114年6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

台灣遭網攻超恐怖 駭客鎖定3大對象！資安國家隊15成員曝光

台灣遭駭客攻擊居亞太地區之冠。（示意圖/達志影像/shutterstock）

05:002025/04/29
中時新聞網

編輯、 吳美觀 、文、先探投資週刊、莊家源
隨著政府、企業數位轉型持續，伴隨而來的網路攻擊、資安事件也隨之增加，台灣身為遭受網路攻擊最頻繁的國家之一，企業、政府對於資安的需求持續增加。

近期亞太區規模最大的資安盛會「台灣資安大會Cybersec 2025」於四月中旬在南港展覽館舉行，今年展覽的亮點主要有三個，首先是ＡＩ時代業者均有相對應的新品和技術；另外，智慧工廠、邊緣運算等風潮，催生新的資安需求，而隨著各國對資安的重視度提升，亦帶動企業加碼資安投資。

網路資安事件創高
今年的台灣資安大會有超過四百家廠商參展，其中包括Google、微軟（Microsoft）、趨勢科技、Fortinet、Palo Alto Networks、CrowdStrike、Symantec等國際知名大廠，國內三大電信公司中華電、台灣大、遠傳也設有攤位，還有眾多國內資訊服務業者如精誠、凌群、邁達特、零壹、關貿、偉康科技、全景軟體、叡揚、安碁資訊等也積極參展。此外，也有不少硬體業者參展，像是安控廠商晶睿、網通業者合勤控及工業電腦業者新漢等。

根據Check Point Research的統計數據顯示，去年全球平均每周網路攻擊次數為一六七三次、年增四四％，其中，台灣的網路攻擊情況最為嚴重，平均每周遭受三九九三次攻擊，位居亞太地區之首，而台灣受攻擊次數最多的前三大產業依序為硬體供應商、政府與軍事機構和製造業。

另外，根據我國數位發展部月報資料顯示，今年三月資安事件通報量達八二件，創下最近半年以來新高，其中大多數是遭到網路分散式阻斷服務（DDoS）攻擊，包含部分縣市政府、地方稅務機關等，導致網站服務緩慢或中斷，但並未造成系統被破壞，各機關多可在短時間內恢復。

因應日漸嚴重的駭客攻擊，台灣的數發部及金管會，針對上市櫃公司均祭出新的資安法規，要求國內六五家金融業者，必須設立資安長（CISO），除了定期召開資安長聯繫會議，強化網路身分驗證，核心資料、資料庫加密與分持，並有雲端備份機制等，再加上二○二七年歐盟網路韌性法案（ＣＲＡ）即將上路，未來在歐盟市場上的數位產品和服務需要通過自查或協力廠商檢查，確認滿足歐盟網路安全標準才可銷售，再加上近年智慧工廠及邊緣運算的興起，科技業的資安標準提升，都將成為企業資安投資的重要動能之一。

精誠、零壹擴大海外布局
根據ＭＩＣ統計，今年資安相關領域（設備、軟體及服務）全球市場規模約二三九二・二億美元，明年將成長至二六○九億美元、年增九・○九％，二○二二～二六年的年複合成長率為十・六四％，其中以軟體與服務的產值占比最高，分別占五一％與三八％；工研院則指出，明年台灣資安市場整體規模將達一○一○億新台幣，二二～二五年的年複合成長率為十・一一％。（全文未完）
全文及圖表請見《先探投資週刊2349期精彩當期內文轉載》

美25歲駭客用AI繪圖外掛入侵迪士尼 盜取1.1TB資料還恐嚇員工「恐面臨10年刑期」

（示意圖／pixabay）

CTWANT/編輯：廖梓翔 2025-05-12　14:04

美國司法部（Department of Justice）近日表示，駭客代號為「NullBulge」的25歲男子克雷默（Ryan Mitchell Kramer）目前，已同意就入侵迪士尼公司電腦系統的行為認罪。這起案件牽涉AI生成藝術工具的惡意操作與數據竊取，為近年來AI領域相關資安事件中最具爭議的案例之一。

根據外媒報導指出，司法部新聞稿表示，克雷默即將承認兩項聯邦重罪指控，包括「非法存取電腦並取得資訊罪」以及「威脅破壞受保護電腦罪」，每項罪名最高可判處5年聯邦監禁，共計10年刑期。

這起案件的核心在於一款廣泛使用的AI圖像生成介面工具ComfyUI，該工具為開源平台Stable Diffusion的擴充套件，主要透過Github發布。克雷默在ComfyUI中植入一個特洛伊木馬，進而入侵安裝該工具的使用者電腦。

透過這個後門，克雷默得以未經授權地存取多位使用者的系統，其中一人正是迪士尼公司的員工。他藉由該員工的電腦登錄迪士尼的Slack系統，並下載多達1.1TB的公司內部資料。

根據2024年7月的記錄，克雷默以「NullBulge」之名與該員工聯繫，威脅將其個人資訊外洩。由於該員工未做出回應，克雷默最終真的將資料公開。

克雷默曾在ComfyUI的Github頁面上留下聲明，聲稱其行為出於對AI藝術生成的意識形態抗議。他認為AI藝術對創意產業造成損害，應該受到限制。他寫道「也許你們可以看看我們的行動，然後對於在如此安全性薄弱的帳號上發布AI工具再三考慮。」

根據資安公司vpnMentor指出，克雷默所修改的ComfyUI版本不僅植入惡意代碼，還能入侵用戶的加密貨幣錢包、注入木馬程式並大量竊取個人資料。另一間資安公司SentinelOne的研究報告則曝光，NullBulge早已是一名長期從事惡意駭客活動並牟利的網路攻擊者。

雖然目前克雷默的認罪協議僅限於迪士尼案，但司法部指出，他已承認至少還有另外兩名受害者在不知情的情況下安裝了他所修改的惡意檔案，使他得以侵入他們的電腦與帳號。聯邦調查局（FBI）正持續深入調查此案，是否涉及更大範圍的網路入侵與資料外洩尚待進一步釐清。

台新銀催收信函、信用卡帳單爆疏失「個資外洩4年」 金管會重罰600萬

周刊王CTWANT |網編組
2025年5月8日 週四 下午5:37

台新銀行。（圖／報系資料照）

金融監督管理委員會今（8）日正式公告，針對台新國際商業銀行（下稱台新銀行）催收信函和信用卡帳單錯寄，導致大量用戶個資外洩，情節嚴重，依法重罰600萬元。最離譜的是，台新銀行相關缺失持續4年之久都未察覺，金管會痛批該行內控系統形同虛設。

金管會表示，台新銀行自109年至今，系統與調整過程中，催收信函地址未同步更新，累積有1089人受影響，恐怕已將用戶個人資料寄錯對象。另外，113年11月台新銀行委外資訊廠商列印信用卡帳單，機台感測器故障導致正反兩面屬於不同用戶，有358名持卡人資料錯置，用戶個資全被看光。

金管會也說明，台新銀行對內未確實執行測試及驗收之作業規範，對外亦未有效督導受委託機構建立完善之內部控制制度，核有未完善建立及未確實內部控制及作業制度之情事，因此違反銀行法第45條之1第1項、第3項及其分別授權訂定之「金融控股公司及銀行業內部控制及稽核制度實施辦法」第3條第1項、第8條第1項及「金融機構作業委託他人處理內部作業制度及程序辦法第6條第1項規定，爰金管會依銀行法第129條第7款規定，故核處新臺幣600萬元罰鍰。

最後金管會對台新銀行提出多項要求，須強化委外廠商管理與資訊人員稽核能力，應將歷年資安缺失全面清查，以防類似事件再發生；以及台新銀行須全面檢視資訊系統進行調整或變更時，跨系統間資訊傳輸之正確性，並建立事前、事中、事後檢核機制，且本案相關改善措施應經外部獨立第三人查核並提報董事會報告，並由稽核單位列管追蹤及納入內部查核重點。

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

Q14　在什麼情況下蒐集個資，不受個資法規範？

A　目前有兩種情況下不受個資法規範：為了個人或家庭活動的目的，而蒐集、處理、利用個人資料；以及在公開場所或公開活動中所蒐集、處理、利用之未與其他個人資料結合之影音資料。

文/iThome

蘋果AirPlay有安全漏洞！電視、喇叭恐遭駭客入侵

資安研究人員發現蘋果AirPlay有漏洞。（圖／美聯社／達志）

CTWANT/編輯：薛羽彤 2025-05-03　08:31

資安研究人員發現蘋果AirPlay協定及 AirPlay軟體開發套件（SDK）有一組重大漏洞，可讓攻擊者在不與用戶互動下，遠端接管蘋果和第三方裝置包含智慧電視、機上盒、喇叭、CarPlay等等。資安專家建議應該儘速更新設備軟體，或完全停用。

據外媒報導，資安業者Oligo最新報告指出，發現一組名為「AirBorne」的AirPlay漏洞，只要駭客能連線同一組Wi-Fi網路，就能遠端傳送惡意程式碼，可能被用來執行遠端程式、存取控制清單、繞過與使用者的互動、任意存取本地端檔案、外洩敏感資訊、中間人攻擊，以及服務阻斷攻擊，甚至經由麥克風竊聽對話。

AirPlay是蘋果所開發的無線通訊協定，可在相容的裝置之間傳送多媒體串流、螢幕畫面，以及相關的元資料，不管是iPhone、iPad、Mac、HomePod或Apple TV等蘋果裝置都支援AirPlay，透過SDK支援AirPlay的第三方裝置，則涵蓋了多個品牌的智慧電視與喇叭等。

Oligo技術長強調，全球Airplay使用的裝置實在太多，有些裝置甚至根本從不下載修補程式，倘若遭到入侵，恐怕要花好幾年時間修復，甚至完全不會執行漏洞修補。

Oligo建議使用者用戶最好儘速升級到最新版本，在不使用的情況下直接禁用AirPlay接收器，此外也可以實作防火牆規則，或將AirPlay許可權設定為「僅現有用戶」以降低感染風險。