資通安全網路月報

一、近期資安事件分享

以常見鍵盤排序設置密碼易遭破解

機關接獲 SOC 通知，發現僅供內部使用之系統出現對外異常連線。經查機關近期因進行防火牆汰換，未逐一檢視防火牆政策套用生效因而導致外部可存取到內部系統進而入侵攻擊，且該系統以常見鍵盤排序設置密碼，導致遭暴力破解成功登入並植入惡意程式。機關透過虛擬機重新建置受影響系統、全面變更密碼，並要求管理者遵守密碼複雜性原則，嚴禁使用鍵盤排列組合作為密碼。

經驗學習(Lessons Learned)

機關雖已依規定導入政府組態基準(GCB)，但使用者帳號密碼仍採「鍵盤排序」方式(如 1qaz2wsx、!QAZ@WSX 等)，雖形式上符合 GCB 密碼長度與複雜度規範，仍因規律性過高，遭暴力破解工具成功猜測登入，顯示安全意識仍有不足。此外，網路設備與設定管理的變更，應落實驗證、檢測與持續控管，以降低資安風險。爰此建議各機關：

1. 高防護等級系統建議導入多因子驗證機制

持續強化帳號與驗證安全，包括密碼設置除長度與複雜度要求外，建議導入「密碼黑名單」機制，排除常見鍵盤序列或可預

測字串。若防護需求等級為「高」之資通系統，建議導入多因子驗證(Multi-Factor Authentication, MFA)，以強化身分識別安全性。

2. 落實設備變更驗證與定期稽核

建置網路設備與設定異動管理機制，例如變更前後驗證程序，確保相關設定完整套用，後續定期稽核以檢查防火牆規則與存取紀錄，以利發現異常開放或遺漏。

3. 強化異常登入行為偵測

強化偵測監控，例如登入失敗次數監控、異常登入時段、短時間內大量登入嘗試，以及早發現異常登入嘗試、重複攻擊或暴力破解行為。

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 5 萬 8,621 件(減少 6,609 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(38%)，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(26%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(18%)，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。

駭客把病毒藏在合法網站，躲避檢查

經進一步彙整分析聯防情資資訊，發現近期駭客於社交工程釣魚郵件中濫用「網際網路檔案館（Internet Archive）」作為惡意

程式的下載站，該網站為合法的數位圖書館服務，提供多媒體資料與網頁內容的保存與閱覽。惟駭客藉由利用其合法網域散布惡意程式，以規避資安偵測機制，相關情資已提供各機關聯防監控防護建議。

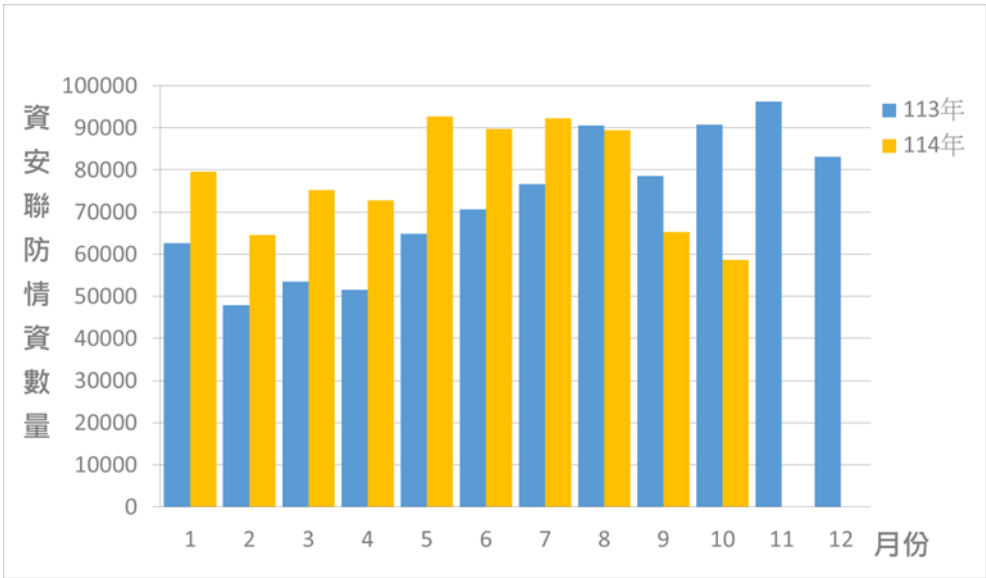

圖 1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共 53 件，較去年同期減少 32.91%，通報類型以非法入侵為主，占本月通報件數 58.49%，仍有機關因可攜式媒體感染 PUBLOAD 惡意程式；此外，亦觀察到有機關監視器遭入侵利用下載惡意腳本。近 1 年資安事件通報統計詳見圖 2。

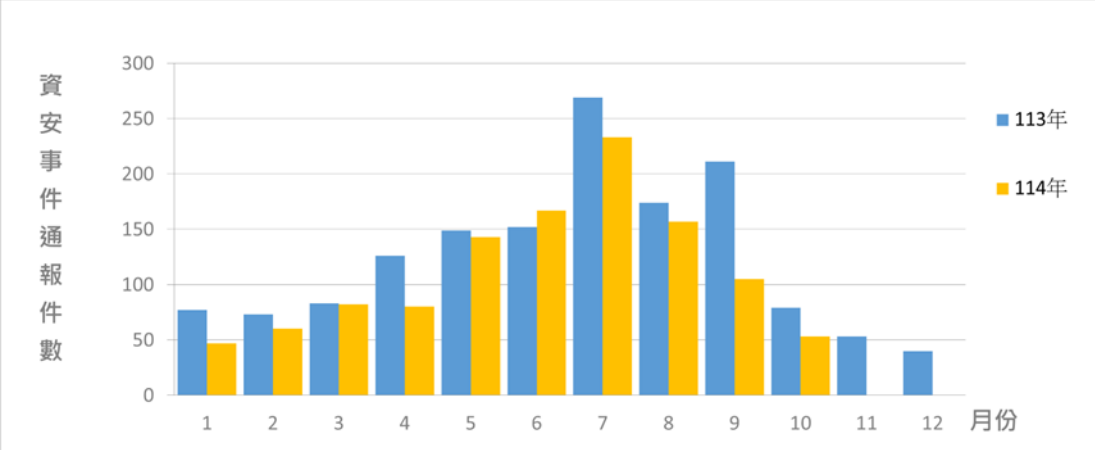

圖 2 資安事件通報統計

(二) 重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	系統服務 傑印資訊筆硯公文管理系統存在安全漏洞 嚴重程度：CVSS：9.8 (CVE-2025-11948)	● 研究人員發現傑印資訊筆硯公文管理系統存在任意檔案上傳(Arbitrary File Upload)漏洞(CVE-2025-11948)。 ● 未經身分鑑別之遠端攻擊者可上傳並執行網頁後門程式，進而於伺服器端執行任意程式碼，請儘速確認並聯繫廠商進行更新。
已知遭駭客利用之漏洞	Microsoft Windows Server Windows Server Update Services (WSUS) 存在高風險安全漏洞 嚴重程度：CVSS：9.8 (CVE-2025-59287)	● 研究人員發現 Windows Server Update Services 存在不安全之反序列化(Deserialization of Untrusted Data)漏洞(CVE-2025-59287)。 ● 未經身分鑑別之遠端攻擊者，可透過向 WSUS 伺服器發送特製事件以系統權限執行任意程式碼。 ● 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。
	Microsoft Windows Server	● 研究人員發現 Windows SMB 用戶端存在 NTLM 反射(NTLM Reflection)

警訊	類別	內容說明
	Windows SMB 存在高風險安全漏洞 嚴重程度：CVSS：8.8 (CVE-2025-33073)	漏洞(CVE-2025-33073)。 ● 取得一般使用者權限之遠端攻擊者，可透過執行惡意腳本，迫使 SMB 用戶端與攻擊者控制之 SMB 伺服器連線並進行身分鑑別，由於 SMB 用戶端在驗證階段存在缺陷，攻擊者可藉此繞過安全檢核以提升至系統權限，進而控制用戶端系統。 ● 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。
	VMware 工具 存在高風險漏洞 嚴重程度：CVSS 7.8 (CVE-2025-41244)	● 研究人員發現 Broadcom VMware Aria Operations 和 VMware Tools 存在「使用不安全操作定義權限」的漏洞(CVE-2025-41244)。 ● 這項漏洞惡意本地攻擊者若擁有非管理員權限，且能夠存取已安裝 VMwar Tools 並由 Aria Operations 管理且啟用了 SDMP 的虛擬機，則可利用此漏洞將權限提升至該虛擬機的 root 使用者。 ● 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。

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、國際資安新聞

➢ Google 修補 Gemini AI 套件中的「Gemini Trifecta」漏洞 (資料來源：Hack Read)

資安公司 Tenable 在 Google 的 Gemini AI 助理套件中，發現了三個關鍵性的安全缺陷，並將其命名為「Gemini 三連擊」（Gemini Trifecta）。這些漏洞約於 10 月初公開揭露，前述漏洞使 Gemini 面臨提示注入（prompt injection）和資料外洩（data exfiltration）的風險，威脅到 Gemini 使用者的資料安全。

三項關鍵漏洞詳情

漏洞一：提示注入與 Chrome 瀏覽記錄

- 影響組件：Gemini 搜尋個人化模型(Search Personalization Model)。
- 攻擊方式：攻擊者可藉由操縱使用者的 Chrome 瀏覽記錄。
- 潛在後果：實現提示注入(Prompt Injection)，使攻擊者能控制 AI 的輸出和行為。

漏洞二：惡意日誌與雲端資源攻擊

- 影響組件：Gemini 雲端助理(Gemini Cloud Assist)。
- 攻擊方式：攻擊者將惡意提示嵌入日誌項目(Log Entry)中，例如利用網頁請求的 HTTP User-Agent 欄位。
- 潛在後果：啟動網路釣魚(Phishing)，並導致對雲端資源執行未經授權的操作。

漏洞三：繞過防禦與私人資料外洩

- 影響組件：Gemini 瀏覽工具(Gemini Browsing Tool)。
- 攻擊方式：繞過 Google 的防禦機制。
- 潛在後果：實現資料外洩(Data Exfiltration)，將使用者的私人資料（例如地理位置）發送到外部的伺服器。

Google 已經回溯（rolled back）了有漏洞的模型，停止了惡意超連結的渲染（rendering），並在整個套件中部署了多層次的提示注入防禦策略。

人為風險報告揭示:企業對網路釣魚防禦「過度自信」

(資料來源：Tech Republic)

根據 Arctic Wolf 發布的年度《人為風險行為快照》(Human Risk Behavior Snapshot)報告顯示，儘管企業對自身的網路安全防禦持續抱持高度信心，但員工的日常行為，如網路釣魚失誤和有風險的 AI 使用習慣，仍是造成資料外洩的主要原因。報告顯示，在 2025 年有 68%的 IT 領導者表示其組織曾遭受資料外洩，較 2024 年增加了 8%。

- 過度自信與實際風險的落差：儘管有近三分之二的 IT 領導者和半數員工承認曾點擊惡意連結，但仍有大約 75%的領導者相信自己的組織是安全的。領導者對防禦措施的過度自信，以及員工規避安全規範的傾向，加劇了想像與實際漏洞之間的差距。
- **生成式 AI 帶來的資訊風險：**隨著生成式 AI 的使用增加，資訊風險也隨之加劇。有 80%的 IT 領導者和 63%的員工在工作中使用 AI 工具，其中 60%的領導者和 41%的員工承認曾將機密資料輸入到這些平台中。
- **應對人為錯誤的態度分歧：**報告同時強調了企業在應對人為錯誤時，做法上的分歧日益擴大。專注於矯正性訓練的公司，成功將風險降低了 88%；然而，有 77%的 IT 領導者表示會解僱上當受騙的員工，這一比例高於去年的 66%。

簡單的提示注入攻擊即可繞過 OpenAI 的安全防護欄

(資料來源：Hack Read)

在 OpenAI 於 10 月 6 日釋出其 AgentKit 工具組，並同步推出 Guardrails 安全框架後，資安公司 HiddenLayer 隨即揭露了其中的一項重大缺陷。

OpenAI 將 Guardrails 描述為一個開源、模組化的安全層，它利用

特殊的 AI 程式，亦即基於大型語言模型（LLM-based）的「評審」（Judges），來阻擋像是「越獄」（Jailbreaks）和「提示注入」（Prompt Injections）等惡意行為。然而，HiddenLayer 找到了一種繞過這些「Guardrails」的方法。

他們指出，如果用於生成回覆的模型與作為安全檢查器的模型是同類型的，那麼這兩種模型就能以相同的方式被欺騙。研究人員成功地癱瘓了主要的安全性偵測器，並說服系統產生有害的回應並執行隱藏的提示注入。

在其中一項測試中，HiddenLayer 透過操縱 AI 評審的置信分數（confidence score），成功繞過了一個原先有 95%信心認為其提示屬於越獄行為的偵測器。他們甚至能夠欺騙系統，使其允許透過工具呼叫（tool calls）進行間接提示注入，這可能導致使用者的機密資料外洩。

四、近期重要資安會議及活動

日期	活動/會議	對象
11 月 13 日全天	政府資通安全防護巡迴研討會(高雄場)	政府機關、關鍵基礎設施資安長
11 月 17 日下午	政府資通安全防護巡迴研討會(臺北場)	
11 月 18 日全天	政府資通安全防護巡迴研討會(臺北場)	
11 月 20 日下午	政府資通安全防護巡迴研討會(臺東場)	
12 月 2 日全天	政府資通安全防護巡迴研討會(臺中場)	