資通安全網路月報

一、近期政策重點

第七期「國家資通安全發展方案(114 年至 117 年)」，以「建構信賴安全之數位社會」為願景，設定「強化全社會資安防禦韌性」、「豐富資安產業生態系」及「構築新興科技防禦技術」為三大目標，並擬具「全社會資安防禦」、「提升關鍵基礎設施資安韌性」、「壯大我國資安產業」及「AI 新興資安科技應用與合作」四項推動策略，由中央各部會及地方政府，共同推動資安防護，以發揮國家整體資安聯防綜效。

二、資通安全趨勢

(一) 我國政府整體資安威脅趨勢

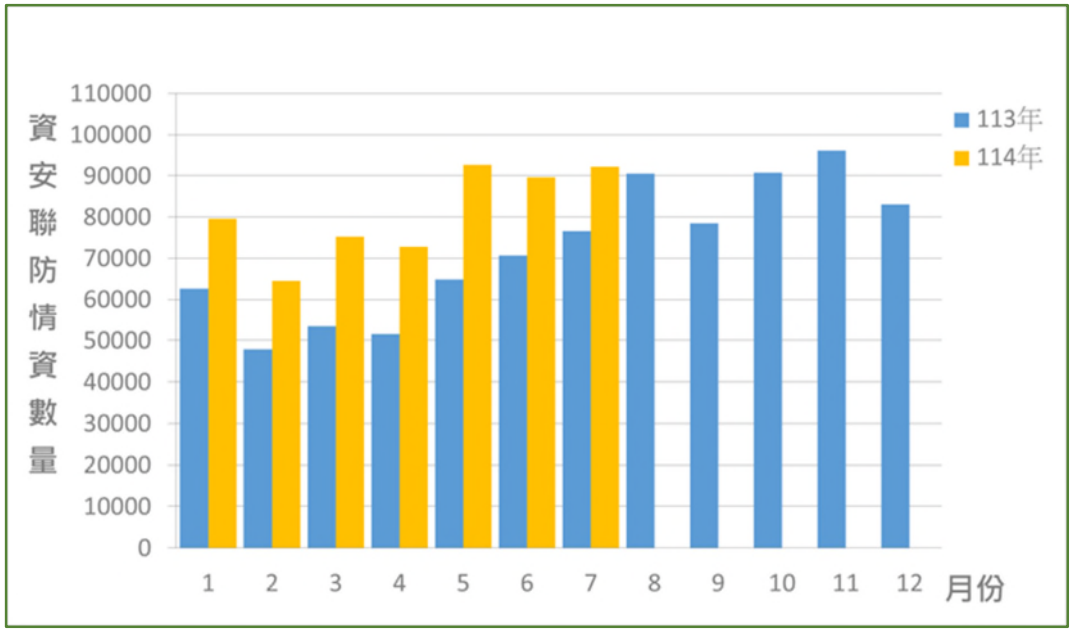
事前聯防監控

本月蒐整政府機關資安聯防情資共 9 萬 2,214 件(增加 2,539 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(36%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵攻擊類(35%)，大多是系統遭未經授權存取或取得系統/使用者權限；以及入侵嘗試類(20%)，主要係嘗試入侵未經授權的主機。統計近 1 年情資數量分布，詳見圖 1。

注意以產品報價為題之社交工程郵件

經進一步彙整分析聯防情資資訊，發現近期駭客偽稱提供業務相關產品報價，寄送內含罕見副檔名.ARJ 之社交工程郵件，並將附件檔名偽裝為常見文件格式（如 pdf），企圖混淆收件人判斷，點擊開啟惡意附件。當收件人執行該惡意程式後，將連線至

Google 雲端硬碟下載 2 階惡意檔案，進一步達成控制收件人電腦



之目的，相關情資已提供各機關聯防監控防護建議。

圖 1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共 235 **件，較去年同期減少** 12.64%，**通報類型以非法入侵為主，持續觀察到多個機關資訊設備疑似安裝冒牌軟體，產生符合後門程式特徵之連線，占本月非法入侵通報件數** 37.96%。**近** 1 **年資安事件通報統計詳見圖** 2。

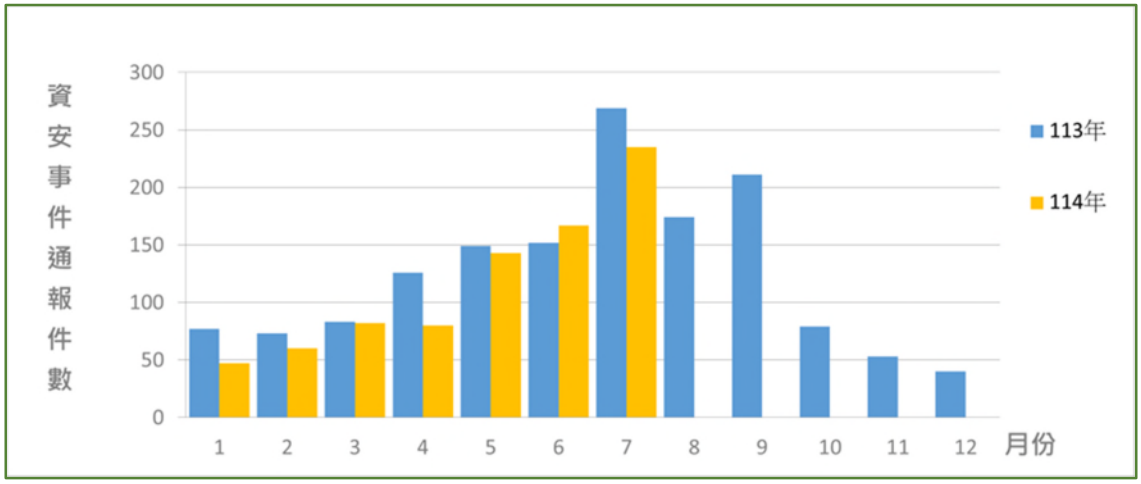


圖 2 資安事件通報統計

(二) 重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	網通設備 Fortinet FortiWeb 存在安全漏洞 嚴重程度：CVSS 9.6 (CVE-2025-25257)	● 研究人員發現 Fortinet FortiWeb 存在驗證繞過(Authentication Bypass)漏洞(CVE-2025-25257) ● 未經身分鑑別之遠端攻擊者可注入任意 SQL 指令讀取、修改及刪除資料庫內容。 ● 官方已針對漏洞釋出修復更新，請參考官方說明儘速確認並進行修補。
	系統平台 Cisco 整合通訊管理平台存在高風險安全漏洞 嚴重程度：CVSS 10 (CVE-2025-20309)	● 研究人員發現 Cisco 整合通訊管理平台(Unified Communications Manager)存在使用硬編碼之帳號通行碼(Use of Hard-coded Credentials)漏洞(CVE-2025-20309 ● 未經身分鑑別之遠端攻擊者可利用透過 SSH 協定以無法變更之 root 權限帳號通行碼登入設備，進而取得設備完整控制權。 ● 官方已針對漏洞釋出修復更新，請參考官方說明儘速確認並進行修補。
已知遭駭客利用之漏洞	網通設備 Citrix｜NetScaler ADC and Gateway 嚴重程度：CVSS 9.3、8.7 (CVE-2025-5777、CVE-2025-5349)	● NetScaler ADC 和 NetScaler Gateway 12.1 和 13.0 版本現已停產(EOL)，且有漏洞(CVE-2025-5777、CVE-2025-5349) ● 使用 NetScaler 執行個體的安全私有存取本機部署或安全私有存取混合部署受此漏洞影響。

警訊	類別	內容說明
		● 將其設備升級到已修復漏洞的受支援版本之一，請參考官方說明儘速確認並進行修補。

警訊說明：

「漏洞警訊」：為已驗證漏洞但尚未遭攻擊者大量利用，修補速度建議儘快安排更新。

「已知遭駭客利用之漏洞」：已知有漏洞成功攻擊情形，建議即刻評估修補

三、近期資安事件分享

小心 USB 可能潛藏惡意程式

本月某機關通報內部多台電腦對外異常連線，經查確認受駭電腦感染來源皆來自同一個 USB，**研判該裝置於同仁出差期間曾接入外部未受信任設備，可能因此遭植入惡意程式，後續該** USB **又接入內部其他電腦進而內部擴散。**

經驗學習(Lessons Learned)

此事件顯示，若在可攜式裝置的使用與管理上，缺乏完善的政策規範、存取控管及檢測機制，容易成為攻擊者入侵的管道，建議各機關：

1. 建立可攜式裝置使用政策

建立並公告可攜式儲存裝置(如 USB、**外接硬碟)使用政策，禁止未受信任外部來源裝置接入機關設備，亦不得將內部裝置接入外部未受信任設備。使用外部裝置前應先進行防毒掃描與安全檢測，以降低惡意程式傳播風險。**

2.防毒自動掃描與隔離使用機制

所有外部接入之裝置，應由防毒系統自動掃描，或在隔離環境下使用。

3. 停用 AutoRun 自動執行功能

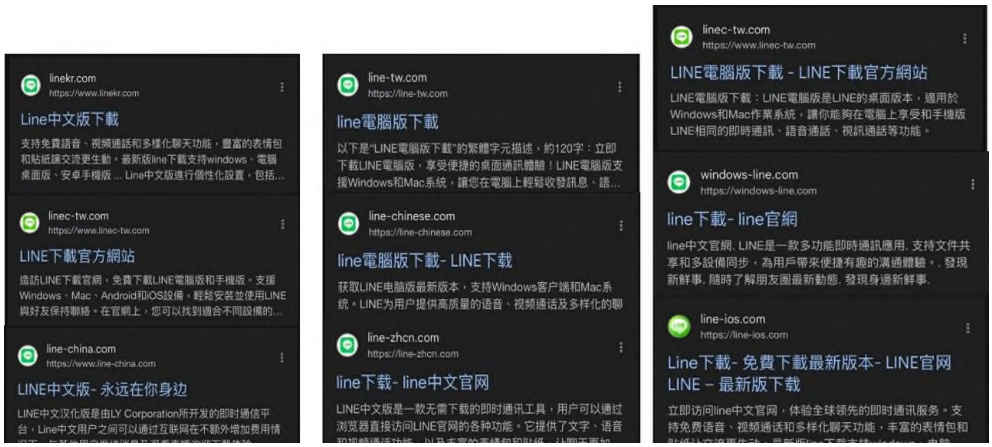
透過群組原則(GPO)將 AutoRun 設定為完全停用，防止 USB 裝置中的 autorun.inf 自動啟動惡意程式，避免在未經使用者同意下於背景執行並感染系統。

四、資安新知

假冒網站高度仿真難分辨，小心下載軟體恐中駭

自本(114)年 2 月起，陸續有多個機關被偵測安裝偽冒軟體並連線惡意中繼站情形，本月此類事件更為頻繁，常見於新進人員報到或設備汰換時，使用者取得新電腦後，透過搜尋引擎查找 LINE 通訊軟體，誤至非官方網站下載偽冒安裝程式，導致電腦遭植入後門程式。

駭客設置之偽冒網站網址與 LINE 官方極為相似，頁面設計亦高度仿真，甚至可能具備良好的搜尋結果排名，代表網站內容與關鍵字高度相關，容易被使用者找到



圖片來源：https://www.twcert.org.tw/tw/cp-104-10279-35bca-1.html

且難以辨識真偽，儘管部分惡意載點已遭封鎖或下架，惟新的載點仍不斷出現，須持續監控與防範：

安裝不焦急多查看留意異常提示與警示

駭客以多層次手法將後門程式與正常安裝檔進行封裝，規避防毒軟體與端點偵測工具等防護機制，因此建議使用者別急著安裝，滑鼠右鍵檢視下載檔案內容的檔案簽章資訊、檔案描述及檔案大小是否異常，過濾掉明顯異常的檔案。

檢視項目	官方安裝檔	非官方(可疑)安裝檔
發行者簽章	LY Corporation 有效簽章)	無簽章、或顯示其他廠商／未知
檔案描述與名稱	LineInstaller、LINE	CMake Setup、ZIP 檔等
檔案大小	約 1 MB	明顯偏大

安裝過程中若出現以下情況，應停止安裝並刪除檔案：

安裝畫面簡略、不像正式產品	防毒軟體跳出警告或封鎖
無授權條款或來源說明	安裝後出現不明程式、閃退或系統異常

五、國際資安新聞

➢ 火車煞車系統恐遭駭客以無線電駭入 (資料來源: Security Week)

美國網路安全暨基礎設施安全局 (CISA) **揭露了** CVE-2025-1727，這是一個影響列車尾端 (End-of-Train, EoT) **和列車前端** (Head-of-Train, HoT) **系統用於傳輸狀態資料的遠端連結通訊協定漏洞。**

由於 EoT **和** HoT **之間透過無線電訊號進行遠端連結的通訊協定並未使用身分驗證或加密，使其存在不安全性。這讓攻擊者得以透過軟體定義無線電** (software-defined radio) **傳送特製的封包，向** EoT **裝置發送指令。利用此漏洞可能讓攻擊者向** EoT **裝置傳送煞車控制指令，進而導致列車緊急停止、煞車失靈、脫軌或營運中斷。**

網路溫控器、智慧電視與監控攝影機成駭客目標

(資料來源: Cybernews)

美國網路安全暨基礎設施安全局（CISA）近日發布警告，指出網路溫控器存在嚴重漏洞（CVSS：9.8），以及監控攝影機韌體存在遠端程式碼執行（RCE）漏洞。網路溫控器的漏洞允許未經身分驗證的攻擊者，無論是透過區域網路，或是經由設定埠口轉發（port forwarding）的路由器遠端存取，直接進入其嵌入式網頁伺服器並重設使用者憑證。

許多物聯網裝置，如智慧電視，經常因開放埠口或預設設定而缺乏安全性，成為駭客入侵的簡易入口。CISA 與資安專家建議，應最小化網路暴露、保持韌體更新、使用防火牆，並透過最新的 VPN 服務保護遠端存取。

六、近期重要資安會議及活動

日期	活動/會議	對象
7 月至 8 月	■ 114 年度 AI 資安學院 （7 月 01 日、7 月 15 日、7 月 22 日、7 月 31 日、8 月 07 日、8 月 14 日）	《資通安全管理法》納管之資通安全責任等級 A 級、B 級公務機關資安人員。

七、資通安全長異動情形

- 連江縣政府資通安全長於 114 年 7 月 15 日起，原由張龍德秘書長兼任，改由陳明傑行政處處長暫代理秘書長並兼任。
- 考選部資通安全長於 114 年 8 月 4 日起，原由鄭中平次長兼任，改由林明裕次長兼任。