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
完善網站目錄瀏覽設定 提升檔案與路徑資訊保護

聯防監控
偵測刺探高居首位 防禦迴避仍具威脅

蜜罐誘捕
Web服務系統攻擊趨勢增加

重大漏洞
Ivanti、Fortinet、Veeam及Check Point 高風險漏洞應盡速修補

外部曝險分析
元件漏洞明顯攀升 整體風險小幅增加

實兵演練
實兵演練揭露檔案上傳漏洞 遠端程式碼執行與系統權限遭取得

網路巡查高風險詐騙
高風險詐騙訊息以私訊導流 低門檻話術降低戒心

焦點文章
網路攻防演練統計與案例

2026.06.25
050

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

完善網站目錄瀏覽設定 提升檔案與路徑資訊保護

本週總計接獲14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異常連線占多數，詳見圖2。本週發現部分機關網站，外部人員於取得檔案連結後，將網址中的檔名去除，僅保留目錄路徑，即可顯示網站目錄列表(Index of)內容，致外部可直接檢視目錄結構及其中檔案。

此類情形表示網站目錄瀏覽功能未妥善關閉，若目錄內含備份檔、測試檔或其他非公開資料，仍可能增加資訊揭露與後續遭利用風險。建議各機關確認已關閉目錄列表功能，另宜將公開檔案、非公開檔案及暫存資料置於不同路徑並分開管理，避免混置於同一路徑，以降低因設定疏漏導致資料暴露風險。

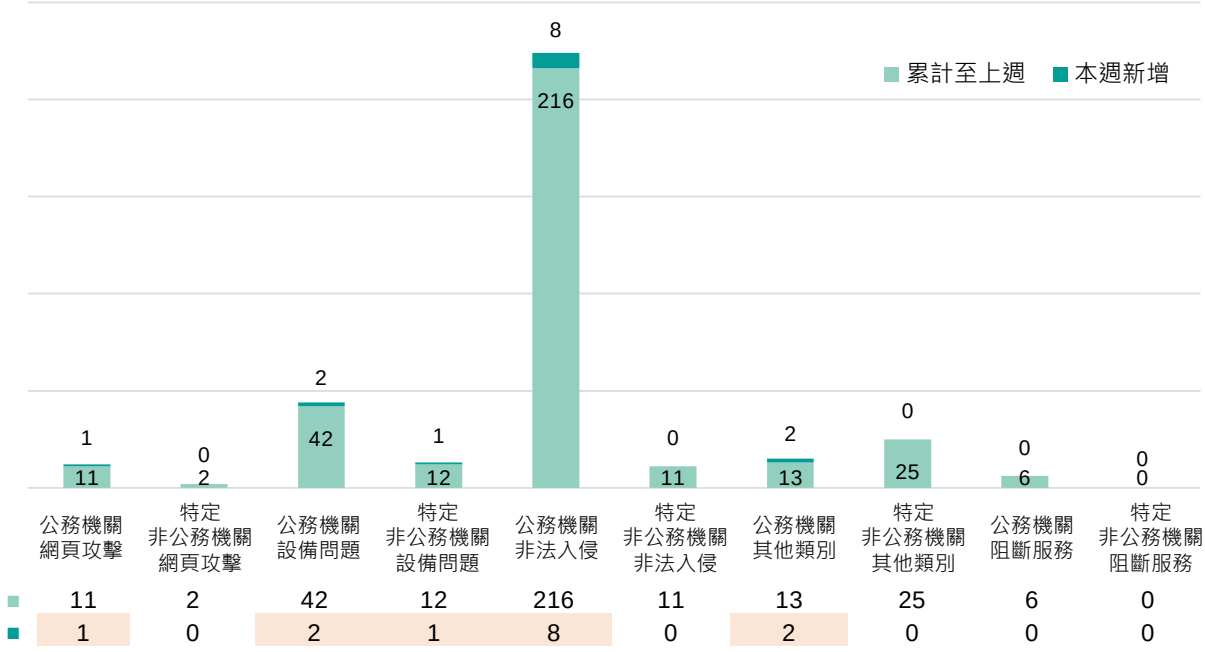

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

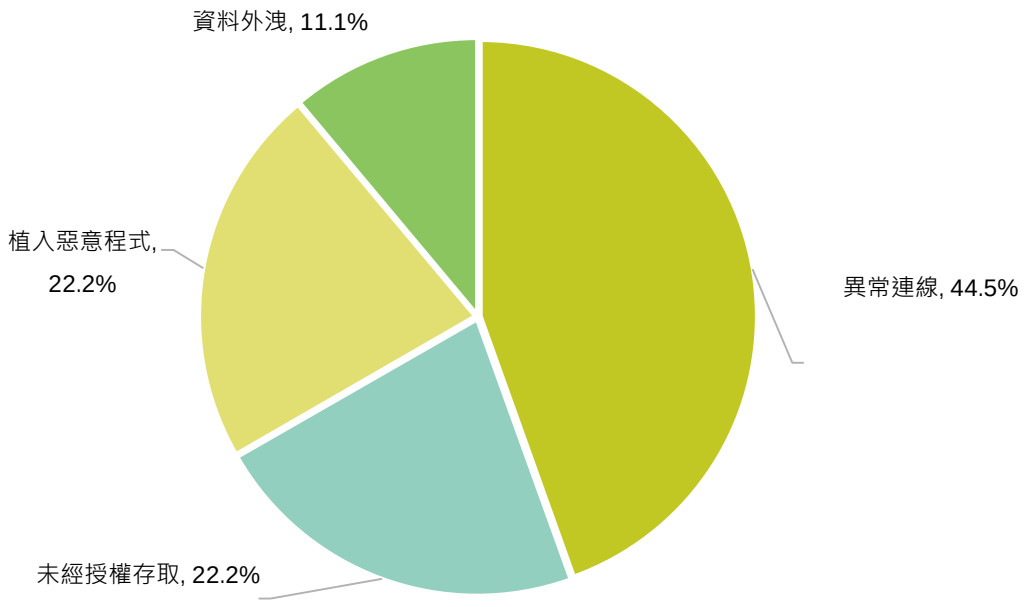

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者可藉由目錄內容蒐集系統情資，作為後續弱點利用或入侵依據 ➢ 若存在未妥善保護之檔案，可能遭大量下載或未授權存取	➢ 公開檔案、非公開檔案及暫存資料應分開存放並分級管理 ➢ 非公開檔案應採身分驗證及授權機制控管存取權限 ➢ 定期清查網站目錄中的備份檔、測試檔及歷史檔案 ➢ 持續監控異常目錄掃描及大量下載行為，及早發現可疑活動

1間民間企業揭露重大資安訊息

本週1家民間企業發布重大訊息，產業類別為電腦及週邊設備業，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
上福全球科技股份有限公司	115年6月16日	上福代重要子公司Katun Corporation發布重大訊息，Katun Corporation資訊設備遭受未授權外部存取，資訊部門立即執行系統隔離作業，防止擴大影響範圍並同步啟動防禦措施，同時委請外部資安專家協助及調查與排除，且加強內部資安偵測與防禦機制。 目前評估該事件對公司營運造成暫停出貨的影響，現階段出貨已陸續恢復中。後續將持續提升網路與資訊架構之安全控管，並持續監控以確保資訊安全。

■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

偵測刺探高居首位 防禦迴避仍具威脅

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。「偵測刺探」為最常見攻擊手法，占比15.4%，顯示攻擊者持續擴大對目標環境的前期偵查與資訊蒐集活動。觀察到的主要手法包括IP區段掃描、主動式掃描、以及憑證資訊蒐集。攻擊者通常利用自動化工具對大量網段與公開服務進行探測，以識別可存取主機、開放埠及服務版本資訊，並同步蒐集與帳號憑證相關的資訊，作為後續登入攻擊或滲透行動的依據。部分活動呈現由大範圍掃描逐步聚焦特定目標的特徵，顯示其偵查行為具備明確目的性與階段性。此類行為雖多屬攻擊前期準備階段，但將直接影響後續攻擊成功率與精準度。建議組織加強對異常掃描流量與帳號探測行為的監控，定期盤點對外暴露資產，並結合威脅情資分析來源活動，以提前辨識潛在攻擊準備跡象。

「防禦迴避」事件本週占比為15.1%，為本週占比次高的攻擊階段，顯示攻擊者持續強化規避監控與降低偵測機率的能力，以隱藏其惡意活動痕跡。觀察到的主要手法包括削弱指令歷程記錄、間接指令執行、以及清除指令歷程。攻擊者可能透過停用或修改系統指令記錄機制，降低安全設備對操作行為的可視性，亦會利用合法程序或腳本間接執行惡意命令，以避免觸發傳統防護規則；部分案例中，攻擊者於完成操作後主動清除 Shell 或系統指令歷程，以掩蓋活動軌跡並阻礙事後鑑識。此類手法具高度隱蔽性，能有效延長攻擊者在環境中的潛伏時間。建議加強對指令執行與日誌異常變更行為的監控，啟用集中式日誌保存機制，並針對可疑腳本與程序鏈進行行為分析，以降低攻擊者規避偵測的風險。

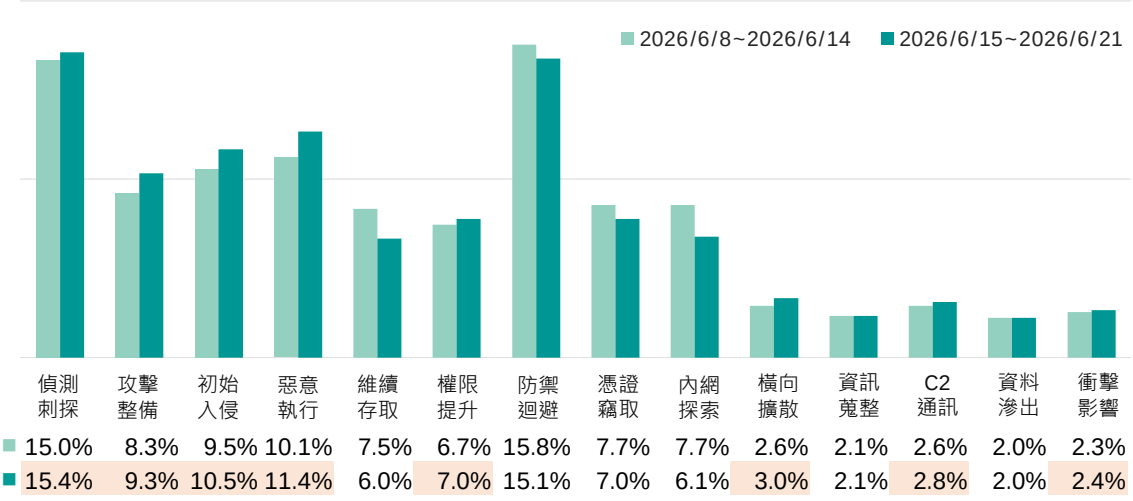

圖3 | 資安聯防監控攻擊階段統計

防護建議 **建議機關採取下列防護措施：**

偵測刺探（Reconnaissance）

- 監控異常掃描行為(大量連線、Port Scan、IP Scan)
- 定期盤點與清查對外公開資產，關閉非必要服務與埠口
- 強化帳號管理，避免帳號資訊外洩於公開網站或系統
- 導入威脅情資，比對可疑來源 IP 與掃描活動
- 設定告警機制，及早發現帳號探測與憑證蒐集行為

防禦迴避（Defense Evasion）

- 啟用集中式日誌蒐集與保存，避免本機日誌遭刪除
- 監控指令歷程(Command History)異常修改或清除行為
- 偵測合法工具(Living-off-the-Land)異常使用情形
- 加強程序鏈(Process Tree)與腳本執行行為分析
- 建立關鍵日誌與稽核設定變更告警機制

■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

Web服務系統攻擊趨勢增加

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71.39%、「遠端控制」服務攻擊占比23.84%，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71.71%。「遠端控制」服務亦有24.25% 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。而Web服務系統比例上升主因為Cisco Secure ASA & Cisco Secure FTD軟體授權缺失漏洞的CVE-2025-20362，遭攻擊次數上升導致。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。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。

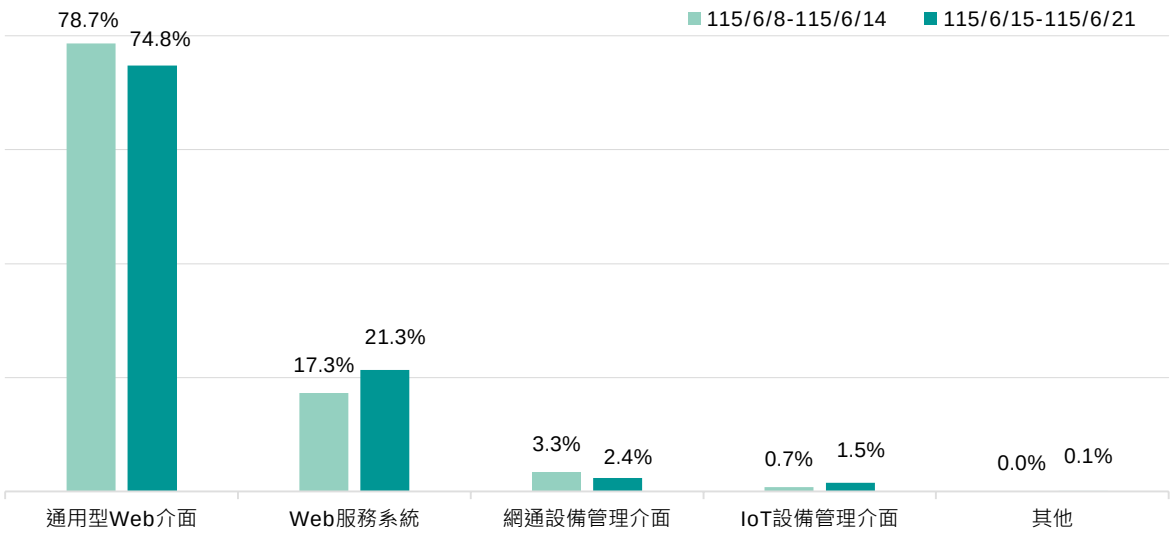

圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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越界讀取漏洞、授權缺失漏洞、跨站請求偽造、身分驗證繞過漏洞及路徑遍歷漏洞，攻擊目標涵蓋程式遞送控制器(ADC)、企業級網路防火牆軟體、多選下拉選單元件、網站主機伺服器管理系統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-2025-5777[1]	Citrix NetScaler ADC	7.5
■	2	↑2	CVE-2025-20362[2]	Cisco Secure ASA & FTD	6.5
■	3	↓1	CVE-2025-47204[3]	Bootstrap Multiselect	6.1
■	4	↓1	CVE-2026-41940[4]	cPanel & WHM	9.8
■	5	-	CVE-2025-30567[5]	WordPress WP01	7.5

類型 ■ 越界讀取漏洞 ■ 授權缺失漏洞 ■ 跨站請求偽造 ■ 身分驗證繞過漏洞 ■ 路徑遍歷漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
2. https://nvd.nist.gov/vuln/detail/CVE-2025-20362
3. https://nvd.nist.gov/vuln/detail/CVE-2025-47204
4. https://nvd.nist.gov/vuln/detail/CVE-2026-41940
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

Ivanti、Fortinet、Veeam及Check Point 高風險漏洞應盡速修補

- Ivanti Sentry存在高風險安全漏洞(CVE-2026-10520[1]與CVE-2026-10523[2])，類型分別為作業系統指令注入(OS Command Injection)與身分鑑別繞過(Authentication Bypass)。
  - CVE-2026-10520：未經身分鑑別之遠端攻擊者可以root權限執行任意程式碼，該漏洞已遭到駭客利用。
  - CVE-2026-10523：未經身分鑑別之遠端攻擊者可建立任意管理員帳戶以取得管理員權限。
- Fortinet FortiSandbox存在作業系統指令注入(OS Command Injection)漏洞(CVE-2026-25089[3])，未經身分鑑別之遠端攻擊者可透過發送特製HTTP請求，於系統上執行任意作業系統指令。
- Veeam Backup & Replication存在不安全之反序列化(Insecure Deserialization)漏洞(CVE-2026-44963[4])，已取得一般權限之遠端攻擊者可透過對未受信任之資料進行反序列化，進而於備份伺服器執行任意程式碼。
- Check Point多項產品存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-50751[5])，未經身分鑑別之遠端攻擊者無需透過帳號通行碼即可建立VPN連線，該漏洞已遭到駭客利用。

1. https://nvd.nist.gov/vuln/detail/CVE-2026-10520
2. https://nvd.nist.gov/vuln/detail/CVE-2026-10523
3. https://nvd.nist.gov/vuln/detail/CVE-2026-25089
4. https://nvd.nist.gov/vuln/detail/CVE-2026-44963
5. https://nvd.nist.gov/vuln/detail/CVE-2026-50751

■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

元件漏洞明顯攀升 整體風險小幅增加

本次針對曝險程度較高之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2,878項。其中，「元件高風險漏洞」以1,019項居首，「過時或弱加密協定」798項次之，「TLS憑證不受信任」553項位居第三。前三項合計2,370項，占前10大風險項目總數約82.3%，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2,788項，整體風險數量增加90項，增幅約3.2%。

進一步分析主要風險變化情形，「元件高風險漏洞」由915項大幅增至1,019項，增幅約11.4%，為本期整體風險增加之主要來源，詳見圖5。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍較為集中，且本期新增PEAR Archive_Tar相關弱點(CVE-2020-36193)，顯示對外網站伺服器、CMS及第三方套件之版本維護仍為後續改善重點。另「TLS憑證不受信任」由594項降至553項，降幅約6.9%；「過時或弱加密協定」由794項微增至798項，增幅約0.5%；「CSP設定不當」由245項微增至248項，增幅約1.2%，變化不大；「未部署WAF」則由95項大幅增至107項，增幅約12.6%。整體而言，本期外部曝險風險小幅上升，主要係受元件高風險漏洞增加影響，後續宜優先追蹤對外網站伺服器及第三方套件之版本維護與修補情形，並持續檢視網站應用層防護設定。

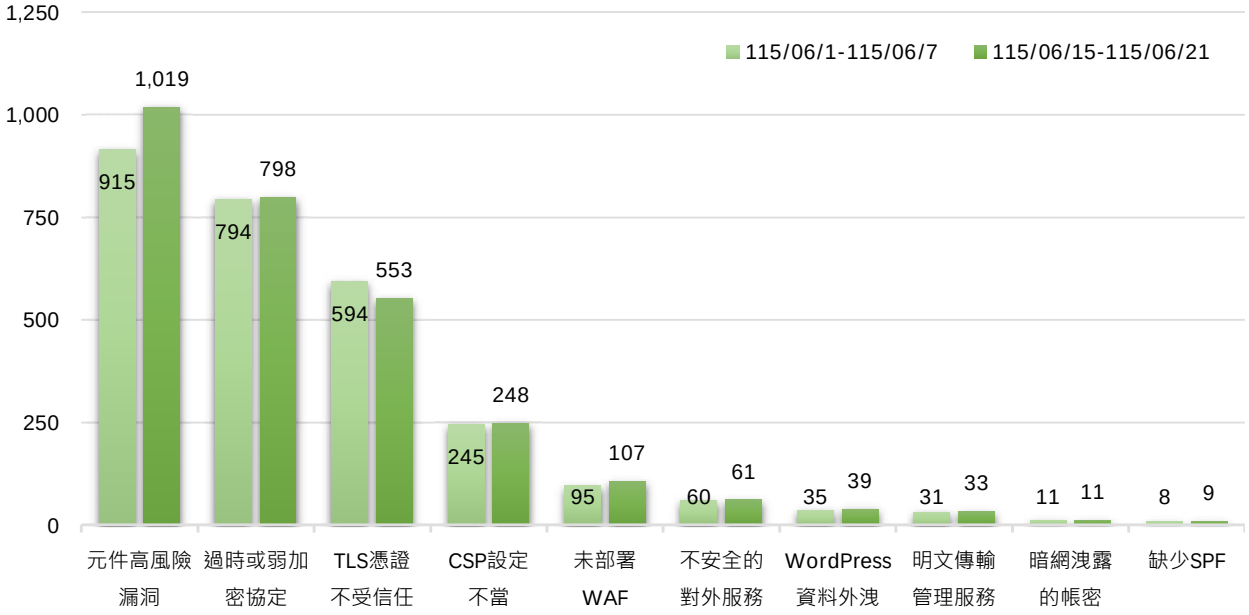

圖5 | EASM檢測結果統計(前10大風險)

防護建議

建議機關或關鍵基礎設施採取下列防護措施	建議機關或關鍵基礎設施採取下列管理措施
➢ 定期更新憑證，全面啟用TLS 1.2以上版本協定，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、主機與應用服務是否已確實完成下線，避免因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管理、加密配置及服務設定之安全意識

■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

實兵演練揭露檔案上傳漏洞 遠端程式碼執行與系統權限遭取得

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6/18止已累計169筆攻擊紀錄，本週新增弱點數量共26筆，分別為「不安全的組態設定」10筆、「無效的存取控管」8筆、「注入攻擊」4筆、「驗證機制失效」3筆及「軟體供應鏈失效」1筆，詳見圖6。

本週演練發現，衝擊性較高之弱點為「無效的存取控管」。攻擊者透過網頁原始碼發現系統檔案上傳功能之路徑與相關參數，並利用工具上傳惡意腳本，發現檔案上傳路徑。由於系統未妥善限制上傳目錄之存取與執行權限，攻擊手得以直接存取上傳檔案並執行系統指令，進一步取得資料庫名稱、資料庫帳號及資料庫密碼，接續從資料庫中取得系統管理者明文帳號密碼並成功登入系統。

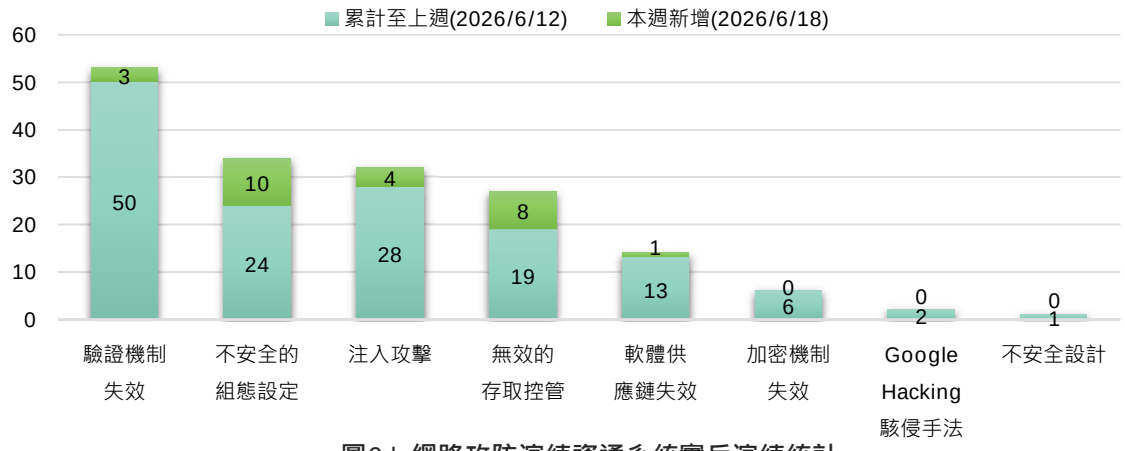

圖6 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應強化檔案上傳功能之身分鑑別與授權檢查，避免未經授權使用者存取或操作上傳功能
- 應於伺服器端落實檔案驗證機制，包含副檔名、MIME Type及檔案內容檢查，避免攻擊者透過偽造格式或混淆方式繞過檢核機制上傳惡意程式，並降低惡意程式執行風險
- 針對帳號密碼等機敏資訊，應避免以明文方式儲存於資料庫或設定檔中，同時落實最小權限原則，以降低機敏資訊外洩風險

■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

高風險詐騙訊息以私訊導流 低門檻話術降低戒心

本週高風險詐騙關鍵字分析

本週高風險詐騙訊息中，「私訊」仍是最主要的導流關鍵字，且明顯搭配「台灣」、「推薦」、「問題」、「健康」、「免費」、「優惠」等高頻字眼操作。從廣告內容觀察，詐騙訊息常先以中古車貸、樹苗販售、服飾團購、保健商品、護眼體驗、在家工作或感情法會等情境吸引民眾注意，再透過「歡迎私訊」、「加 LINE 下訂有折價」、「留言 +1 傳連結」、「私訊獲得免費體驗」等方式，將民眾導向私人通訊、短網址或不明表單，進一步蒐集個資、財務資料或引導付款，詳見圖7。

「私訊」不只是聯絡方式，而是離開公開平台的第一步

本週「私訊」出現次數明顯居首，且相關內容橫跨車貸、果樹苗、護眼商品、精品代購、感情法會及在家工作等類型。常見廣告會先以「全額貸款」、「低月付」、「品質保證」、「免費體驗」、「歡迎私訊報名」等話術引起興趣，再要求民眾改以 LINE、私訊或電話洽談。

提醒民眾，凡商品價格、貸款條件、工作內容、報名資訊或付款方式需透過私訊、LINE 或表單才會提供者，都應提高警覺。進入私人通訊管道後，對方可能要求提供姓名、電話、地址、身分證件、帳戶、信用卡或財力資料，也較容易避開平台交易保障及公開檢舉機制。

「台灣、推薦、設計」被用來包裝可信度與流行感

本週「台灣」與「推薦」均為高頻字眼，常被用來營造商品可靠、多人使用或正在熱銷的印象。例如服飾廣告標榜「台灣女生瘋搶」、「台灣設計」、「台灣熱銷」；團購內容則以「真心推薦」、「私心推薦必買」吸引留言互動；樹苗與保健商品也常使用「台灣優質」、「品質保證」、「院長推薦」等說法提高信任感。

惟「台灣」、「推薦」、「品質保證」、「官方認證」等字眼本身不代表交易安全。若廣告缺乏清楚商家資訊、產品標示、退換貨規範及公開客服管道，卻要求透過短網址、私訊或 LINE 完成交易，仍可能涉及假賣場、假代購、假認證或付款後失聯風險。民眾不宜僅憑在地、熱銷或推薦話術即判斷可信。

從「健康問題」切入，再用快速改善與專業背書推動購買

本週「問題」、「健康」、「血壓」、「保養」、「配方」、「調理」、「草本」、「枇杷」等關鍵字集中出現，顯示健康焦慮仍是重要話術。相關廣告常針對血壓、血脂、血糖、喉嚨乾癢、咳嗽、腰椎、視力、皮膚、肝臟保養及疲勞等需求，搭配「一喝有感」、「三效潤喉」、「草本配方」、「排毒燃脂」、「調節血壓血糖血脂」、「眼科醫生推薦」等說法，讓民眾誤以為商品能快速改善身體問題。

提醒民眾，凡保健商品宣稱可快速見效、改善多種症狀、逆轉疾病或取代治療，或以醫師、院長、日本進口、專利配方、GMP 認證等作為主要賣點者，都應先查證產品來源、合法標示及是否涉及誇大療效，不宜只憑廣告案例、使用見證或推薦名義就下單。

圖7 | 詐騙關鍵字文字雲

「免費、優惠、退費」常用來降低警覺，後續才是風險重點

本週「免費」與「優惠」出現頻率高，常見於樹苗、保健商品、車貸、護眼產品、線上課程及兼職招募等內容。例如「死苗免費補發」、「栽種後不結果全額退款」、「一盒免費體驗」、「0 元帶回家」、「零頭期」、「留言想了解」等說法，先讓民眾覺得參與成本低、風險不高，進而願意留言、私訊或加入 LINE。

但實際風險往往出現在後續流程，包括要求填寫表單、提供個資、身分證件、銀行帳戶、財力資料，或先支付運費、訂金、手續費、保證金。提醒民眾，凡以免費、優惠、零元、全額退款或免頭期吸引互動，卻在後續要求提供資料或先行付款者，均應暫停操作並查證來源。

「適合、必備、神器」放大生活需求，製造立即下單理由

本週廣告內容也大量使用「適合」、「必備」、「神器」、「簡單」、「穩定」、「不用」等字眼，將商品包裝成容易上手、立即需要的生活解方。例如樹苗廣告強調「適合盆栽地栽」、「新手容易照顧」、「不用噴藥不用套袋」；服飾廣告標榜「夏天必備」、「顯瘦神器」、「穿上瞬間降溫」；居家清潔與護腰產品則以「一台抵多台」、「快速清潔」、「穩定支撐」等說法吸引購買。

此類話術常再搭配「限量補貨」、「買到賺到」、「手慢等明年」、「現在下單再送」等急迫語氣，促使民眾在未查證前快速下單。提醒民眾，對於商品資訊不完整、只提供短網址或要求私訊下單的廣告，應先確認賣家身分、交易平台及付款方式是否安全。

本週防詐提醒

1. 「私訊」仍是本週最重要的風險訊號，凡廣告要求私訊、加 LINE、留言後才提供價格、連結、貸款條件、報名或下單方式者，應先查證商家身分與交易保障。
2. 看到「台灣熱銷」、「台灣設計」、「多人推薦」、「品質保證」、「官方認證」等字眼，不代表一定可信，仍應確認公司資訊、產品標示、客服管道、退換貨規範及付款頁面是否安全。
3. 保健商品若宣稱「一喝有感」、「調節血壓血糖」、「排毒燃脂」、「草本配方」、「眼科醫生推薦」、「日本進口」等，應查證產品合法來源及是否涉及誇大療效。

4. 「免費補發」、「全額退款」、「一盒免費體驗」、「0 元帶回家」、「零頭期」等低門檻話術，不代表沒有風險；若後續要求提供個資、帳戶或先付款，應立即提高警覺。
5. 車貸、在家工作、感情法會、精品代購及樹苗販售等內容，若採私訊成交、私下匯款，或缺乏清楚契約、售後、退換貨與交易保障機制，應避免倉促操作。

綜合觀察

綜合本週資料觀察，詐騙訊息多半先以「私訊」作為收口方式，再透過「台灣」、「推薦」、「健康」、「問題」建立可信度與需求感，並用「免費」、「優惠」、「必備」、「適合」降低戒心、放大購買理由。尤其本週可見車貸、樹苗、服飾、保健、護眼、兼職與感情服務等內容，均可能透過看似一般廣告的方式，引導民眾提供資料或付款。提醒民眾，凡遇到不明連結、短網址、私訊交易、資訊不完整，或要求提供個資、信用卡、銀行資料及先付款才能取得商品或服務者，均應先行查證，以降低受騙風險。

焦點文章

網路攻防演練統計與案例

從IoT設備與共通系統架構觀察攻擊擴散風險

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6月18日已累計169筆攻擊紀錄，包含10筆重大衝擊性弱點、88筆高衝擊性弱點、4筆中衝擊性弱點及67筆低衝擊性弱點，主要發現弱點案例如下：

「不安全的組態設定」弱點

某機關之IoT設備與其設備管理服務存在「不安全的組態設定」弱點，攻擊者於掃描過程中發現對外開放之服務埠為設備登入介面。攻擊者透過登入介面畫面搜尋到該設備預設帳號密碼，後續利用設備所提供ONVIF服務成功新增帳號，並取得設備資訊及使用者清單等資料，詳見圖8。

圖8 | 攻擊者藉由不安全組態設定新增未授權帳號

本案例顯示部分IoT設備於帳號管理、身分驗證機制及存取控制設計上仍有不足，若遭惡意利用，可能導致設備資訊外洩及未授權存取風險。

「注入攻擊」弱點

某機關之網站系統存在「注入攻擊」弱點，攻擊者發現該網站與其他機關使用同一家廠商開發之系統，具有相似之登入介面與功能路徑，並存在SQL Injection弱點，於是利用SQLMap等工具針對相同之網址參數進行測試，成功透過SQL Injection攻擊取得帳號、密碼，詳見圖9。

焦點文章

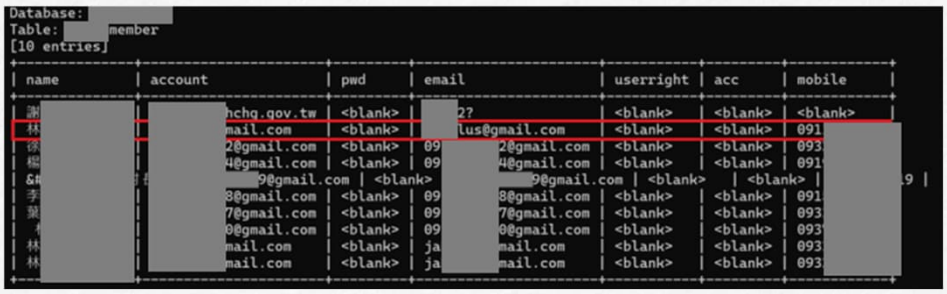

圖9 | 透過SQL Injection攻擊取得帳號、密碼

本案例顯示，若採用相同系統程式架構、驗證邏輯或功能模組，當系統存在弱點時，相同弱點極可能同時影響至不同單位或機關，攻擊者重複利用相同弱點進行攻擊，導致攻擊受駭範圍擴大。

改善建議：

- 應落實IoT設備安全管理，避免使用原廠預設帳號密碼。
- 設備管理介面與相關服務應依業務需求進行存取控制與來源限制，降低未經授權存取風險。
- 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)安全機制，避免因未妥善處理使用者輸入內容而產生注入攻擊風險。
- 針對由同一廠商開發或採用相似系統架構之系統，應於發現弱點後同步進行全面性檢測與複查，避免攻擊者利用相同手法於不同系統間進行重複利用。

關鍵字：網路攻防演練、資通系統實兵演練、IoT

刊名　資安週報第 50 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