資通安全網路月報

一、政策重點

配合資通安全管理法修正，《資通安全法施行細則》、《資通安全維護計畫實施情形稽核辦法》、《資通安全通報應變及演練辦法》及《資通安全情資分享辦法》等 4 項子法，已於 115 年 1 月 7 日修正施行。《資通安全責任等級分級辦法》已於 115 年 1 月 9 日修正施行。《公務機關所屬人員辦理資通安全事項作業辦法》於 115 年 1 月 15 日修正施行。

二、近期資安事件分享

外部網站潛藏惡意指令，明碼資訊恐遭竊取

機關人員於執行公務期間瀏覽外部企業網站，惟該網站已遭駭客植入惡意指令，使人員於瀏覽該網站時，被自動導向至其他惡意網站，進而觸發惡意程式背景下載，並誘導安裝執行。該惡意程式啟動後，將電腦資料打包上傳至中繼站，造成資訊外洩。

經驗學習(Lessons Learned)

本案駭客利用竄改網站腳本方式，誘導使用者連線下載並安裝惡意程式。顯示端點防護機制應強化對異常指令特徵、程式載入及行為控管之偵測及阻擋機制。建議各機關評估採取下列強化防禦措施：

1. **應用程式下載及安裝管控：**使用者下載及安裝應用程式應建立管控機制，並由機關內部管理政策統一規範，並加強使用者資安意識，避免下載不明或可疑程式。
2. **建立端點偵測及應變機制(EDR)：**持續監控端點設備之可疑行為，即時偵測駭客活動跡象，降低後續可能引發之資安風險。

三、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 7 萬 2,743 件(增加 1 萬 1,163 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(41%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(24%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(17%)，大多是系統遭未經授權存取或取得系統/使用者權限。統計近 1 年情資數量分布，詳見圖 1。

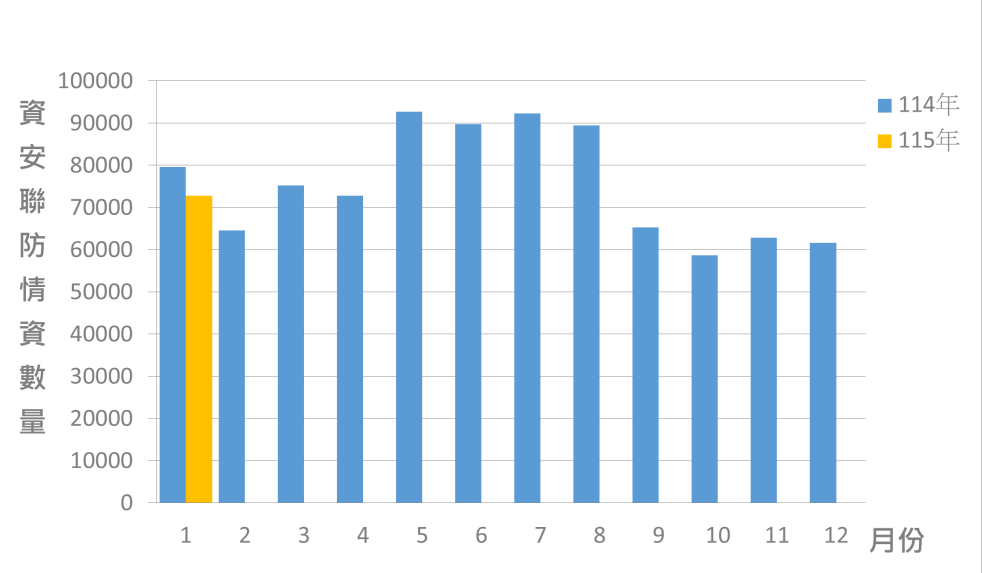

圖 1 資安聯防監控資安監控情資統計

假冒行政訴訟通知之社交工程郵件攻擊

經進一步彙整分析聯防情資資訊，發現近期駭客以「行政訴訟」為誘因，針對政府機關發動社交工程電子郵件攻擊。駭客於寄件人顯示名稱中標示為「行政訴訟起訴狀」，以營造具法律效力與急迫性假象，藉此提高收件者開啟郵件之意願；同時，駭客於郵件主旨中刻意使用收件者所屬機關名稱，並將郵件內容偽裝為「法院通知書」，包含案件編號、案件名稱等看似正式之資訊，以提升郵件可信度，進而引導收件者點擊郵件內所附連結，查閱所謂「相關資料」，進而下載並植入惡意後門程式(ValleyRAT)以達竊取電腦機敏資料目的，相關情資已提供各機關聯防監控防護建議。

事中通報應變

本月資安事件通報數量共 84 件，是去年同期的 1.79 倍，通報類型以非法入侵為主，占本月通報件數 66.67%。本月份仍以接獲機關因安裝冒牌軟體以致植入惡意程式之通報最多，占總通報件數 16.67%。近 1 年資安事件通報統計詳見圖 2。

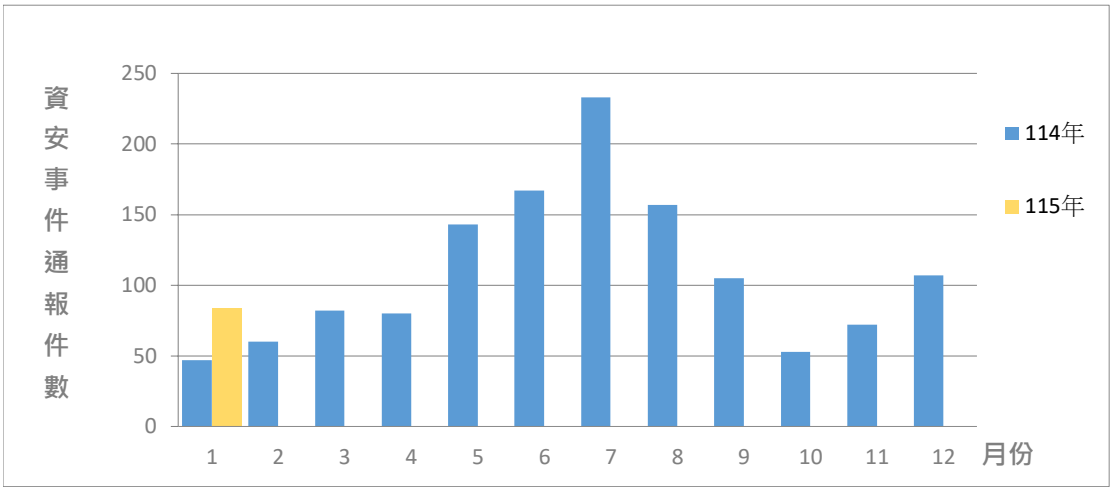

圖 2 資安事件通報統計

(二) 重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	監控攝影機 利凌監控主機與監控攝影機 嚴重程度：CVSS 8.8 (CVE-2026-0854、CVE-2026-0855)	● 研究人員發現利凌部分監控主機與監控攝影機型號分別存在作業系統指令注入(OS Command Injection)漏洞(CVE-2026-0854與CVE-2026-0855)。 ● 已通過身分鑑別之遠端攻擊者可

警訊	類別	內容說明
		注入任意作業系統指令並於設備上執行，請儘速確認並進行修補。 ● 官方已提供安全公告，請參考官方說明儘速確認並採取相關緩解措施。
	應用程式 QNAP NAS 嚴重程度：CVSS 8.1 (CVE-2025-59384、CVE-2025-59387)	● 研究人員發現 QNAP NAS 應用程式存在高風險安全漏洞，請儘速確認並進行修補。 ● Qfiling 存在路徑遍歷(Path Traversal)漏洞(CVE-2025-59384)，未經身分鑑別之遠端攻擊者可利用此漏洞讀取未授權之檔案或系統資料。 ● MARS(Multi-Application Recovery Service)存在 SQL 注入(SQL Injection)漏洞(CVE-2025-59387)，未經身分鑑別之遠端攻擊者可注入並執行未授權

警訊	類別	內容說明
		指令。 ● 官方已提供安全公告，請參考官方說明進行更新：(CVE-2025-59384)、 (CVE-2025-59387)
	集中式管理平台 Trend Micro Apex Central 嚴重程度：CVSS 9.8 (CVE-2025-69258)	● 研究人員發現 Trend Micro Apex Central 存在遠端執行程式碼(Remote Code Execution)漏洞(CVE-2025-69258)。 ● 未經身分鑑別之遠端攻擊者可促使系統載入惡意 DLL 檔案並執行任意程式碼，請儘速確認並進行修補。 ● 官方已提供安全公告，請參考官方說明儘速確認並採取相關緩解措施。
已知遭駭客利用之漏洞	郵件管理系統 Cisco AsyncOS 軟體 嚴重程度：CVSS 10.0	● 研究人員發現 Cisco Secure Email Gateway (SEG)與 Secure Email and Web Manager

警訊	類別	內容說明
	(CVE-2025-20393)	(SEWM)所使用之 AsyncOS 作業系統存在不當輸入驗證(Improper Input Validation)漏洞(CVE-2025-20393)。 ● 在垃圾郵件隔離功能(Spam Quarantine)啟用且可由網際網路存取時，未經身分鑑別之遠端攻擊者可利用此漏洞以 root 權限於受影響設備底層作業系統執行任意指令，該漏洞已遭駭客利用，請儘速確認並進行修補。 ● 官方已提供安全公告，請參考官方說明儘速確認並採取相關緩解措施。
	整合通訊 Cisco 整合通訊 嚴重程度：CVSS 9.8 (CVE-2026-20045)	● 研究人員發現 Cisco 整合通訊多項產品存在程式碼注入(Code Injection)漏洞(CVE-2026-20045)

警訊	類別	內容說明
		● 未經身分鑑別之遠端攻擊者可透過傳送特製 HTTP 請求至受影響設備以執行任意指令，進而提升至 root 權限。 ● 該漏洞已遭駭客利用，請儘速確認並進行修補。 ● 官方已提供安全公告，請參考官方說明儘速確認並採取相關緩解措施。

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

四、國際資安新聞

數十款 Chrome 擴充功能遭駭客攻擊，數百萬用戶面臨資料外洩風險

(資料來源：The Hacker News)

一項新的攻擊行動鎖定了多個知名的 Chrome 瀏覽器擴充功能，至少有 35 個擴充功能遭到入侵，導致超過 260 萬名使用者 面臨資料外洩及帳密遭竊

的風險。該攻擊透過網路釣魚手法鎖定 Chrome Web Store 上的擴充功能開發者，利用其存取權限，將惡意程式碼植入原本合法的擴充功能中，以竊取使用者的 Cookie 及存取權杖。114 年 12 月 27 日，網路安全公司 Cyberhaven 披露，攻擊者入侵了其瀏覽器擴展程序，並註入惡意代碼，與外部指揮與控制伺服器進行通訊，下載額外的設定檔，並將使用者資料外傳。這封釣魚郵件偽裝成來自 Chrome 線上應用程式商店開發者支援團隊，聲稱擴充功能因違反開發者政策而面臨即將下架的風險，刻意營造高度急迫感。受害者會被重新導向至一個授權頁面，誘導他們授予惡意 OAuth 應用程式相關權限。

廣泛使用的惡意擴充功能竊取 ChatGPT 和 DeepSeek 對話

(資料來源：Security Boulevard)

OX Security 的研究人員發現了兩款惡意擴充功能偽裝成合法工具，被不法分子用來竊取用戶的瀏覽資料以及他們與 ChatGPT 和 DeepSeek 等 AI 模型的對話。這兩款擴充功能分別是：Chat GPT for Chrome with GPT-5、Claude Sonnet & DeepSeek AI(使用者超過 60 萬)和 AI Sidebar with DeepSeek, ChatGPT,Claude and more（使用者超過 30 萬）。這些擴充功能每 30 分鐘就會將專有原始碼、商業策略、個人識別資訊(PII)、機密公司通訊、完整的 Chrome 標籤頁 URL、搜尋查詢等資訊洩露到遠端命

令與控制(C2)伺服器。攻擊者偽裝成 AITOPIA 的合法側邊欄擴展程序，利用其廣泛的權限即時監控和提取敏感資料。如果使用者卸載了某個擴充程序，惡意軟體會提示使用者安裝另一個擴充程序，從而持續存在。OX Security 於 114 年 12 月 29 日通知 Google 有關惡意擴充功能的問題，Google 於同年 12 月 30 日回應正在審查該問題。

jsPDF 嚴重漏洞：駭客可透過產生的 PDF 檔案竊取機密資訊
(資料來源：Bleeping Computer)

此漏洞的編號為 CVE-2025-68428 (CVSS: 9.2)，用於在 JavaScript 應用程式中產生 PDF 文件的 jsPDF，被發現存在一個嚴重漏洞，透過將本機檔案內容納入產生的文件中，進而竊取本機檔案系統中的敏感資料。該漏洞利用本機檔案包含和路徑遍歷漏洞，允許在 jsPDF4.0 之前的版本中，將未經過濾的路徑傳遞給 loadFile 方法。當使用者可控的輸入被當作檔案路徑傳遞時，就會出現此問題，導致 jsPDF 將檔案內容合併到產生的 PDF 輸出中。其他檔案載入方法亦受到影響，包括 'addImage'、'html' 和 'addFont'。CVE-2025-68428 已於 jsPDF 4.0 版中修復，透過預設限制檔案系統存取權限，並改為依賴 Node.js 權限模式來強化安全性。不過，Endor Labs 的研究人員指出，該權限模式在 Node 20 中仍屬實驗性功能，因此建議使用 22.13.0、23.5.0 或 24.0.0 以上版本。

五、近期重要資安會議及活動

日期	活動/會議	對象
115 年 2 月 9 至 2 月 12 日	資安考科集中實務訓練	資安考科錄取人員