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

資安週報

Cyber Security Weekly Newsletter

事件通報
登入頁面不宜揭露過多帳號規則 以降低帳號遭推測利用之風險

聯防監控
防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕
企業級網路防火牆軟體仍為攻擊熱點

重大漏洞
Cisco與Splunk高風險漏洞應盡速修補

外部曝險分析
外部曝險程度小幅上升 需持續強化加密通訊、憑證管理及網站防護

實兵演練
實兵演練揭露SQL Injection漏洞與明文密碼儲存風險

網路巡查高風險詐騙
倒數優惠與限量下單成高風險廣告主要誘因

焦點文章
社交工程郵件攻擊案例分析

2026.07.09
052

資安儀表板

事件通報、聯防監控、蜜罐誘捕、重大漏洞、外部曝險分析及實兵演練等六類量化指標

■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

登入頁面不宜揭露過多帳號規則 以降低帳號遭推測利用之風險

本週總計接獲16件公務機關與特定非公務機關事件通報，詳見圖1，公務機關非法入侵事件中以系統遭入侵占多數，詳見圖2。本週發現有機關網站登入頁面之使用說明中，直接揭露帳號命名規則與範例，並搭配統一預設密碼，致外部可依公開資訊推算帳號後成功登入。

建議各機關網站登入說明內容，避免揭露可推算帳號之命名規則、範例或業務識別資訊，並應停止使用固定或可預測之預設密碼；另宜於系統功能設計中納入首次登入強制變更密碼、密碼強度要求、登入失敗鎖定及異常登入監控等機制，以降低因帳號規則與預設密碼過於簡單而遭猜測登入之風險。

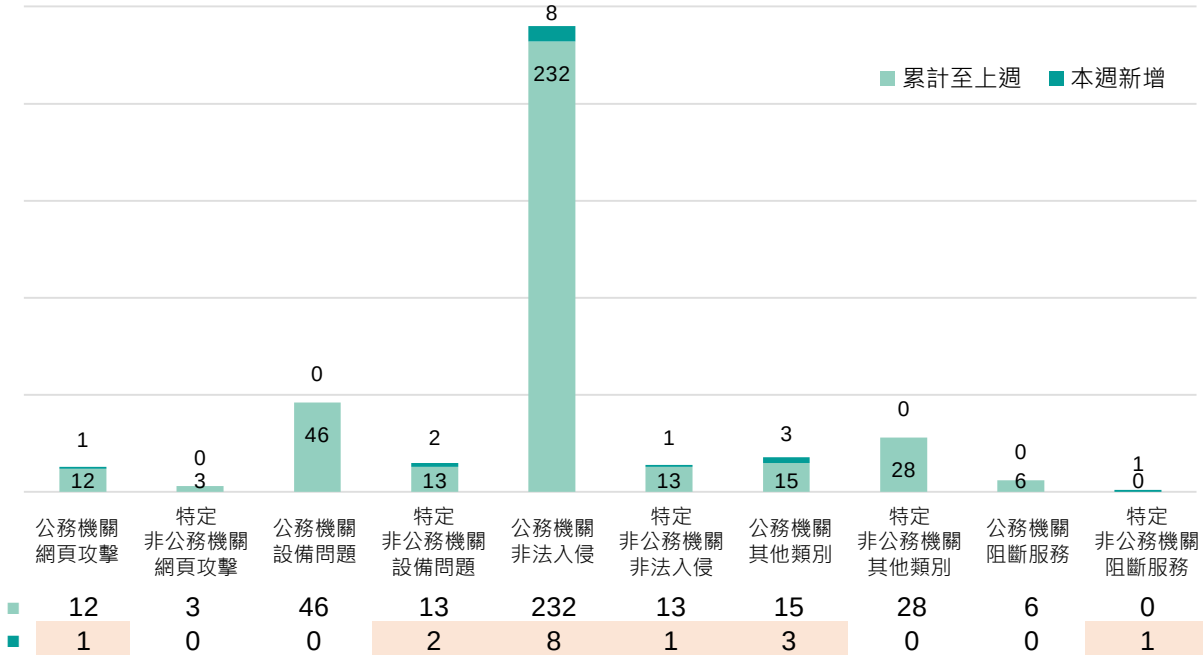

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

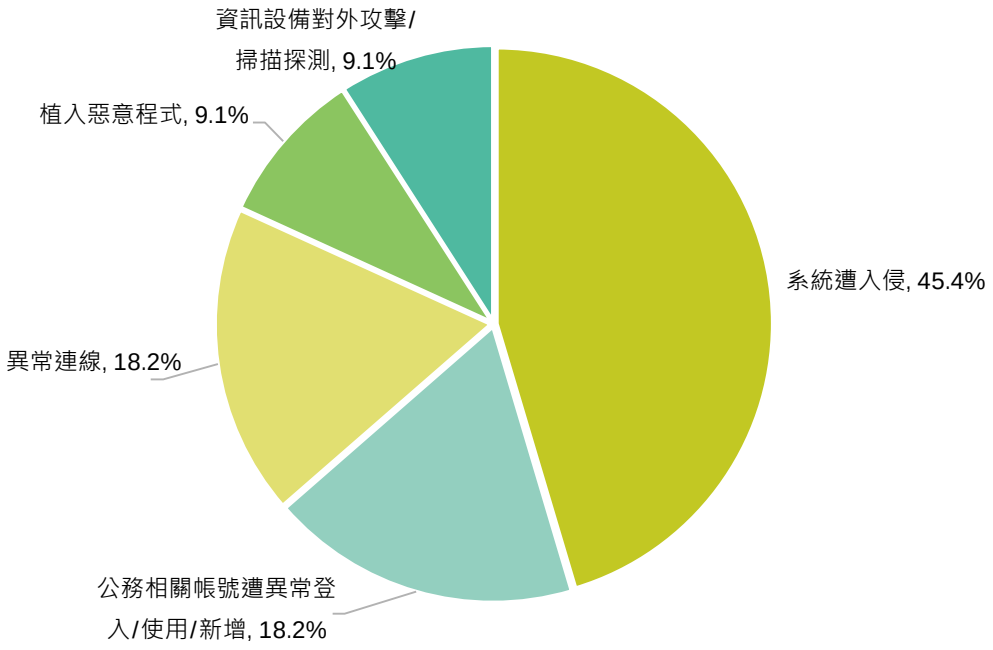

圖2 | 本週公務機關非法入侵事件類型占比

防護建議 **除修補漏洞外，應：**

以攻擊為出發評估潛在風險	針對潛在風險執行相應改善
➢ 網站說明直接揭露帳號命名規則與統一預設密碼，使攻擊者能利用公開資訊輕鬆推算並批量登入 ➢ 歷史外洩憑證於網路流傳，若管理或 VPN 帳號沿用舊密碼且缺乏 MFA，邊界防線極易遭破入	➢ 立即中止涉嫌外洩之連線，停止使用固定或可預測之預設密碼，並強制執行首次登入變更密碼 ➢ 針對管理介面與 VPN 全面強制導入多因子驗證（MFA），從根本阻絕憑證遭竊取後的冒用風險 ➢ 清除網頁說明中的帳號規則與業務識別範例，管理介面同步導入來源 IP 白名單限制存取 ➢ 納入登入失敗鎖定與異常行為監控，定期深入審查設備設定與操作日誌，嚴防未授權帳號異動

3間民間企業揭露重大資安訊息

本週3家民間企業發布重大訊息，產業類別為數位雲端、汽車工業，詳見表1。

表1 | 本週民間企業重大資安訊息彙整

公司名稱	發布時間	事件說明
走著瞧股份有限公司	115年7月1日	GOGOLOOK公司資安團隊在監控發現伺服器的測試環境有不明人士惡意嘗試未經授權存取，已全面啟動資安防禦與阻攔機制，同時與外部服務商積極展開調查，目前未有會員個資及公司內部機密資料遭存取情形。 後續將持續依案件辦理情形及參酌主管機關建議，評估委請第三方資安專業廠商協助進一步調查及檢視。
網路家庭國際資訊股份有限公司	115年7月1日	網家公司針對媒體報導引述駭客組織Settra於暗網聲稱入侵本公司關聯企業拍付國際相關系統，並提及其相關支付服務內容。拍付國際其交易系統、會員資料庫及營運管理均與網家公司各自獨立，經初步調查，目前並未發現網家公司及Pchome 24h購物交易資料庫受本事件影響。 拍付國際已立即啟動資安應變程序，會同資安專家進行全面系統檢測與鑑識調查並已通報主管機關，後續將持續關注及督促拍付國際資安管理及改善措施。
麗清科技股份有限公司	115年7月2日	麗清公司偵測部份資訊系統遭駭客網路攻擊，已立即啟動資安防禦機制，並委請外部資安專家協處。 初步評估對公司運作無重大影響，後續將修復安全漏洞並持續提升網路與資訊基礎架構之安全管控以確保資訊安全。

■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

防禦迴避高居首位 偵測刺探仍具威脅

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3。「防禦迴避」為最常見攻擊手法，占比14.8%，攻擊者通常會透過關閉或刪除指令紀錄，並利用合法的系統工具間接執行惡意命令，以達到規避監控的目的。因應此類威脅，建議導入端點防護措施，加強指令紀錄的稽核能力，限制高風險工具的濫用，並強化特權帳號的管理，以避免攻擊者繞過偵測並消除其行為痕跡。

「偵測刺探」事件本週占比為13.5%，為本週占比次高的攻擊階段，顯示攻擊者持續加強對目標環境的偵查與資訊蒐集活動，以提升後續攻擊行動的成功率。觀察到的主要手法包括主動式掃描、憑證資訊蒐集、以及IP 區段掃描。攻擊者透過自動化工具對外部網段與公開服務進行大規模探測，蒐集系統架構、開放埠與服務資訊，同時搜尋與帳號憑證相關的公開資料或外洩資訊，作為後續登入嘗試與目標鎖定的依據。部分活動呈現由廣泛掃描逐步聚焦特定系統與帳號的特徵，顯示其偵查行為具備明確的攻擊目標與規劃。此類行為雖多屬攻擊前期準備階段，但其蒐集成果往往成為後續入侵與橫向移動的重要基礎。建議組織加強監控異常掃描流量與帳號探測行為，定期盤點對外暴露資產，並結合威脅情資分析可疑來源，以提前發現潛在攻擊準備活動並採取防禦措施。

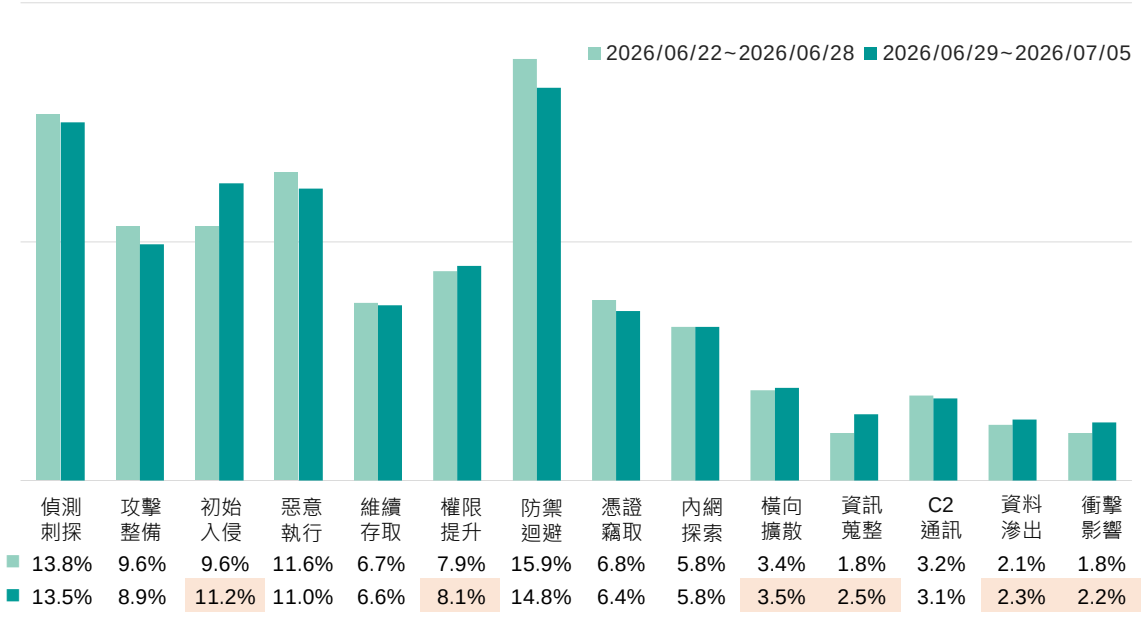

圖3 | 資安聯防監控攻擊階段統計

防護建議 **建議機關採取下列防護措施：**

防禦迴避(Defense Evasion)

- 導入 EDR / 端點防護機制，監控可疑程序與命令執行
- 保留並定期稽核指令紀錄（如 PowerShell、Shell、Windows Event Log）
- 限制合法管理工具（Living-off-the-Land Binaries, LOLBins）的使用權限
- 落實最小權限原則與特權帳號管理（PAM），降低高權限帳號遭濫用風險
- 建立異常行為告警機制，偵測日誌清除、服務停用等規避行為

偵測刺探(Reconnaissance)

- 監控異常掃描流量、連線探測及大量存取行為
- 定期盤點並降低對外暴露資產，關閉非必要服務與連接埠
- 建立暴力破解與帳號探測偵測機制，強化登入監控
- 結合威脅情資封鎖已知惡意 IP、網域及掃描來源
- 定期檢視公開資訊與外洩憑證，並落實密碼更新及多因素驗證（MFA）

■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

企業級網路防火牆軟體仍為攻擊熱點

本週透過部署於國內外之蜜罐系統觀測攻擊行為動態，相較於上週「網頁應用」服務攻擊占比80.37%、「遠端控制」服務攻擊占比16.64%，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81.26%。「遠端控制」服務亦有16.12% 的誘捕比例，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，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，為優先防護之項目。本週網頁應用介面之誘捕狀況，詳見圖4。本週通用型Web介面占比最高，此類別為攻擊者廣泛的進行HTTP掃描與探測，顯示攻擊者企圖尋找可能存在之Web漏洞進行攻擊。

另Web服務系統類別包含各類以網頁為基礎的服務與應用，例如常見的網頁框架、應用程式伺服器、檔案傳輸與資料管理平台等，由於此類服務多建置於企業應用環境，且直接面向外部提供功能與資料交換，為僅次於通用型介面的攻擊目標。網通設備管理介面涵蓋路由器、防火牆等網通設備管理介面，以及智慧攝影機、NAS等物聯網設備管理介面，皆容易遭受攻擊者透過弱密碼、預設帳號或已知漏洞進行入侵。而IoT設備管理介面比例下降主因為監視器產品存在命令注入漏洞的CVE-2021-36260，遭攻擊次數下降導致。其他類型服務雖比例極小，但若涉及關鍵業務系統，仍需留意潛在風險。

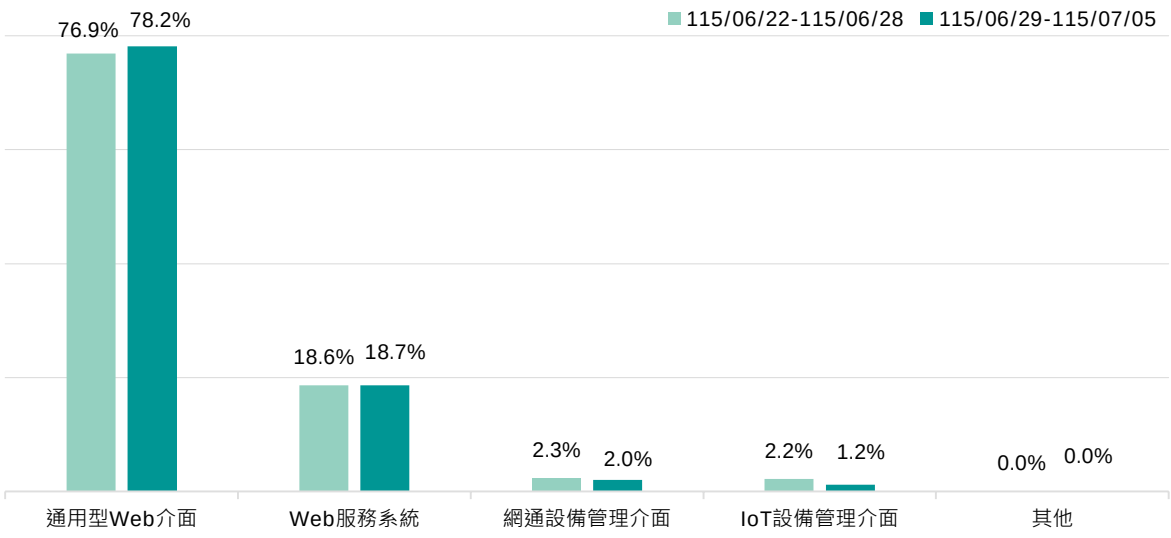

圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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。近2年揭露之攻擊漏洞，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授權缺失漏洞、越界讀取漏洞、資訊外洩漏洞、跨站請求偽造及路徑遍歷漏洞，攻擊目標涵蓋企業級網路防火牆軟體、程式遞送控制器(ADC)、開源後端伺服器框架、多選下拉選單元件及內容管理系統之網站優化外掛程式。

防護建議

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。

表2 | 本週前5大攻擊使用之近2年漏洞排行列表

排名			漏洞編號	受影響產品	CVSS 3.x Base Score
■	1	-	CVE-2025-20362[1]	Cisco Secure ASA & FTD	6.5
■	2	-	CVE-2025-5777[2]	Citrix NetScaler ADC	7.5
■	3	⬆1	CVE-2025-53364[3]	Parse Server	5.3
■	4	⬇1	CVE-2025-47204[4]	Bootstrap Multiselect	6.1
■	5	-	CVE-2025-30567[5]	WordPress WP01	7.5

類型 ■ 授權缺失漏洞 ■ 越界讀取漏洞 ■ 資訊外洩漏洞
■ 跨站請求偽造 ■ 路徑遍歷漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2025-20362
2. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
3. https://nvd.nist.gov/vuln/detail/CVE-2025-53364
4. https://nvd.nist.gov/vuln/detail/CVE-2025-47204
5. https://nvd.nist.gov/vuln/detail/CVE-2025-30567

■重大漏洞

近一週本院研究人員發現以下重大漏洞資訊，建議組織內部進行檢查與修補

Cisco與Splunk高風險漏洞應盡速修補

- Cisco Unified Communications Manager存在伺服器請求偽造(Server-side Request Forgery)漏洞(CVE-2026-20230[1])，未經身分鑑別之遠端攻擊者，可傳送特製HTTP請求，於受影響系統寫入檔案進而取得管理員權限，該漏洞已遭到駭客利用。

- Splunk Enterprise、Splunk Cloud Platform及Splunk Secure Gateway存在不安全之反序列化(Insecure Deserialization)漏洞(CVE-2026-20251[2])，已通過身分鑑別之遠端攻擊者可透過對未受信任之資料進行反序列化，進而於受影響伺服器上執行任意程式碼。

1. https://nvd.nist.gov/vuln/detail/CVE-2026-20230
2. https://nvd.nist.gov/vuln/detail/CVE-2026-20251

■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

外部曝險程度小幅上升 需持續強化加密通訊、憑證管理及網站防護

本次針對93個A、B級關鍵基礎設施(CI)進行EASM資安曝險檢測，前10大風險項目共計2,954項。其中，「元件高風險漏洞」以957項居首，「過時或弱加密協定」852項次之，「TLS憑證不受信任」614項位居第三。前三項合計2,423項，占前10大風險項目總數約82%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密通訊及憑證管理等議題。相較上期2,878項，整體風險數量增加76項，增幅約2.6%，詳見圖5。

進一步分析主要風險項目變化情形，「元件高風險漏洞」仍為最大宗風險，數量由1,019項降至957項，減少62項，降幅約6.1%。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍較為集中；本期PEAR Archive_Tar相關弱點(CVE-2020-36193)已見減少，惟新增Drupal核心相關弱點(CVE-2020-13671)，後續仍須持續關注相關元件版本與修補情形。「TLS憑證不受信任」由553項增至614項，增幅約11%；「過時或弱加密協定」由798項增至852項，增幅約6.8%。另在網站防護設定方面，「CSP設定不當」由248項微增至255項，增幅約2.8%；「未部署WAF」由107項增至114項，增幅約6.5%。整體而言，本期外部曝險程度小幅上升，增加項目主要集中於加密通訊、憑證管理及網站防護設定等風險類別，顯示各受測單位仍需持續強化加密協定設定、憑證生命週期管理及網站安全防護措施。

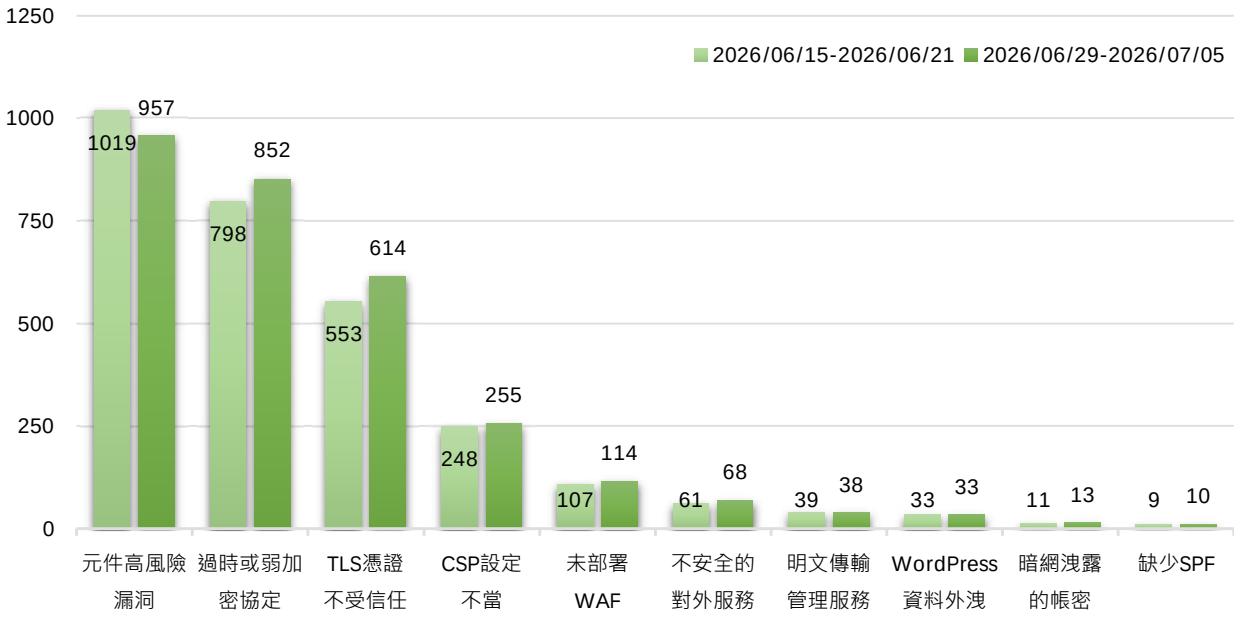

圖5 | EASM檢測結果統計(前10大風險)

防護建議

建議受測單位採取下列防護措施	建議受測單位採取下列管理措施
➢ 定期更新憑證，全面啟用TLS 1.2以上版本協定，並停用未加密或舊版協定 ➢ 儘速修補已知漏洞，並淘汰已無維護之軟體版本 ➢ 部署網站應用程式防火牆(WAF)，並導入內容安全政策(CSP)等網站安全標頭，以降低XSS攻擊與惡意存取風險 ➢ 關閉不必要之對外服務，並定期盤點已停用站台、主機及應用服務是否已確實下線，避免資產未完全關閉而持續對外曝露；如確有遠端管理需求，應嚴格限制來源IP，並採用加密通道(如SSH)	➢ 定期盤點並更換外洩帳號憑證，搭配多因素驗證(MFA)，以強化存取安全 ➢ 建立弱點修補與驗證機制，確保風險持續改善 ➢ 強化資安教育訓練，提升系統維運人員對憑證生命週期管理、加密協定設定及對外服務管理之安全意識

■實兵演練

實兵演練係模擬真實攻擊情境，檢驗資通系統弱點、防護能力及應變機制，以提升整體資安防禦韌性

實兵演練揭露SQL Injection漏洞與明文密碼儲存風險

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，於擇定時間進行演練，至7/3止已累計199筆攻擊紀錄，本週新增弱點數量共12筆，分別為「無效的存取控管」6筆、「注入攻擊」3筆、「不安全的組態設定」2筆及「驗證機制失效」1筆，詳見圖6。

本週演練發現，衝擊性較高之弱點為「注入攻擊」。攻擊者於系統登入頁面輸入任意帳號密碼，透過瀏覽器開發者工具擷取登入請求內容並匯出，接續利用SQLMap等工具進行測試，成功利用SQL Injection弱點進行注入攻擊。攻擊者進一步取得使用者帳號密碼資料表，發現資料表內除儲存經Base64編碼之密碼外，亦保留明文密碼欄位，導致一旦資料庫遭入侵，使用者帳號密碼將直接曝露。

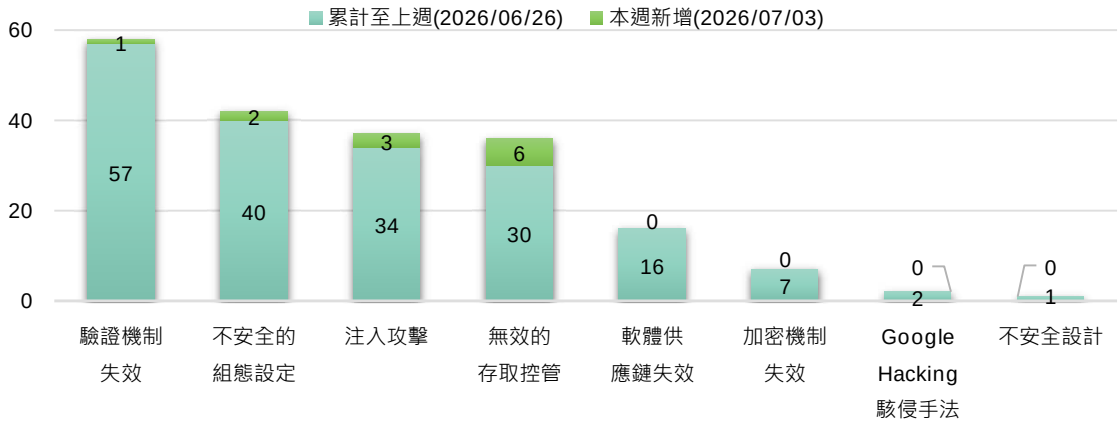

圖6 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 系統與資料庫介接時，應全面採用參數化查詢(Parameterized Query)或預備語句(Prepared Statement)，避免以字串拼接方式組成SQL指令，降低SQL Injection攻擊風險
- 應針對所有使用者輸入參數實施白名單驗證、特殊字元過濾及長度限制，並搭配WAF或其他防護機制阻擋異常請求，降低惡意語法成功注入之風險
- 使用者密碼不得以Base64等可逆方式編碼儲存於資料庫，亦不得保留明文密碼欄位，應採用具加鹽(Salt)之單向雜湊演算法進行儲存，以降低資料外洩後帳號遭利用之風險

■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

倒數優惠與限量下單成高風險廣告主要誘因

本週高風險詐騙關鍵字分析

本週高風險廣告仍以「優惠」出現次數最高，其次為「健康」、「配方」、「免費」、「投資」、「台灣」、「下單」、「老師」、「日本」及「AI」。除投資、保健類話術持續出現外，本週更明顯可見「倒數 1 小時」、「線上下單」、「數量有限」、「虧本價清倉」、「加賴洽談」等促購語氣，並擴散至樹苗水果、手串飾品、廚房用品、遊戲掌機及快速貸款等多種商品與服務情境，詳見圖7。

倒數優惠與限量下單製造急迫感

「優惠」、「下單」、「限量」、「虧本價」等字眼常搭配「倒數 1 小時」、「44 折優惠」、「數量有限」、「先到先得」、「全店虧本價清倉」等說法，促使民眾在未查證前快速付款或下單。提醒民眾，限時、限量、清倉或折扣過大的廣告，應先確認賣家身分、商品來源、退換貨規範及付款平台。

圖7 | 詐騙關鍵字文字雲

投資課程結合 AI 工具與老師名義

「投資」、「股票」、「老師」、「AI」、「APP」、「市場」等關鍵字顯示，投資廣告從課程銷售延伸至 AI 看盤系統、ETF 追蹤 APP、期貨教學及副業收入方案。提醒民眾，投資工具、AI 系統或老師課程均不能保證獲利，凡以限時折扣、免費報名、專屬工具或高收入案例吸引付款者，均應查證公司資訊、合約內容及退費機制。

健康配方話術轉向快速有感與居家護理

「健康」、「配方」、「日本」、「推薦」、「居家」、「古法」、「靈芝」、「烏黑片」等關鍵字，常見於草本清潤片、筋骨外用產品、護眼液、男性保健膠囊及烏黑片。廣告多以「一抹滲透快速有感」、「無需手術」、「中醫師推薦」、「古法草本」、「讓頭髮黑起來」等說法放大身體焦慮。凡宣稱快速改善症狀、治療疾病或取代醫療行為者，均應查證合法標示與產品來源。

樹苗、山竹與生活用品也成導流情境

本週可見山竹樹苗、新鮮山竹、液壓千斤頂、廚房剪、手串飾品、涼感內衣、止汗產品及遊戲掌機等內容，常以「全台灣可種植」、「貨到付款」、「直接加賴洽談」、「加 LINE 詢問購買」、「僅限線上下單」導向私下交易。提醒民眾，生活商品看似金額不高，仍可能有假賣場、付款後失聯或個資蒐集風險。

本週防詐提醒

1. 「倒數」、「限量」、「虧本價」、「先到先得」常用來催促下單，不代表交易安全。
2. 投資、期貨、AI 看盤、ETF APP 及副業課程，不得宣稱保證獲利。
3. 草本、漢方、護眼、筋骨、男性保健及烏黑片等商品，若宣稱快速見效，應查證合法標示。
4. 樹苗、水果、廚房用品、遊戲掌機、飾品等商品若要求加 LINE或私訊交易，應提高警覺。
5. 不要提供身分證、金融帳戶、信用卡、驗證碼或病歷資料給陌生賣家、客服、貸款人員或課程招募者。

綜合觀察

本週高風險廣告除延續投資與健康話術外，更明顯透過「倒數優惠」、「線上下單」、「限量清倉」、「加賴洽談」推動即時交易，並擴及樹苗水果、生活用品、遊戲掌機、AI 投資工具及快速貸款等多元場景。凡遇到來源不明、資訊不完整、要求私下聯繫或先付款的廣告，均應暫停操作並查證。

焦點文章

社交工程郵件攻擊案例分析

社交工程郵件濫用免費圖片託管與分享空間PNGUP

近期資安院發現，駭客於社交工程釣魚郵件攻擊當中，濫用免費圖片託管與分享空間PNGUP作為惡意檔案下載站，該網站為免費之雲端分享空間，提供使用者上傳檔案並產生下載連結，以供檔案存取或分享。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。

本次攻擊手法中，駭客以「請求報價」為由，偽裝成一般商業往來信件，要求收件者依據附件內容提供發票，同時要求加蓋公司印章以利後續付款流程，藉此誘使收件者開啟惡意附檔，進而感染收件者之電腦設備，詳見圖8。

圖8 | 社交工程釣魚郵件內容範例

附件中內含一經混淆之惡意JavaScript腳本，若使用者點擊執行，將觸發執行PowerShell指令，並連線至免費圖片託管與分享空間「PNGUP」下載第二階段惡意檔案，經解碼載入後，最終惡意程式(AgentTesla)感染裝置並與惡意中繼站建立連線，詳見圖9。

焦點文章

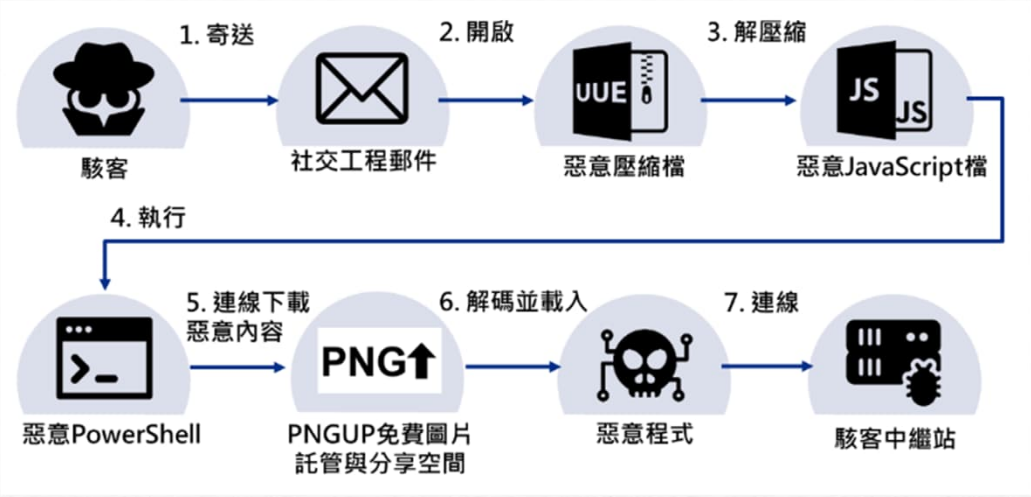

圖9 | 社交工程攻擊流程

防護建議：

- 收到「請求報價」、「提供發票」等商業往來相關之郵件時，應提高警覺，透過可信管道查證、確認，請勿隨意開啟來路不明或非預期需求之附件。
- 附件壓縮檔內含 .js、.vbs、.bat、.cmd、.ps1、.exe、.scr 等高風險之檔案類型，應避免隨意開啟執行，以免觸發惡意指令導致連線至外部網站下載惡意程式，並進一步感染裝置。
- 隨時維持防毒軟體、作業系統及瀏覽器為最新版本，並開啟即時防護功能，以降低惡意附件、腳本檔或不明下載檔案執行後造成感染之風險。

關鍵字：社交工程攻擊、圖片託管、分享空間

刊名　資安週報第 52 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
訂閱網址　www.nics.nat.gov.tw/newsletter/
讀者信箱　www.nics.nat.gov.tw/mail2center/

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