 年 2 月 1 日發布

全球惡意行為者日益濫用合法雲端服務來託管網路釣魚與技術支援詐騙內容，原因在於其具備快速部署、低營運成本及易於輪替等特性，同時能混入正常流量以規避基礎型的阻擋機制。近期案例顯示，針對日本企業與消費者的技術支援詐騙郵件已發動多波攻擊，攻擊者利用微軟 Azure 靜態網站端點 (web.core.windows.net) 託管其詐騙內容。

遙測數據顯示活動分為兩個階段：初期大規模發送於 12 月 26 日達到高峰，隨後出現短暫驟降，直至一月初活動重新啟動並持續輪替，且發送量穩步攀升。



此攻擊如何運作？Azure Blob Storage 支援靜態網站功能，可直接從儲存帳戶提供 HTML／JavaScript 內容。啟用此功能後，內容將透過服務管理的端點存取。

URL 範例：

- hxxps://codedudacu[.]z1[.]web[.]core[.]windows[.]net/
- hxxps://wesoyifuv[.]z28[.]web[.]core[.]windows[.]net/
- hxxps://ereashzi[.]z31[.]web[.]core[.]windows[.]net/
- hxxps://tionuayeti[.]z33[.]web[.]core[.]windows[.]net/
- hxxps://airodoee[.]z5[.]web[.]core[.]windows[.]net/

在此行動中，所觀察到的運作模式具有持續與重複的特性：

- 配置：建立新的 Azure 儲存帳戶 (通常為短期使用)。
- 託管：啟用靜態網站託管服務，並上傳技術支援詐騙內容。
- 傳遞：發送惡意電子郵件，直接連結至託管頁面。
- 輪替：當網址遭舉報或封鎖時，迅速遷移至新儲存帳戶。

該詐騙電子郵件警告收件者其帳戶已遭其他裝置存取，並敦促收件者立即採取行動。郵件指示用戶檢查其帳戶設定、登出未知裝置並變更密碼--透過安全警示的包裝營造其緊迫性。

當受害者點擊惡意網址時，將被導向假的技術支援詐騙頁面---一個偽造的「Windows Defender／Microsoft Security」網站。

該登錄頁面採用恐嚇手段 (聲稱受害者存在木馬／間諜軟體、顯示「錯誤代碼」及「電腦存取遭封鎖」訊息)，藉此恐嚇用戶致電冒充微軟技術支援的電話號碼。其目的在於誘使受害者提供付款資訊及／或授予遠端存取權限，攻擊者隨後就可竊取資料、植入惡意軟體或勒索用戶。

觀察到的電子郵件主旨範例：

- 「您的帳戶已從其他裝置存取。」
- 「未收到回覆。」
- 「系統偵測到帳戶出現異常活動，或判定您的憑證資訊可能已遭洩露。」

賽門鐵克保護您免受此威脅，其特徵如下：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。

欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。

原廠網址：https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-azure-hosted-tech-support-scam-campaign-targets-japan

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**。