資安儀表板

事件通報、聯防監控、蜜罐誘捕、外部曝險分析及網路巡查高風險詐騙等五類量化指標

■ 事件通報

近一週公務機關資安事件通報之類型與數量，同時包含民營機構依規定揭露重大資通安全訊息。

- 公司名稱：易飛網國際旅行社股份有限公司
- 發布時間：114/7/28
- 事件說明：公司接獲少數客戶反應疑似個資外洩事件，經評估對公司財務及業務並無重大影響

表1 | 本週企業重訊發布列表

本週總計1家民間企業發布重大訊息，詳見表1，產業類別屬旅行業。

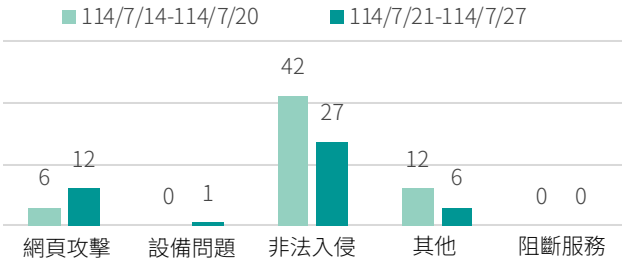

圖1 | 本週公務機關資安事件通報概況

▶提醒使用者要持續加強資安意識，注意郵件來源正確性與隨身儲存環境安全。

本週總計接獲46件事件通報，詳見圖1，非法入侵類型中持續觀測到機關因安裝冒牌軟體產生惡意程式特徵之連線，但相較於上週數量較為減少；此外亦有機關疑似因社交工程或可卸除式磁碟(例如隨身碟、錄音筆)感染惡意程式，以致連線惡意中繼站。

■ **聯防監控** 近一週以MITRE ATT&CK Matrix分析攻擊者行為，提醒公務機關留意攻擊趨勢變化，是否由初期之偵測刺探進入影響層面更大竊取資料與破壞資通系統。

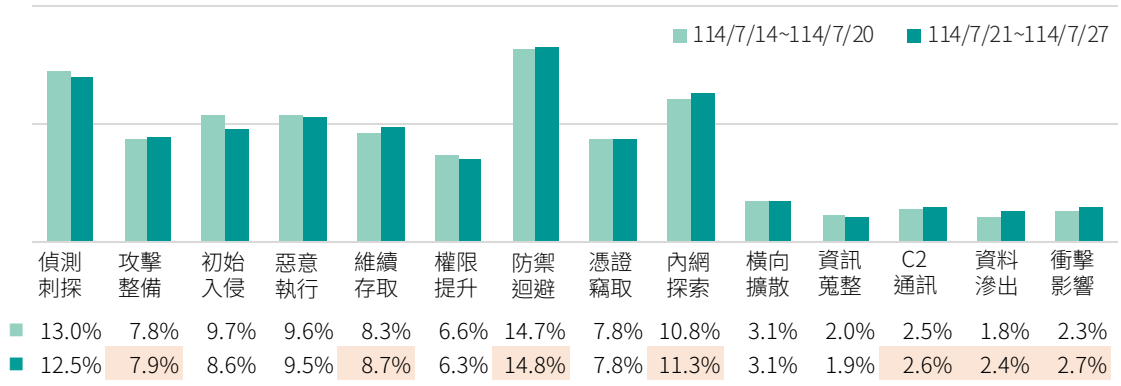

圖2 | 資安聯防監控攻擊階段統計

本週政府領域資安聯防監控參考MITRE ATT&CK Matrix分析TTP戰術框架分布顯示，本週趨勢相較上週無顯著差異，詳見圖2，「防禦迴避」為最常見攻擊手法，占比14.8%，攻擊者常透過關閉或清除指令紀錄，並以系統合法工具間接執行惡意命令，以規避監控，建議導入端點防護，強化指令紀錄稽核、限制高風險工具濫用，並落實特權帳號管理，以防範攻擊者規避偵測並抹除行為痕跡。

「衝擊影響」階段占比2.7%，主要為攻擊者嘗試透過大量連線或封包癱瘓應用層、服務端口或網路頻寬資源，可能造成系統無法回應正常請求。

▶建議部署流量清洗與速率限制機制，搭配服務資源管控與異常行為監控，強化系統對大規模連線與封包耗盡攻擊的韌性與即時應對能力。

■ **蜜罐誘捕** 近一週誘捕系統所捕捉到的攻擊樣態趨勢變化以及所利用的弱點趨勢。

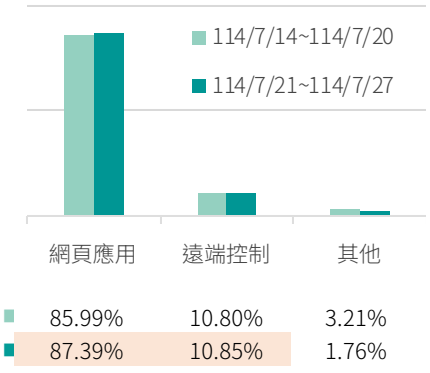

圖3 | 本週蜜罐系統觀測攻擊行為動態

本週透過部署於國內外之蜜罐系統觀測攻擊行為動態，詳見圖3，相較於上週「網頁應用」服務攻擊占比85.99%、「遠端控制」服務攻擊占比10.8%，本週各類服務之平均偵測攻擊比例無明顯變化，結果顯示「網頁應用」服務仍為攻擊主軸，占比高達 87.39%。「遠端控制」服務亦有 10.85% 的偵測比例，反映攻擊者仍積極針對公開遠端連線介面進行入侵行動。

▶由於網頁應用是最為常見之對外服務類型，若存在已知漏洞或弱點，將面臨高風險曝露情形，易成為攻擊者入侵與滲透重要管道，須做為優先防護之項目。

類型 ■遠端程式碼執行漏洞 ■檔案上傳漏洞 ■權限提升

排名		漏洞編號	受影響產品	CVSS 3.x Base Score
■ 1		CVE-2021-38647	Microsoft OMI管理伺服器	9.8
■ 2		CVE-2016-3088	Apache ActiveMQ訊息代理程式	9.8
■ 3	↑NEW	CVE-2023-20198	Cisco IOS XE網通設備作業系統	10.0
■ 4	↓1	CVE-2017-17215	Huawei路由器	8.8
■ 5		CVE-2024-36401	GeoServer	9.8
■ 此為新型漏洞尚未進入排行		CVE-2025-24813	Apache Tomcat	9.8

表2 |本週前5大攻擊使用之漏洞排行列表

進一步解析國內外之蜜罐系統誘捕漏洞攻擊之情形。詳見表2，前5大攻擊以「網頁應用」服務之漏洞為主要入侵路徑，本週漏洞類型多集中於遠端程式碼執行、檔案上傳漏洞與特權提升漏洞，攻擊目標涵蓋應用伺服器、開源套件、作業系統及路由器，顯示此類系統已成為高風險熱點。其中，Cisco IOS XE 網通設備作業系統之 CVE-2023-20198 漏洞於本週首度進入前5名，攻擊排行上升至第3名。

除上述漏洞外，本週誘捕亦發現Apache Tomcat的CVE-2025-24813新型漏洞遭攻擊利用，其為複合型態的遠端程式碼執行（RCE）與資訊洩露漏洞。該漏洞源於 Apache Tomcat 預設 Servlet伺服器端程式在不當設定下，未正確處理含有內部點號路徑之請求，導致攻擊者可利用特製請求進行讀寫敏感檔案或觸發遠端程式碼執行。

▶建議存在漏洞之設備應更新至最新版本軟體或韌體以修補漏洞；若原廠已無法提供更新支援，應考慮汰換存在漏洞之設備或軟體套件，如因故無法汰換，應採對應之漏洞緩解措施。

▲ 近期重大弱點提醒

近一週本院研究人員發現以下重大弱點資訊，建議組織內部進行檢查與修補：

▶建議儘速更新至最新版本

- Sophos防火牆之Secure PDF eXchange (SPX)功能與Legacy (Transparent) SMTP Proxy分別存在2項高風險安全漏洞(CVE-2025-6704與CVE-2025-7624)，類型分別為任意檔案寫入(Arbitrary File Writing)與SQL注入(SQL Injection)，前者可使未經身分鑑別之遠端攻擊者執行任意程式碼，後者則允許攻擊者於電子郵件處理過程中注入惡意SQL指令以達成遠端程式碼執行
- 達煬科技WinMatrix3應用程式伺服器端與Web套件存在2個高風險安全漏洞(CVE-2025-7916與CVE-2025-7918)，類型分別為反序列化漏洞(Insecure Deserialization)與SQL注入(SQL Injection)，兩者分別可使未經身分鑑別之遠端攻擊者透過發送惡意序列化內容於伺服器端執行任意程式碼與注入任意SQL指令讀取、修改及刪除資料庫內容

■ 外部曝險分析

經由外部檢測，政府機關資通安全狀況，例如使用EASM工具或實兵演練，及早發現曝露於外部之風險。

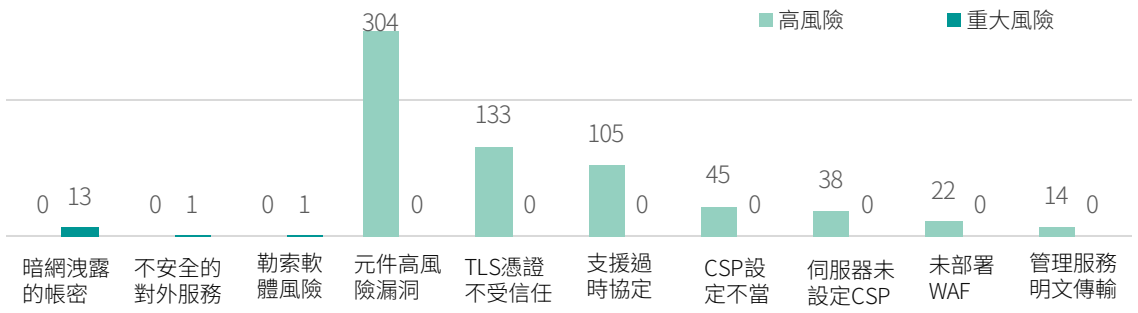

圖4 | EASM檢測結果統計(前10大風險)

本週針對55個公部門單位執行EASM資安曝險檢測，本次統計係擷取前十大風險項目(包含重大與高風險)，重大風險共計15項，與上週持平，風險類型亦無明顯變化。高風險弱點共計661項，顯示部分單位面臨多重高風險弱點威脅，詳見圖4。

▶建議相關單位儘速清查並更新可能外洩之帳號密碼，關閉非必要對外服務，定期備份關鍵資料，並優先修補或升級存在漏洞之系統元件、更換無效的TLS憑證，以及停用不安全通訊協定，以強化資安防護，降低弱點遭利用之風險。

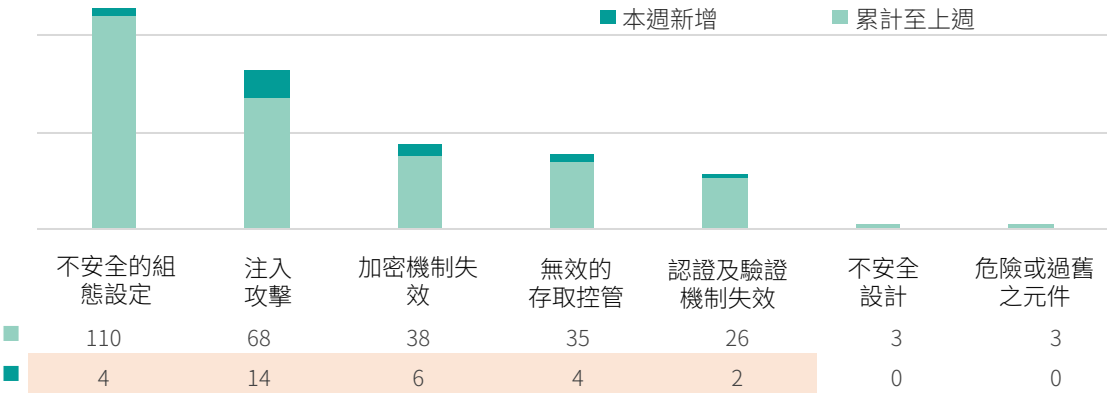

圖5 | 網路攻防演練資通系統實兵演練統計

本年資通系統實兵演練針對政府機關與關鍵基礎設施提供者，並於擇定時間針對前述機關進行演練，詳見圖5，至7/27止已累計313筆攻擊紀錄，本週新增弱點數量共30筆，分別為「注入攻擊」14筆、「加密機制失效」6筆、「不安全的組態設定」4筆、「無效的存取控管」4筆及「認證及驗證機制失效」2筆。部分系統未妥善處理輸入內容，導致可透過網址注入惡意指令，進一步存取資料庫帳號密碼等敏感資訊；亦有系統因設定不當，導致原始碼外洩，攻擊者利用提權工具執行程式碼，取得作業系統控制權限。

■ 網路巡查高風險詐騙

追蹤詐騙訊息與手法演變，掌握政府機關實施之打詐政策與機制，是否達成其控制目標。

根據團隊研究發現，近期產品服務類詐騙數量顯著上升，內容多以「分享立即領取」、「免費試用」、「線上課程限時贈送」等話術進行包裝，藉由看似無害且高互動性的訊息，誘使民眾點擊連結或留下個資，進而引導至高風險外部平台，如圖6、圖7所示。

圖6 | 主題為多肉植物分享活動的詐騙廣告

圖7 |主題為免費課程的詐騙廣告

▶為應對此類新興詐騙樣態，本院已投入新的偵測模型，強化對文宣語言結構、誘導機制與連結行為的自動化分析能力，期望能提升系統對變形詐騙的即時辨識效能，並協助相關單位進行風險通報與社群內容下架處理。

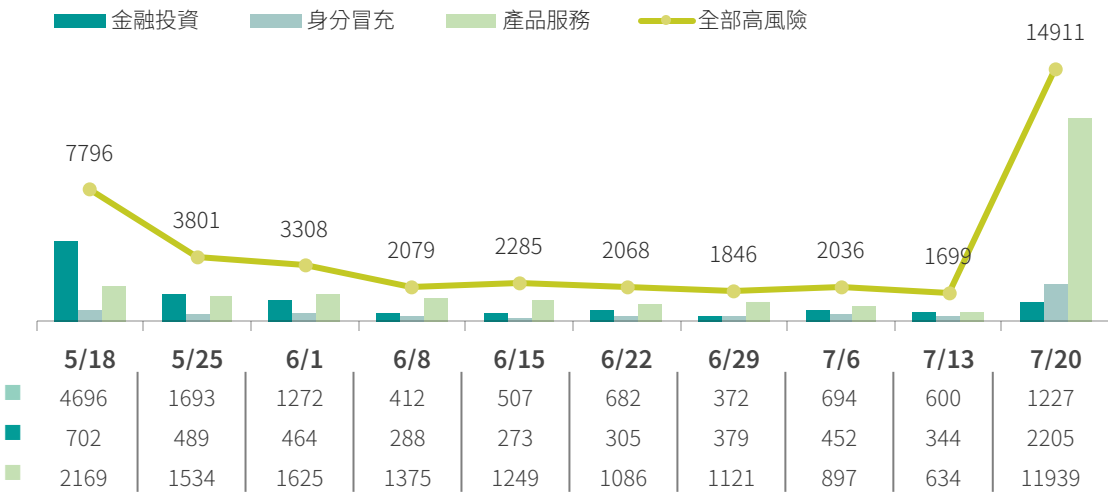

圖8 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙週趨勢

本院於網路巡查中偵獲之高風險詐騙案件總量，以及其中金融投資類、身分冒充類、產品服務類詐騙之週趨勢統計，詳如圖8所示。本週偵獲案件總量與產品服務類詐騙數量大幅增加，即是新偵測模型之強化效果。

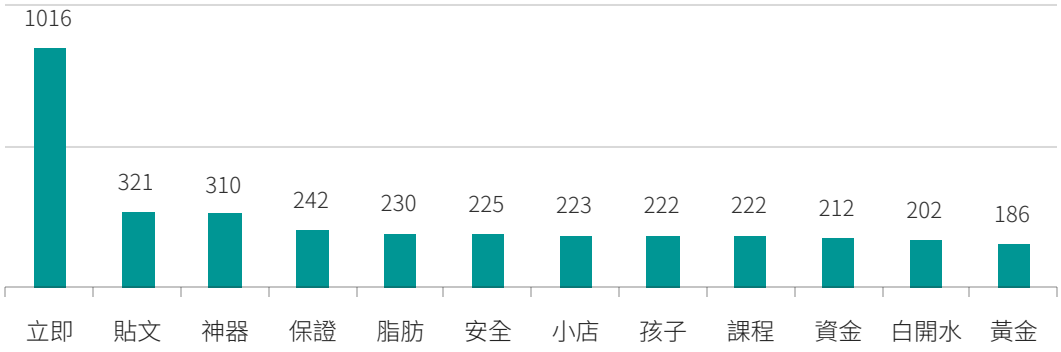

圖9 | 本週 Top12 詐騙關鍵字排名

本週通報的代表性詐騙關鍵字前12名，詳見圖9。除了延續先前的投資理財、免費諮詢貸款誘騙手法之外，本週出現了以**「神器」**、**「脂肪」**、**「白開水」**等為主的虛假瘦身、保健產品詐騙。**「立即」**、**「保證」**等字眼則持續用於強化急迫性與可信度，以促使受害者快速下單。

此外，本週也特別注意到透過教育「課程」折扣、「黃金」飾品、「小店」出清庫存等名義，以私訊留言或貼文互動，誘騙民眾主動提供個資或付款資訊，落入詐騙陷阱。

焦點文章

建立資安實務人才培育新模式：推動網路安全實務與社會人才培訓及實習輔導計畫

計畫緣起

面對日益頻繁且複雜的資安攻擊，強化組織的資安韌性與培育實務人才已成為當務之急。在Google.org的支持下，資安院啟動為期兩年的NICS臺灣資安計畫，並自去年著手推動「網路安全實務與社會人才培訓及實習輔導計畫」，借鏡美國網路安全診所聯盟（Consortium of Cybersecurity Clinics, CCC）之課程概念，攜手國內大專院校打造本土化「資安健檢團」模式。

資安健檢團是一種結合理論學習與實務應用的創新課程模式，由大學院校教授開設選修課程，並與修課學生共同組隊，提供健檢服務。課程前十週為知識講授，後六週則實地走進中小企業及非營利組織服務，深入了解其資安現況與需求，並根據需求提出政策面、人員意識面或技術面之改善建議。推動過程須串聯政府、學界與民間組織多方角色，資安院作為協調者，負責整合資源、提供課程指引與品質把關，過程挑戰重重。

執行成果

截至目前，資安院已與全台9所大學合作，完成培訓三百多位學生，實地服務五十多間組織，涵蓋社會福利、公益教育、醫療服務等類型組織。健檢團深入晤談與診斷，協助組織發現過往未察覺的資安風險，如帳號權限管控不足、缺乏資料備份機制及資安意識仍待提升等問題。其中，對於資安意識提升部分，更是有團隊規劃社交工程演練，協助組織識別較為脆弱的防護環節，進行針對性的教育訓練，強化員工資安意識與警覺性。

後續規劃

資安院正積極爭取後續資源，未來也將擴大合作學校與服務對象，並建立更完善的媒合機制，讓更多有資安需求的組織能夠受惠。

關鍵字
資安健檢團、人才培育、中小微型企業、非營利組織、資安韌性

刊　　名　資安週報試刊號第3期
發 行 人　國家資通安全研究院　林盈達院長
主　　編　國家資通安全研究院　國際合作及資安治理中心
出 版 者　國家資通安全研究院
網　　址　www.nics.nat.gov.tw
讀者信箱　www.nics.nat.gov.tw/mail2center/

國家資通安全研究院
National Institute of Cyber Security