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
凡網頁要求複製貼上指令者 宜提高警覺並審慎確認

聯防監控
防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕
Web服務系統攻擊趨勢減少

外部曝險分析
關鍵基礎設施外部曝險加劇 加密協定與TLS憑證風險急升

實兵演練
實兵演練揭露SQL Injection與驗證機制弱點風險

網路巡查高風險詐騙
詐騙訊息常以優惠與健康話術誘導點擊不明連結

2026.05.28
046

資安儀表板

事件通報、聯防監控、蜜罐誘捕、外部曝險分析及實兵演練等五類量化指標

■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

凡網頁要求複製貼上指令者 宜提高警覺並審慎確認

本週總計接獲5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。本週偵測機關設備連線異常網域，經情資顯示相關網域疑與假CAPTCHA頁面有關，駭客可能透過偽裝驗證或操作提示，誘導使用者手動開啟PowerShell或執行不明指令，進而下載惡意程式。

此類手法不同於傳統惡意附件或連結下載，而是將攻擊行為轉移至使用者操作階段，藉由要求複製貼上指令、開啟系統工具或執行命令等方式，提高誘導成功率並增加辨識難度。建議持續留意異常網域連線、PowerShell執行及可疑下載行為，並提醒宣導，凡網頁要求複製貼上指令、開啟系統工具或執行不明命令者，均應提高警覺，避免依指示操作。

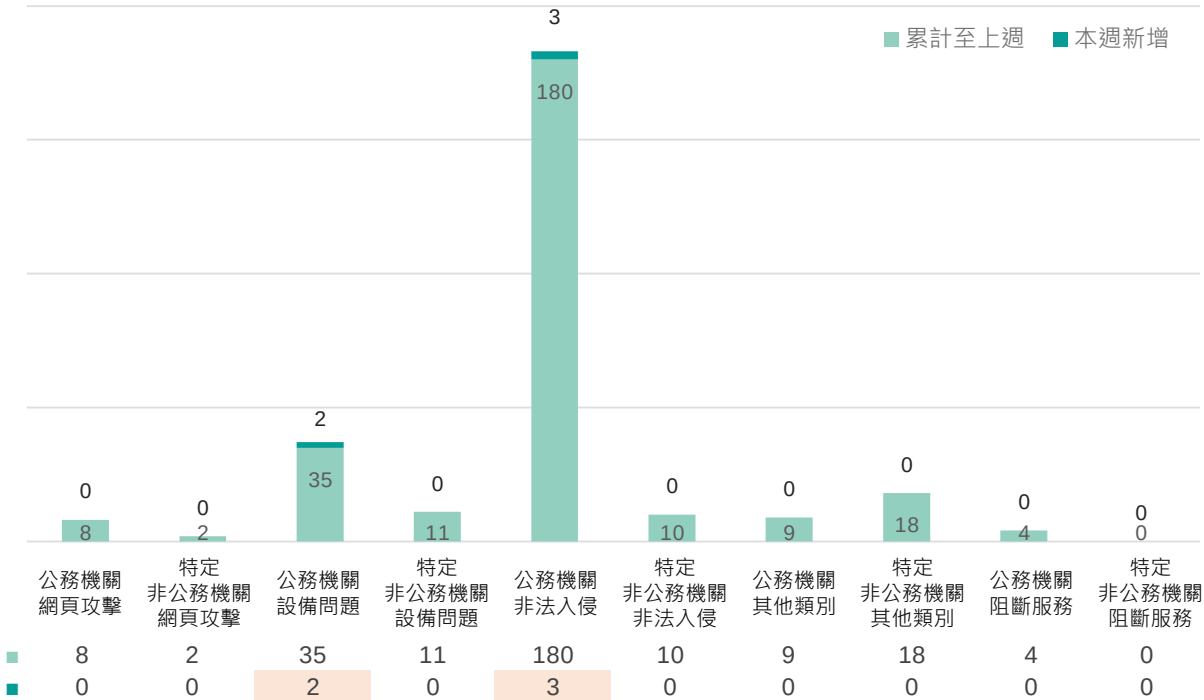

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

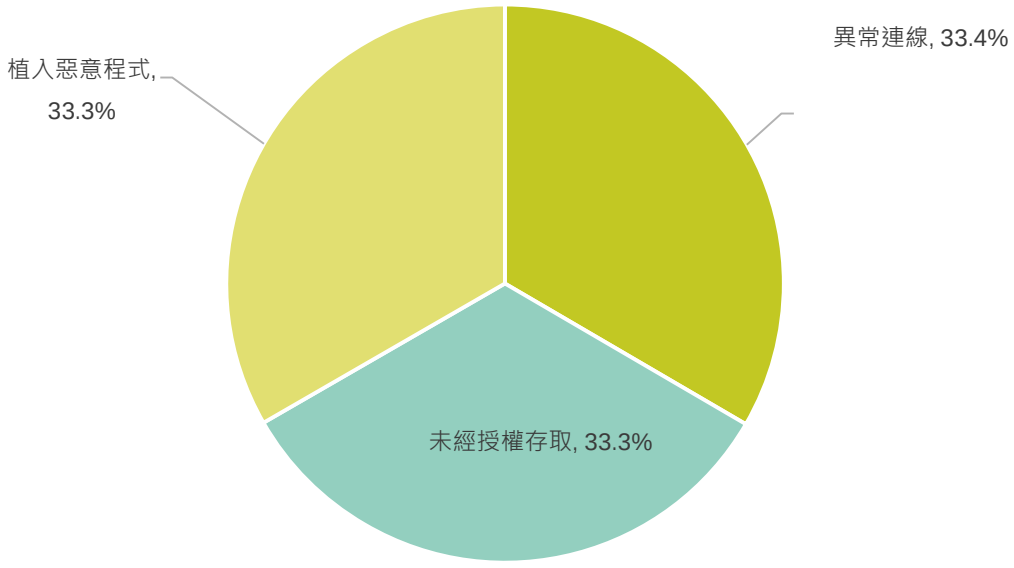

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 使用者誤信偽冒驗證頁面導致惡意程式下載與設備遭遠端控制 ➢ 設備建立異常對外連線後可能遭利用進行橫向移動與資料外洩	➢ 限制PowerShell與高風險腳本工具執行權限並保留稽核紀錄 ➢ 強化端點異常行為與對外連線監控即時發現可疑活動 ➢ 定期辦理新型社交工程攻擊情境演練提升人員警覺能力 ➢ 建立惡意網站與可疑網域阻擋機制降低連線風險

2間民間企業揭露重大資安訊息

本週2家民間企業發布重大訊息，產業類別皆為其他電子業，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
建德工業股份有限公司	115年5月20日	建德工業公司之資訊系統疑似遭駭客網路攻擊，已立即啟動相關防護機制，且無個資、機密資料外洩等情事發生，對公司營運無重大影響。 目前已全面盤查資訊系統，確保無植入木馬程式等攻擊手段，後續將持續提升網路資訊安全架構，並持續嚴密監控，以確保資訊安全。
弘塑科技股份有限公司	115年5月21日	弘塑公司資訊系統於4月10日遭受勒索病毒攻擊，全面停止舊系統使用，並於第一時間借助外部專業團隊進行相應措施，於最短時間內復原運營所需資料。 本次事件對公司生產及進出貨等主要營運未造成重大影響，公司商業機密及重要資訊迄今未發現外洩情事，主要在報廢及修復受影響之軟硬體設施、聘請外部專業團隊及復原資料，亦產生部分支出造成損失金額約2,200萬。 後續將持續加強資訊安全監控與防護機制，提升網路與資訊基礎架構之安全管理，並導入更完善之資安控管措施，以降低未來風險。

■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16.9%，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15.9%，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前期偵查與資訊蒐集行動。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。攻擊者透過自動化工具大規模掃描外部網段與公開服務，以識別可存取主機、開放埠與系統類型，同時蒐集與帳號憑證相關的資訊，作為後續登入嘗試或攻擊行動的基礎。部分活動顯示攻擊者會先進行廣泛探測，再逐步聚焦特定服務與帳號目標，以提高後續攻擊成功率。此類行為多屬攻擊前期準備階段，雖不直接造成破壞，但能有效提升後續滲透與入侵效率。建議強化對異常掃描流量與登入探測行為的監控，定期檢視對外資產暴露情形，並結合威脅情資分析掃描來源，以提前辨識潛在攻擊準備活動。

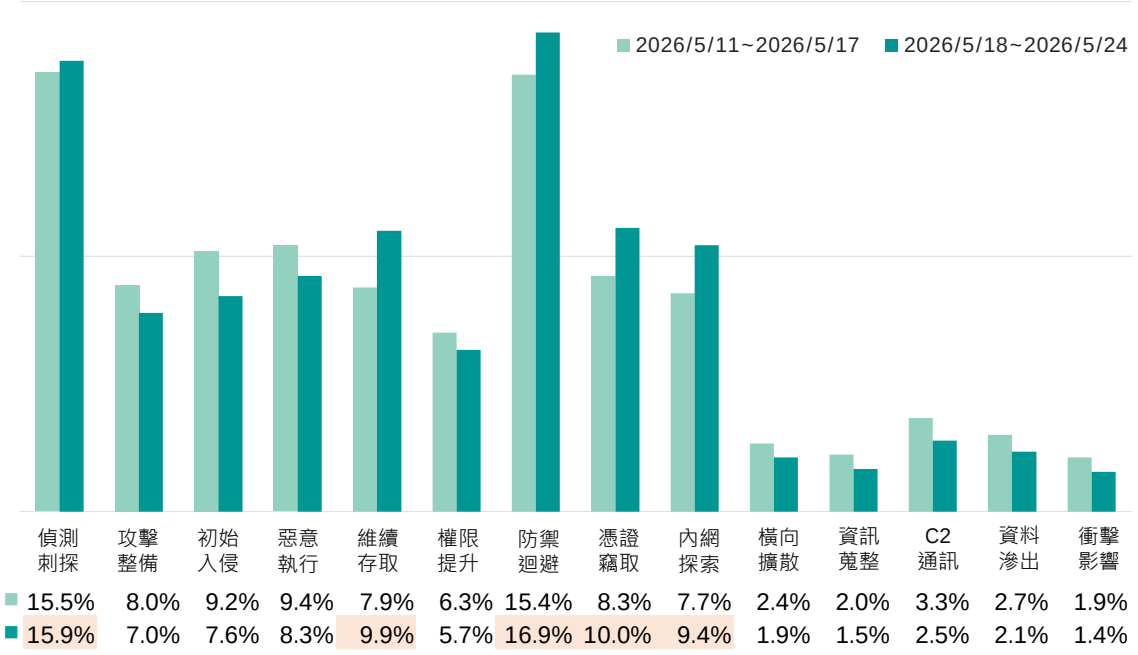

圖3 | 資安聯防監控攻擊階段統計

防護建議 **建議機關採取下列防護措施：**

偵測刺探（Reconnaissance）

- 強化對外服務與網段的掃描行為監控
- 部署 IDS / IPS 或流量分析機制，偵測異常探測流量
- 定期盤點與檢視對外暴露資產，降低攻擊面
- 監控異常登入嘗試與憑證蒐集行為
- 封鎖已知惡意來源 IP，並結合威脅情資分析掃描來源
- 針對公開服務落實弱點修補與存取限制
- 建立異常掃描與探測行為告警機制，提升早期預警能力

防禦迴避（Defense Evasion）

- 強化端點防護機制（EDR / 防毒）並定期更新規則
- 啟用並保留系統與指令操作紀錄，避免遭關閉或刪除
- 限制 PowerShell、PsExec、WMI 等高風險工具使用權限
- 加強特權帳號管理，落實最小權限與多因素驗證（MFA）
- 監控異常指令執行、程序注入與可疑系統工具使用行為
- 建立集中式日誌保存機制，避免攻擊者清除本機紀錄

■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服務系統攻擊趨勢減少

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64.79%、「遠端控制」服務攻擊占比30.72%，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67.25%。「遠端控制」服務亦有28.92% 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服務系統比例下降主因為Atlassian Confluence Server遠端程式碼執行漏洞的CVE-2024-21683，遭攻擊次數下降導致。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。

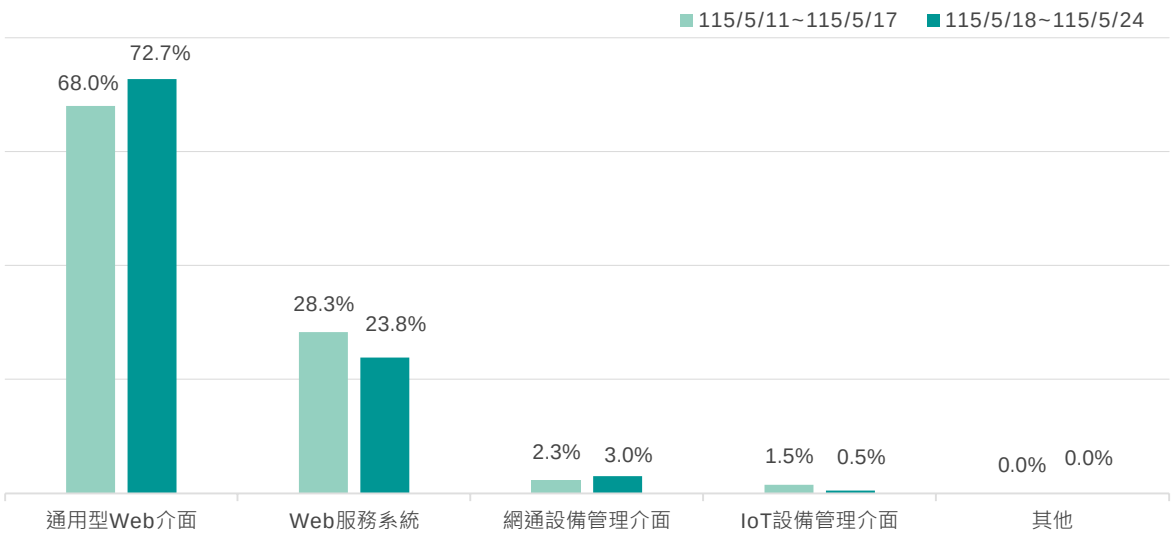

圖4 |本週網頁應用介面之誘捕攻擊比例統計

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3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、跨站請求偽造、作業系統命令注入漏洞及遠端程式碼執行漏洞，攻擊目標涵蓋企業級網路防火牆軟體、程式遞送控制器(ADC)、Bootstrap Multiselect、PHP伺服器端腳本語言及知識管理與團隊協作系統。

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3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-2025-47204[3]	Bootstrap Multiselect	6.1
■	4	↑1	CVE-2024-4577[4]	PHP	9.8
■	5	↓2	CVE-2024-21683[5]	Atlassian Confluence Server	8.8

類型 ■ 授權缺失漏洞 ■ 越界讀取漏洞 ■ 跨站請求偽造 ■ 作業系統命令注入漏洞 ■ 遠端程式碼執行漏洞

▶近期重大弱點提醒

近一週本院研究人員發現以下重大弱點資訊，建議組織內部進行檢查與修補：

- Cisco Catalyst SD-WAN存在高風險漏洞(CVE-2026-20182[6])，類型為身分鑑別繞過(Authentication Bypass)，因對等連線(Peering)驗證機制運作異常，導致未經身分鑑別之遠端攻擊者可透過發送特製請求，取得管理權限帳號。
- 以Chromium為基礎之瀏覽器存在79個高風險安全漏洞(CVE-2026-8509至CVE-2026-8587[7])，類型包含使用釋放後記憶體(Use After Free)與堆積型緩衝區溢位(Heap-based Buffer Overflow)等，最嚴重可使未經身分鑑別之遠端攻擊者誘使使用者開啟特製HTML頁面，進而逃脫瀏覽器沙盒環境。

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-2025-47204
4. https://nvd.nist.gov/vuln/detail/cve-2024-4577
5. https://nvd.nist.gov/vuln/detail/cve-2024-21683
6. https://nvd.nist.gov/vuln/detail/CVE-2026-20182
7. https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html

■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

關鍵基礎設施外部曝險加劇 加密協定與TLS憑證風險急升

本期針對 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 2,393 項 ，較上期 1,562 項增加 831 項，增幅約 53.2%，整體風險總量大幅上升，外部曝險態勢明顯惡化，詳見圖5。

其中，「元件高風險漏洞」以 912 項居首，「過時或弱加密協定」615 項次之，「TLS 憑證不受信任」393 項排名上升至第三，「CSP 設定不當」243 項排名下滑。前三項合計 1,920 項，占前 10 大風險項目總數約 80.2% ，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。

進一步觀察整體風險項目（含高風險與重大風險）變化，本期風險增幅主要來自加密通訊與憑證管理相關項目。其中，「過時或弱加密協定」增至 615 項，為上期約 2.5 倍 ；「TLS 憑證不受信任」增至 393 項，為上期約 11.6 倍，顯示部分外部服務在加密協定汰換、憑證信任鏈維護及憑證更新管理方面已有明顯惡化情形。此外，「元件高風險漏洞」仍以 912 項居首，較上期增加約 9.4%，代表元件版本控管與弱點修補仍是主要曝險來源；「CSP 設定不當」小幅上升 ，「未部署 WAF」則變化有限。整體而言，本期外部曝險風險除元件漏洞仍居高不下外，加密通訊協定過舊與 TLS 憑證管理風險增幅尤為顯著，建議列為後續優先改善重點。

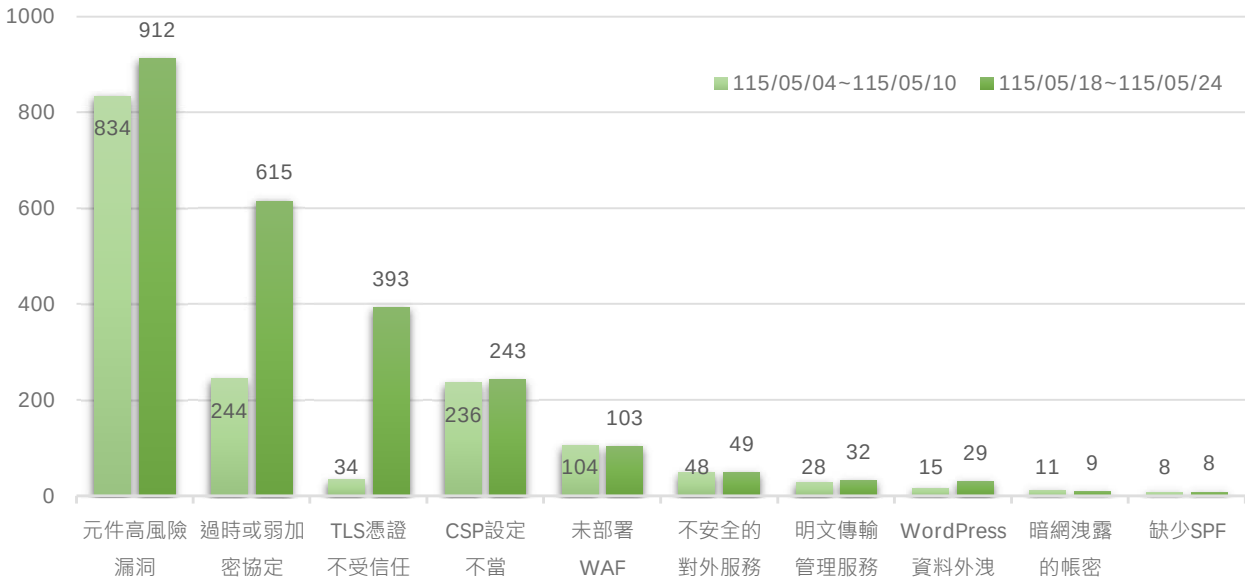

圖5 | EASM檢測結果統計(前10大風險)

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 以上版本之加密通訊協定 ➢ 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SQL Injection與驗證機制弱點風險

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5/22止已累計62筆攻擊紀錄，本週新增弱點數量共20筆，分別為「驗證機制失效」8筆、「不安全的組態設定」5筆、「注入攻擊」4筆、「無效的存取控管」2筆及「GoogleHacking駭侵手法」1筆，詳見圖6。

本週演練發現，由同一家廠商開發給不同機關之系統，其登入介面與功能路徑相似，導致在其中一個機關之系統發現弱點後，攻擊者亦可在其他機關之系統發現相同弱點。此外，攻擊者本週透過SQLMap等工具進行測試，成功利用SQL Injection弱點進行注入攻擊，進一步取得資料庫明文帳號密碼等資訊，並利用取得之帳號密碼成功登入其他系統。另發現部分系統存在驗證機制失效情形，攻擊者輸入帳號密碼後，系統於驗證失敗情況下仍允許存取管理頁面，成功新增內容至公告頁面，且於其他相似系統亦發現相同弱點。

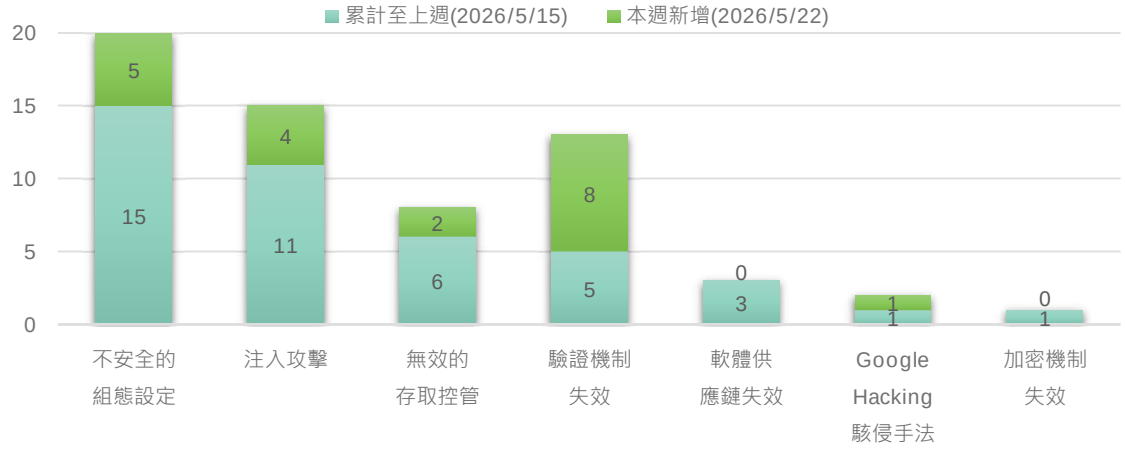

圖6 | 網路攻防演練資通系統實兵演練統計

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)，可有效將輸入資料視為純文字參數，而非可執行之SQL語法，降低SQL Injection攻擊成功風險
- 應針對所有輸入參數實施白名單驗證、特殊字元過濾與長度限制，避免惡意語法影響後端系統執行
- 系統登入與驗證流程應落實後端驗證機制，確認帳號、密碼及Session驗證邏輯正確性，避免於驗證失敗情況下仍允許使用者登入系統
- 建議針對相似系統進行全面性弱點檢測與複查，確認是否存在相同功能路徑、相同驗證邏輯或相同弱點，避免攻擊者利用相同手法進行存取

■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

詐騙訊息常以優惠與健康話術誘導點擊不明連結

本週高風險詐騙關鍵字分析

本週高風險詐騙訊息仍以商品廣告、保健宣傳及生活用品促銷作為主要包裝方式，常用「生活必備」、「台灣熱賣」、「貼心設計」、「限時優惠」、「多人推薦」等說法吸引民眾注意，營造商品來源可靠、價格划算、現在購買最適合的印象。這類內容看似一般購物廣告，實際上可能透過不明連結、表單、私訊或 LINE 帳號，引導民眾留下個資、聯絡方式或進入付款流程。

健康與保健話術觀察

從本週文本內容觀察，健康焦慮與身體不適是重要話術主軸。詐騙訊息常針對膝蓋、足跟、腰椎、關節、咳嗽、呼吸、疲勞等問題，搭配「草本配方」、「深層修護」、「高效舒緩」、「改善頑固問題」、「醫師推薦」、「臨床驗證」等字眼，宣稱可快速見效、免治療或一次改善。此類內容容易利用民眾對健康不適的焦慮，誘導購買來路不明商品，甚至要求填寫個人資料或信用卡資訊。

生活用品與促銷話術觀察

另有部分訊息以居家用品、收納、清潔、廚房好物、透氣鞋款等生活情境切入，透過「居家必備」、「清潔神器」、「收納空間」、「不用技巧」、「一鍵搞定」等說法，強調商品能快速解決生活困擾。此類廣告常搭配限時促銷、熱銷補貨或優惠倒數，讓民眾降低查證意願，在未確認賣家身分、網站網址及付款方式前就匆忙下單。

高單價商品與私下交易風險

此外，本週也出現珠寶、翡翠、水晶等較高單價商品宣傳，常以「正品保證」、「獨家設計」、「推廣優惠」、「實物拍攝」等說法提高可信度，並引導民眾透過留言、私訊或非正式管道完成交易。提醒民眾，此類商品若缺乏清楚的來源證明、鑑定文件、付款保障及退換貨機制，均應提高警覺，避免因私下交易導致付款後失聯或商品爭議難以處理。

本週防詐提醒

1. 健康焦慮是本週需特別注意的詐騙話術，凡涉及膝蓋、足跟、腰椎、牙痛、關節、咳嗽、呼吸或其他身體不適，並宣稱「快速修復」、「免治療」、「一次改善」者，都應先停下來查證。
2. 珠寶、翡翠、水晶等商品若採留言喊價、私訊成交或私下付款，應先確認鑑定證書、商品來源、付款方式及退換貨機制，不要只憑圖片、直播或賣家說法就匯款。
3. 「日本進口」、「醫師推薦」、「臨床驗證」、「正品保證」等字眼不代表一定可信，仍應檢視產品標示、商家資訊、合法販售管道及是否有誇大療效情形。
4. 若遇車貸、整債、博彩等廣告引導加入 LINE、填寫表單，並要求提供個資、財務資料、銀行帳戶或先行儲值、繳費者，應提高警覺，避免個資遭濫用或財物損失。
5. 凡出現短網址、不明賣場、商家資訊不完整，卻持續催促下單、入群、私訊、競標或付款的頁面，都應先查證再動作，不要因限時優惠或名額有限而倉促操作。

綜合觀察

綜合本週觀察，詐騙訊息多半先以「必備」、「台灣」、「設計」、「優惠」、「推薦」等高頻話術吸引注意，再透過「配方」、「健康」、「安心」、「神器」、「限時」等字眼增加可信度與急迫感，最後引導民眾點擊連結、私訊聯繫或進入不明付款頁面。提醒民眾，凡遇到要求點擊不明連結、填寫個人資料、提供信用卡資訊，或先付款才能取得商品、優惠或服務者，均應先停下來查證，避免落入詐騙陷阱，詳見圖7。

圖7 | 詐騙關鍵字文字雲

刊　　名　資安週報第 46 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