114年8月號

公務機密
資訊安全維護

林業及自然保育署
臺東分署

公務機密 資訊安全維護

目錄

01

資安時事案例

- 注意！微軟伺服器遭大規模網攻 約100個組織遭駭客入侵
- 蘋果用戶注意！iPhone陷最新資安威脅 4危機這一項最容易被騙

02

個人資料保護法

- 9300萬筆個資外洩！知名徵信社涉非法蒐集 負責人、工程師被逮
- 快速瞭解個資法Q&A 60則個資法常識(每月一常識)
  Q16 特定目的是自己說了就算嗎？

03

生活中的資安

- 公務機關網路電話設備遭外部駭入 數發部提3建議

04

數位學習

手機、電腦被駭也沒什麼大不了？小心刑事警察帶你進牢房！快用四招資安習慣讓駭客退散！

資安時事案例

注意！微軟伺服器遭大規模網攻 約100個組織遭駭客入侵

2025-07-22 11:11/科技玩家
中央社／ 華盛頓／倫敦21日綜合外電報導
兩個參與揭露此次網路 間諜活動的機構今天表示，截至上週末，針對微軟（Microsoft）伺服器 軟體的大規模網攻已影響大約100個組織。

路透社報導，微軟19日發布警報 指出，政府機構與企業用於組織內部共享文件的伺服器軟體正遭受「主動攻擊 」。微軟表示，位於雲端 Microsoft 365 的SharePoint Online並未受到波及。

這場攻擊被稱為「零日」（zero day）攻擊，因為其利用先前未知的漏洞 ，讓間諜得以滲透易受攻擊的伺服器，並可能植入後門程式，以持續存取受害組織的系統。

荷蘭網路安全公司Eye Security首席駭客 柏納（ Vaisha Bernard）18日發現旗下客戶遭遇駭客攻擊後，與Shadowserver基金會合作進行的網路掃描共發現近100個受害者，而這還是在駭客攻擊背後技術尚未廣為人知前的調查結果。

他不願透露受影響的組織名稱，僅表示已通知相關國家主管機關。

Shadowserver基金會證實有100個組織遭駭客入侵，其中大多位於美國和德國，受害組織包括政府機構。

兩個參與揭露此次網路間諜活動的機構今天表示，截至上週末，針對微軟（Microsoft）伺服器軟體的大規模網攻已影響大約100個組織。。（美聯社）

資安時事案例

蘋果用戶注意！iPhone陷最新資安威脅 4危機這一項最容易被騙

蘋果。記者吳康瑋／攝影

2025-07-18 11:26/科技玩家
經濟日報／ 記者吳康瑋／台北即時報導

Apple 裝置管理與安全領域大廠Jamf（NASDAQ: JAMF）18日發表最新Security 360年度資安 趨勢報告中文版，分析行動裝置（iPhone ）與macOS環境所面臨的威脅現況。該報告除聚焦企業現今面臨的風險之外，並提供資安決策者在保護使用者、裝置、應用程式 與網路層面時可採行的重要洞察與建議。

Jamf產品策略副總裁Josh Stein表示，我們的目標是協助資安領導者掌握影響其組織的風險，不論是來自Mac 或行動裝置，並且提供實質的建議來協助防範日益精密的攻擊 。從存在已久卻依然具威脅性的網路釣魚攻擊，到近期日益嚴重的資訊竊取程式。Jamf一直致力於深入研究各類威脅，不僅為了保護我們的客戶，也為了將這些珍貴洞察回饋給廣大的資安社群。

行動裝置環境面臨的威脅

行動裝置是許多員工主要使用的裝置。不論任何產業，都追求能夠隨時、隨地、從任何裝置連上企業，因此也需要提升員工對常見行動裝置威脅的認知，並採取實際的步驟將駭客 阻絕在外。Jamf的最新行動裝置威脅分析，將全球企業最需要優先處理的威脅分為四大類型：

1.行動裝置網路釣魚

行動裝置讓員工能隨時上網，也讓駭客的觸角不斷延伸。過去12個月來，Jamf已偵測到大約1千萬次網路釣魚攻擊，並且發現有25%的企業曾經遭遇社交工程攻擊，每10位使用者就有1位點選了惡意的網路釣魚連結。員工教育訓練對於防範網路釣魚非常有用。此外，採用一套多層式防護並搭配零信任方法也同樣有效。

2.漏洞 管理

Jamf發現，32%的企業都擁有至少一個含有重大漏洞的裝置，此外，工作用的行動裝置中，有55.1%都正在使用含有漏洞的作業系統。Apple或Google會定期發布資安更新 來修補已知漏洞，因此預防損害最好的辦法就是將裝置更新到最新版本。

3.應用程式風險與惡意軟體

2025年初Jamf發表研究揭露影響iOS裝置透明度、同意及控管（TCC）的漏洞，並示範「側載」（從第三方應用程式商店下載）的應用程式如何侵害使用者隱私權。這說明即便使用最新版的作業系統仍不足以保障企業安全，資安防護必須涵蓋到應用程式層面。

4.惡意軟體與間諜軟體

高風險使用者如記者、政治人物及外交官等，經常成為傭兵間諜軟體的攻擊目標。2024年，Apple曾發布間諜軟體入侵通知給約100個國家的使用者。雖然惡意軟體在行動裝置上出現頻率較低，但一旦發現，往往非常高明且具針對性。企業必須像對待其他端點裝置一樣看待行動裝置，不能對行動裝置惡意軟體的威脅掉以輕心。

macOS環境的威脅趨勢

Mac過去是高階管理和創意工作者在使用的裝置，現在逐漸成為全球各企業日常營運的工具。Mac面臨的威脅也越來越多樣，攻擊手法更加新穎。Jamf的Mac威脅報告將Mac環境的威脅情勢分為三大類：

1.應用程式風險與惡意軟體

Jamf發現，資訊竊取程式占所有Jamf分析到Mac惡意軟體的28.36%，遠高於去年（2024年）報告的0.25%。這些發現也與Jamf的研究相符，不論是從訓練或資安工具的角度來看，高風險的產業領域如加密領域，企業員工必須隨時保持警覺。

2.漏洞管理

Jamf Threat Labs威脅實驗室已多次打破Mac百毒不侵的迷思，去年也發現Gatekeeper中存在漏洞。Gatekeeper 是Mac相當重要的元件，用來防止使用者從網際網路下載到無合法開發者識別碼的應用程式。適當的控管與教育訓練對於防範macOS漏洞所造成風險至關重要。

3.社交工程

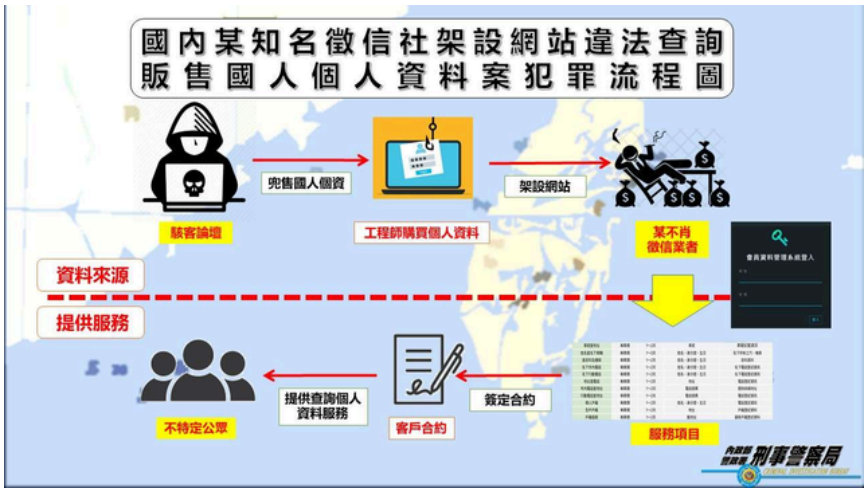
隨著Mac在工作場所日益普及，其攻擊面也不斷擴大。網路釣魚常被認為只侷限於電子郵件，但實際情況絕非如此。Jamf Threat Labs曾經發表一份研究來探討北韓如何在攻擊行動當中使用LinkedIn訊息作為最初的誘餌。訓練員工了解Mac環境可能遭遇的各種網路釣魚型態，是避免不良後果的重要關鍵。

研究方法

Jamf調查Jamf產品所保護的140萬台裝置，分析執行時間為2025年第1季，並重新檢視先前12月的資料，涵蓋全球 90個國家與多種平台，包含iOS、iPadOS、Android行動裝置以及Mac。分析報告以Jamf的威脅情報為基礎，廣泛蒐集來自威脅研究、實際使用數據、新聞分析以及多種資料來源的各種洞察。

個人資料保護法

9300萬筆個資外洩！知名徵信社涉非法蒐集 負責人、工程師被逮



知名徵信社工程師從非法管道購得個資，再用於公司業務之用，甚至在該公司網站上公然標售個資。
圖：警方提供

2025-07-18 16:03 桃園電子報／ 聯合新聞網

國內某知名徵信社涉嫌非法蒐集、販售民眾個資，刑事警察局會同多地警力組成專案小組，於今(114)年6月16日兵分多路在台中西屯區等地執行搜索，查獲9300萬筆外洩個資，並拘提包括實際負責人、網站工程師等10人到案。全案依違反《個人資料保護法》移送士林地檢署偵辦。

刑事局指出，該局科技犯罪防制中心與電信偵查大隊接獲情資，發現有不法集團將巨量個資儲存於私人伺服器中，涉嫌違反個資法。經報請士林地檢署羅姓檢察官指揮，並聯合保三總隊及基隆、桃園、台中、新竹、嘉義、宜蘭等6地警察局展開調查。專案小組追查發現，該資料庫屬於台中某知名徵信社，疑為該公司網站工程師從非法管道購得，再用於公司業務之用，甚至在該公司網站上公然標售個資，外洩筆數高達9300萬筆，包含姓名、電話、住址等敏感資訊，情節重大。

刑事局進一步提到，警方於6月16日展開拘提與搜索行動，查獲包含陳姓實際負責人、薛姓負責人、廖姓網站工程師、副總邱姓經理、會計及多名員工等10人，並查扣資料庫伺服器、WiFi機、電子備份資料與洩漏個資等大量證據。警方指出，該徵信社未經當事人同意，未具正當法律目的，即非法蒐集、處理並利用個人資料，涉嫌違反個人資料保護法第19條第1項之規定，應有特定目的及同條項各款之事由，始得蒐集或處理個人資料，及同法第20條不得任意非法蒐集、處理、利用及洩漏個人資料等情，警詢後依個資法第41條等罪嫌移請士林地方檢察署續辦。

刑事局表示，警方已立即查扣私人伺服器並關閉查詢網站。警方並強調，面對重大個資外洩事件，無論是政府機關或民間企業應定期檢視資安防護機制及進行滲透測試，加強資料庫存取控管與漏洞掃描，杜絕駭客可乘之機。民眾亦不可掉以輕心，應建立資安意識，謹慎保管個人資料，避免在來源不明平台註冊帳號、填寫個資或金融資訊，並定期更新密碼及開啟雙重驗證功能，以降低潛在風險，唯有政府、企業與民眾三方共同強化資安意識與行動，才能有效阻絕個資外洩事件一再重演。

每月一常識

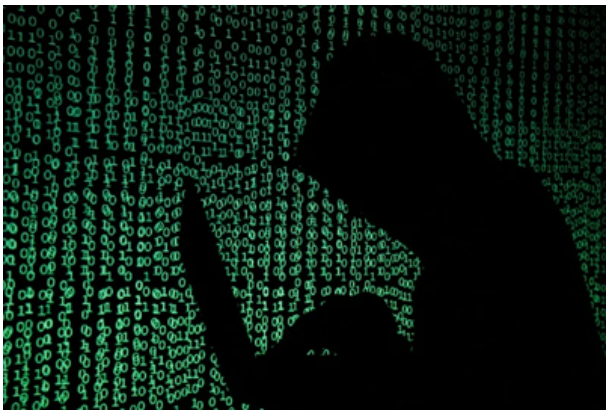
新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

Q16 特定目的是自己說了就算嗎？

A 不行，未來法務部會公布「特定目的」的項目，對於個資的蒐集、處理、利用，都不能逾越特定目的。

文/iThome

公務機關網路電話設備遭外部駭入 數發部提3建議



數發部資安署6月資安月報顯示，有公務機關使用網路電話，發現電話節費盒密碼遭外部人士破解使用進行詐騙。路透

2025-07-19 09:43 中央社／ 台北19日電

數發部資安署6月資安月報顯示，有公務機關使用網路電話，發現電話節費盒密碼遭外部人士破解使用進行詐騙。資安署表示，由於撥打電話顯示為機關來電，嚴重影響聲譽，呼籲機關強化網路電話設備管理，這也是首次觀察到電信公司節費盒密碼遭盜用。

資安署6月資安月報顯示，發現有公務機關電話遭不明人士盜打進行詐騙的案件，調查網路電話撥打紀錄發現，有透過外部IP打電話，結果是機關使用的電信公司節費盒因為設定弱密碼遭到暴力破解。機關發現後立即變更設備的帳號密碼，評估後續使用效益與資安風險，決定停用。

所謂電信公司節費盒是透過網路打電話，不是透過傳統固網，可以降低通話費用。由於這類案件是外部駭入公務機關網路電話設備，導致對外撥出的電話，也會顯示為機關來電，讓接到電話的民眾可能誤以為是機關來電。

資安署向中央社說明，這是首次觀察到電信公司節費盒密碼遭破解而被盜用，有通報資安事件，公部門清查後發現沒有影響內部資通系統，但也已經停用。這類電話恐怕對機關聲譽產生嚴重影響，希望透過分享情資，強化國家整體資通安全防護能量。

資安署指出，網路電話設備如果沒有妥善設定帳號密碼、防火牆及監控機制，很容易成為詐騙集團攻擊漏洞，造成財務損失、影響政府信任度，提出3點建議。

第1，如果透過遠端存取方式管理資通設備，應是「原則禁止，例外允許」。假設機關因地理限制，提供高雄的人員可遠端存取台北的資通設備時，應該要經過審查才能開放遠端存取權限，開放期間應以短天期為限，針對異常連線行為要有管理機制。

第2，強制使用高強度密碼、定期更新並移除預設帳密。資安署指出，部分廠商把產品說明書公開在網路上，內容可能涉及預設密碼，如果後續使用者沒變更預設密碼，易遭有心人士盜用。

第3，評估設備是否支援定期軟體更新與資安修補，避免使用已停產或不受支援的設備。資安署說，設備出廠後有機會出現資安漏洞，因此需要更新軟體，若設備已停產或不再提供更新，就可能出現資安風險，建議納入管理流程，透過定期盤點，評估是否淘汰設備。