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。

■ 本週無企業發布資通安全事件重大訊息。

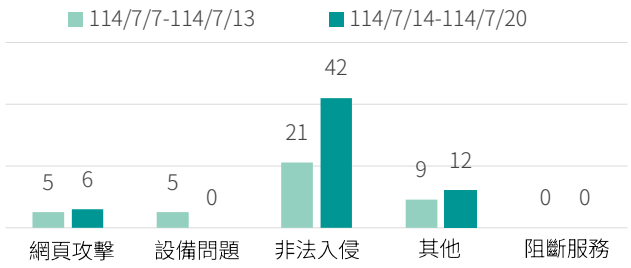


圖1 | 本週公務機關資安事件通報概況

本週總計接獲**60**件事件通報，詳見圖1，以非法入侵類型居多，仍為機關接獲資安院警訊通知，資訊設備疑似安裝冒牌軟體，產生符合惡意程式特徵之連線為主。

▶再次提醒使用者下載任何應用程式前，請先至官方網站確認其網址是否正確，以確保資訊系統安全。

■ 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。

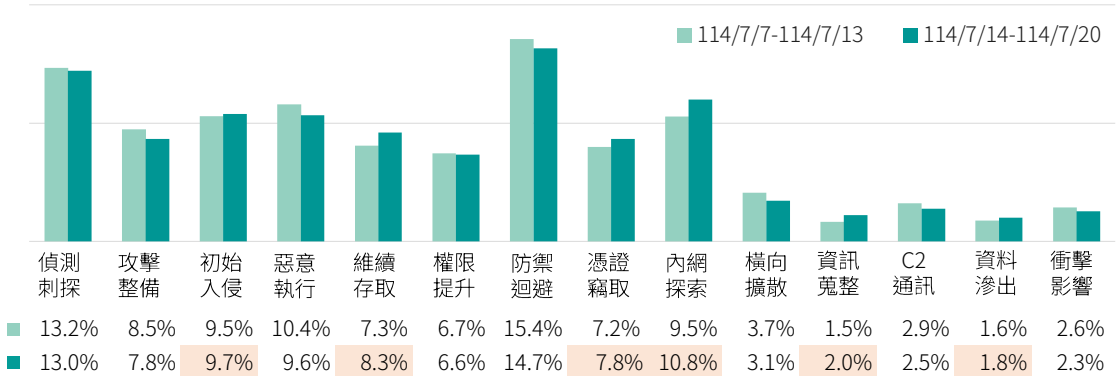


圖2 | 資安聯防監控攻擊階段統計

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（Defense Evasion）為最常見攻擊手法，占比14.7%，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。

■ **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。

「網頁應用」仍為國內外攻擊行為主軸，須優先防護

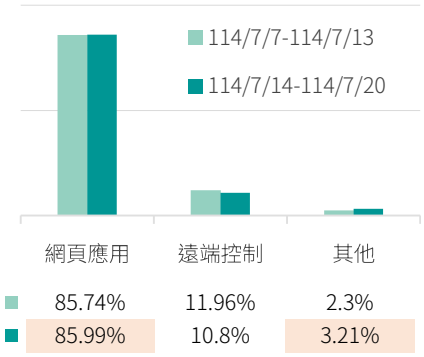


圖3 | 本週蜜罐系統觀測攻擊行為動態

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85.74%、「遠端控制」服務攻擊占比11.96%。

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 85.99%。「遠端控制」服務亦有 10.8% 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。

▶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

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	↑1	CVE-2016-3088	Apache ActiveMQ訊息代理程式	9.8
■ 3	↓1	CVE-2017-17215	Huawei路由器	8.8
■ 4		CVE-2023-42793	TeamCity伺服器	9.8
■ 5		CVE-2024-36401	GeoServer	9.8

表1 |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1，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與檔案上傳漏洞，攻擊目標涵蓋路由器、應用伺服器及開源套件，顯示此類系統已成為高風險熱點。

▶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；如原廠已無更新支援，應研議汰換具該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，官方多數已經發布新版：

▶建議儘速更新至最新版本

- Cisco ISE與ISE-PIC未有效驗證特定API參數(CVE-2025-20337)，未經身分鑑別之遠端攻擊者以root權限在底層作業系統上執行任意程式碼。
- 微軟SharePoint Server存在反序列化漏洞(CVE-2025-53770)，未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼，微軟警告已發現利用此漏洞之惡意活動。
- 桓基科技開發之iSherlock存在OS Command Injection 漏洞 (CVE-2025-7451)，允許未經身分鑑別之遠端攻擊者注入任意作業系統指令並於伺服器上執行。

▶建議儘速確認並進行修補或暫時停用

- WordPress部分擴充功能出現10個嚴重風險資安漏洞 (CVE-2020-36847、CVE-2020-36849、CVE-2025-5392、CVE-2025-5393、CVE-2025-5394、CVE-2025-6058、CVE-2025-7340、CVE-2025-7341、CVE-2025-7360 及 CVE-2025-7401)，包含 AIT CSV import/export、Alone – Charity Multipurpose Non-profit、GB Forms DB 1.0.2、HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder、Premium Age Verification / Restriction、Simple-File-List及WPBookit，以上漏洞皆有遠端程式碼執行之風險。除 Premium Age Verification / Restriction套件尚未釋出更新，建議停用之外，其餘套件應儘速更新。

■ 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。

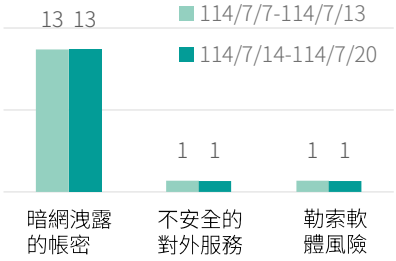


圖4 | 重大風險發現數量

本週針對55個公部門單位執行EASM資安曝險檢測，重大風險發現(Critical Finding)數量共計15個，與上週相同，風險類型亦無明顯變化，顯示重大風險曝險項目仍持續存在，詳見圖4。

▶建議相關單位加速清查並更新受影響帳號密碼，關閉不必要對外開放之服務，以及定期備份關鍵資料，強化端點防護與漏洞修補作業。

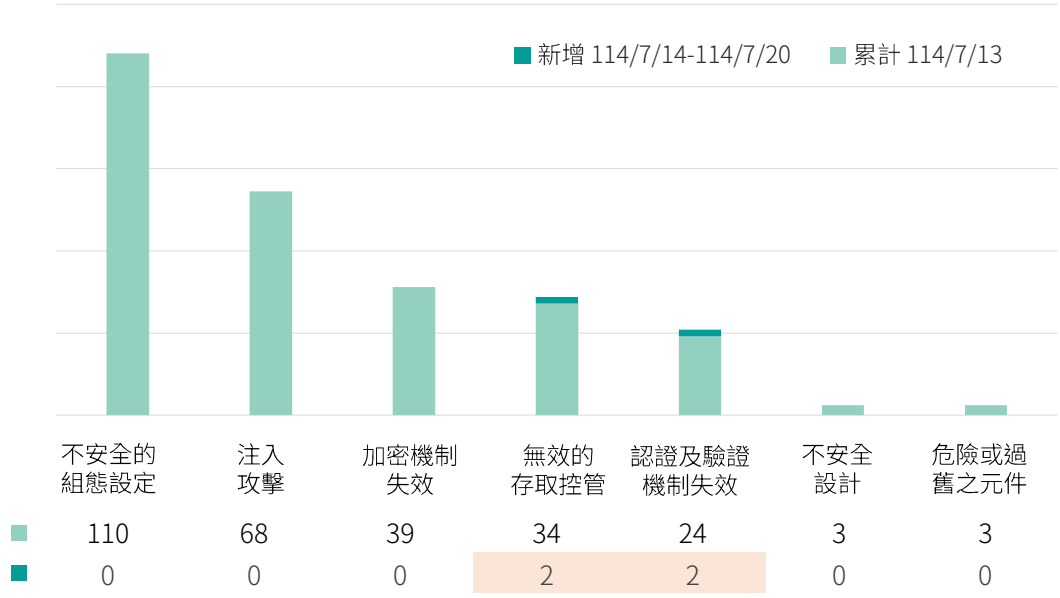


圖5 | 網路攻防演練資通系統實兵演練統計

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7/20止已累計285筆攻擊紀錄，本週新增弱點數量分別為「無效的存取控管」2筆與「認證及驗證機制失效」2筆，導致使用者可透過異常方式存取或操作未授權資源，曝露或竄改系統資訊，或能取得其他使用者帳號，進而洩漏機敏資料。

▶為避免此類風險，後台應落實權限驗證機制，建議系統根據使用者身分，判斷其可操作範圍，避免接受來自前端手動指定重要參數，以強化整體存取控制。

▶同時也建議加強使用者認證流程，避免身分偽造或繞過驗證機制，提升整體帳號安全性。

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。

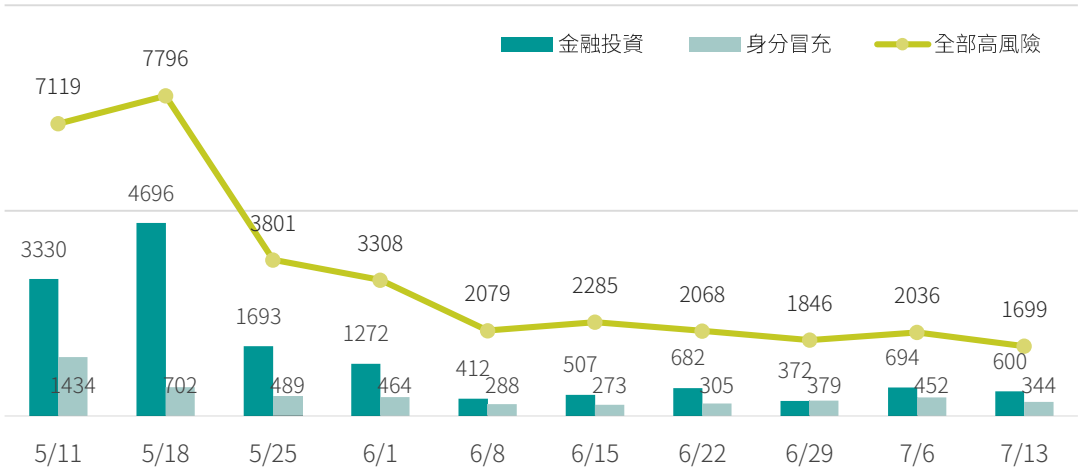


圖6 | 偵獲高風險金融投資類及身分冒充類詐騙週趨勢

本院於網路巡查偵獲之高風險詐騙總數，以及金融投資類、身分冒充類詐騙之週趨勢統計，詳見圖6。可看出詐騙數量自五月中旬起已逐步降低，原因可能與政府強力要求平台業者積極下架詐騙廣告有關，但同時本院仍應持續精進、強化分析能力，避免詐騙集團針對偵測機制進行反制。

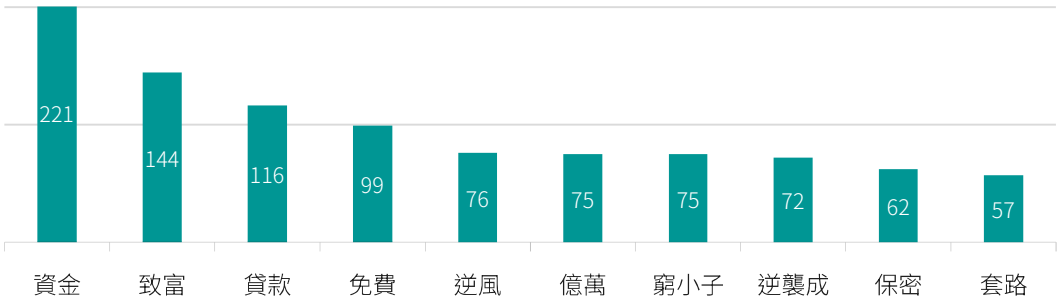


圖7 | 本週 Top10 詐騙關鍵字排名

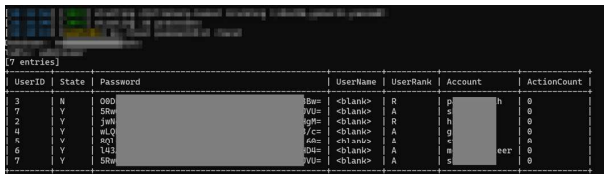
本週的通報詐騙關鍵字統計排名前10名，詳見圖7。除了延續先前的快速致富、投資理財、融資貸款等主題外，本週明顯強化了以「**窮小子**」、「**逆風**」、「**逆襲成**」、「**億萬**」等為主的情緒激勵與勵志翻身包裝手法。這類關鍵字透過逆襲成功的故事情節，營造從貧窮或債務困境迅速致富的幻想，誘騙受害者輕信並投入資金。此外，也透過「**免費**」、「**保密**」、「**沒有套路**」等強調他們不是詐騙、零風險與保密性的包裝伎倆，藉此進一步降低民眾的戒心，使其更容易陷入詐騙陷阱。

焦點文章

網路攻防演練統計與案例

網路攻防演練主要係針對政府機關與關鍵基礎設施提供者執行資通系統實兵演練，運用駭客常用攻擊手法，對機關之對外服務系統(含共用性系統)與連網設備進行攻擊，以發現可能存在之資安漏洞。資通系統實兵演練截至7月20日已累計285筆攻擊紀錄，包含5筆重大衝擊性弱點、46筆高衝擊性弱點、7筆中衝擊性弱點及227筆低衝擊性弱點，主要發現弱點案例如下：

■ 案例1



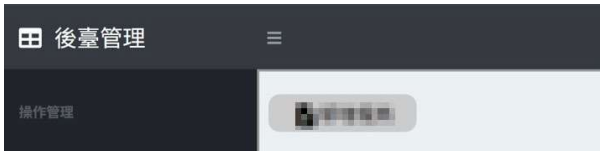
「注入攻擊」弱點

某機關之網站存在「注入攻擊」弱點，攻擊者透過網址取得參數後，使用攻擊工具，成功取得資料庫中儲存之系統帳號與密文密碼。

■ 案例2

「加密機制失效」弱點

某機關之網站存在「加密機制失效」弱點，攻擊者使用網頁開發人員工具於網頁原始碼取得帳號與密碼。



利用發現之帳號密碼進行登入，成功取得管理者權限並竄改頁面。

▶改善建議

針對網頁任何來源之輸入內容，皆應進行過濾，避免非預期的輸入內容造成系統異常或執行非預期的指令，導致系統權限被取得或是資訊外洩。此外，系統於開發完成後應進行相關資安檢測作業，確認敏感系統資訊無法從任何公開頁面被取得，所導致之風險。

關鍵字 網路攻防演練、資通系統實兵演練、弱點

刊　　名　資安週報第2期　試刊號
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