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

資安週報

Cyber Security Weekly Newsletter

2026.07.16
053

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

非必要管理功能應予關閉 必要功能應限制網段存取，並啟用身分驗證

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異常連線占多數，詳見圖2。本週發現有機關網站啟用Spring Boot Actuator管理功能，該功能主要供維運人員查看網站運作狀態、效能資訊及進行異常診斷，其中heapdump記憶體傾印功能未限制外部存取，致外部人員可直接匯出並下載Java應用程式執行期間之記憶體內容，並擷取其中留存之資料庫連線帳密。

由於網站運作時，記憶體中可能留存資料庫連線帳密、登入帳號密碼、使用者連線資訊、憑證、金鑰及個人資料等內容。建議確認網站是否啟用 Actuator 或其他系統診斷管理功能，非必要功能應予關閉；如有維運需求，應限制僅能由內部管理網段存取，並搭配身分驗證或防火牆等存取管控措施。另如確認記憶體傾印檔曾遭未授權下載，應立即停用相關功能，查核存取紀錄，並更換可能受影響之資料庫密碼、金鑰及憑證。

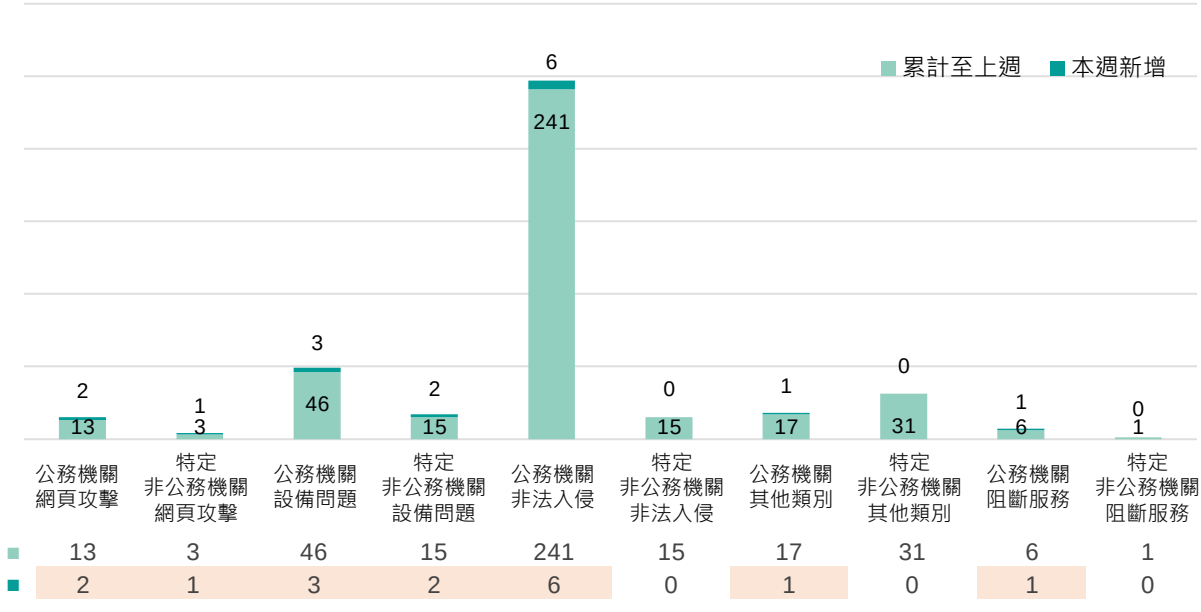

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

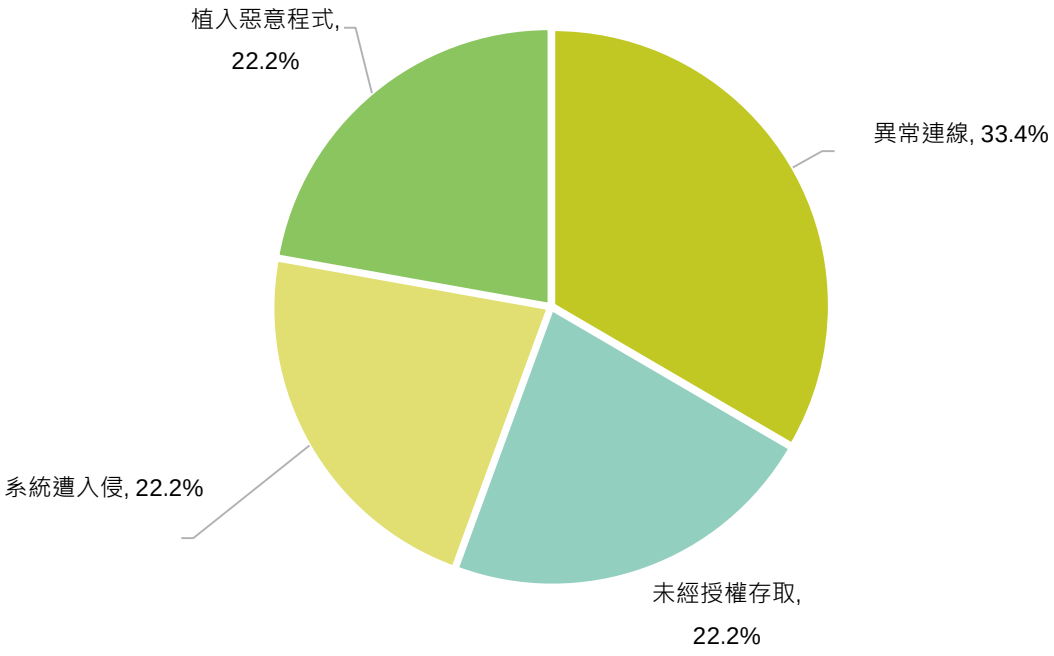

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 未限制 Actuator 管理功能存取，攻擊者可下載記憶體傾印檔竊取敏感資訊 ➢ 記憶體留存帳密、金鑰及憑證等資料，可能遭利用進一步入侵核心系統	➢ 關閉非必要 Actuator 與記憶體傾印功能，降低敏感資訊曝露風險 ➢ 限制管理介面僅允許內部管理網段存取，並啟用身分驗證機制 ➢ 建立網站管理功能定期盤點機制，確認診斷介面未對外開放 ➢ 發現記憶體傾印外洩時，立即更換帳密、金鑰及憑證並追查存取紀錄

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，產業類別為生技醫療業，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
優盛醫學科技股份有限公司	115年7月7日	優盛公司發現官網遭受駭客攻擊後，已立即啟動各項資安防護措施，將該網站進行隔離處理，並與委外資安技術公司及專家協助處理，後續依程序向主管機關通報。 該事件對公司營運、資訊安全、個資等無重大影響，後續將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

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14.7%，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14.2%，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。

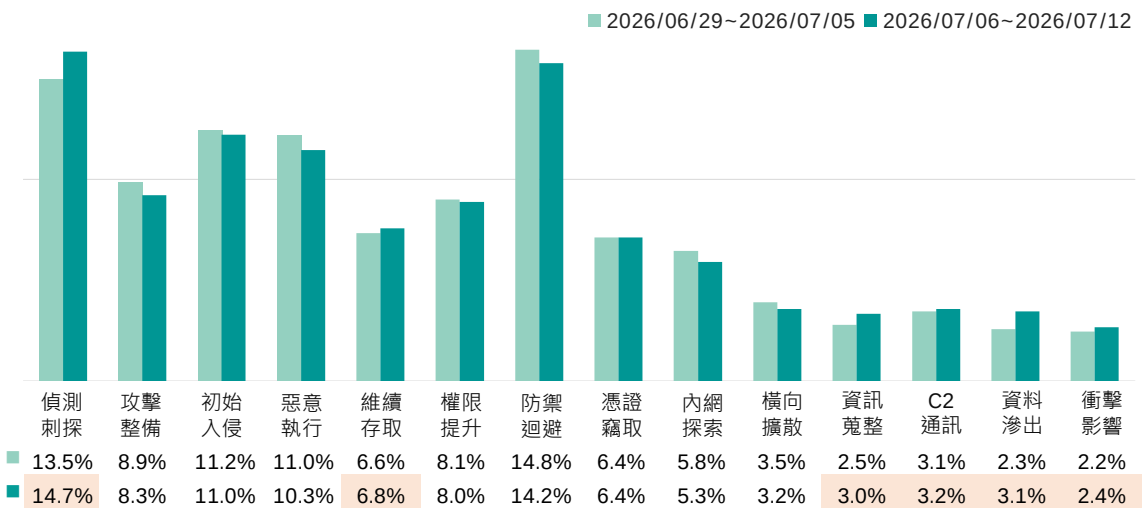

圖3 | 資安聯防監控攻擊階段統計

防護建議 **建議機關採取下列防護措施：**

偵測刺探(Reconnaissance)

- 監控異常掃描流量（如大量連線、Port Scan、IP 掃描）
- 定期盤點並減少對外暴露資產與服務
- 關閉不必要的連接埠及服務，降低攻擊面
- 加強帳號登入與憑證探測行為監控，啟用多因素驗證（MFA）
- 結合威脅情資（Threat Intelligence）封鎖已知惡意來源 IP

防禦迴避(Defense Evasion)

- 啟用集中式日誌蒐集與保存，避免日誌遭竄改或刪除
- 監控指令歷程（Command History）及日誌設定異常變更
- 偵測異常 PowerShell、Shell Script 及程序鏈（Process Tree）行為
- 啟用 EDR / 行為式偵測機制，識別間接指令執行與可疑腳本
- 定期檢查系統稽核與安全性設定，避免監控功能遭停用或削弱

■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81.26%、「遠端控制」服務攻擊占比16.12%，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78.64%。「遠端控制」服務亦有17.88% 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Web服務系統比例上升主因為GeoServer遠端程式碼執行漏洞的CVE-2024-36401，遭攻擊次數上升導致。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。

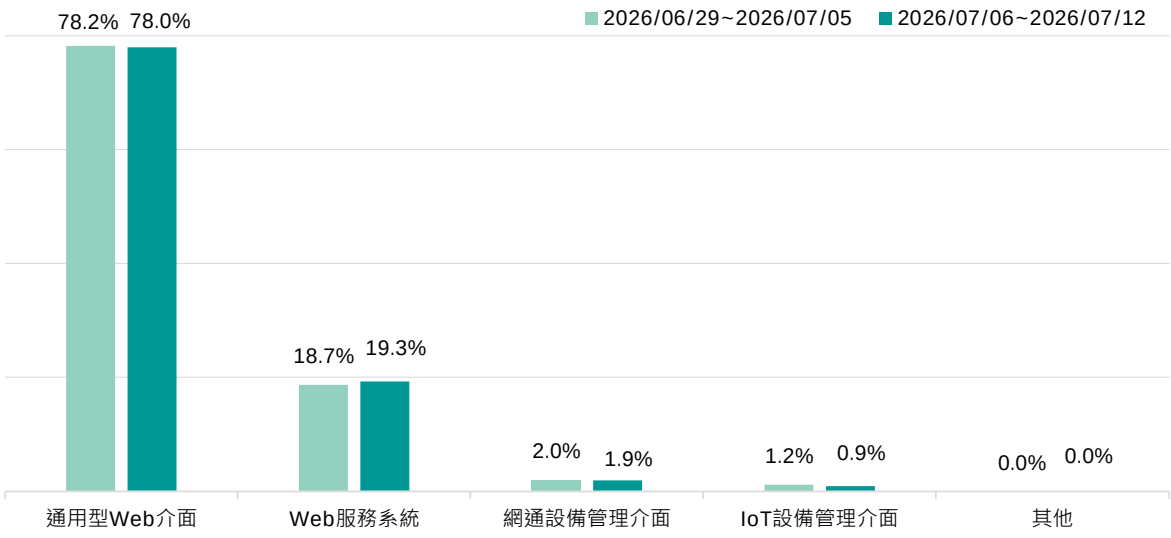

圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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、跨站請求偽造、資訊外洩漏洞及路徑遍歷漏洞，攻擊目標涵蓋企業級網路防火牆軟體、程式遞送控制器(ADC)、多選下拉選單元件、開源後端伺服器框架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-2025-47204[3]	Bootstrap Multiselect	6.1
■	4	⬇1	CVE-2025-53364[4]	Parse Server	5.3
■	5	-	CVE-2025-30567[5]	WordPress WP01	7.5

類型 ■ 授權缺失漏洞 ■ 越界讀取漏洞 ■ 跨站請求偽造
■ 資訊外洩漏洞 ■ 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-2025-47204
4. https://nvd.nist.gov/vuln/detail/CVE-2025-53364
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

NetScaler、pgAdmin及WatchGuard高風險漏洞應盡速修補

- NetScaler ADC與NetScaler Gateway存在多項高風險安全漏洞(CVE-2026-8451、CVE-2026-8452、CVE-2026-8655、CVE-2026-10816、CVE-2026-10817及CVE-2026-13474)[1]，其中最嚴重之CVE-2026-8452為記憶體溢位(Memory Overflow)漏洞，當受影響裝置被設定為Gateway或AAA Virtual Server功能時，未經身分鑑別之遠端攻擊者可利用此漏洞造成系統異常、阻斷服務或其他非預期行為。

- pgAdmin 4存在多項高風險安全漏洞(CVE-2026-12044至CVE-2026-12050)[2]，其中最嚴重之CVE-2026-12046為不安全反序列化(Insecure Deserialization)漏洞，當產品以伺服器模式運作，且攻擊者已知pgAdmin之Flask SECRET_KEY並具備寫入pgAdmin之Session目錄權限時，可利用此漏洞執行任意程式碼。

- WatchGuard Fireware OS存在使用釋放後記憶體(Use After Free)漏洞(CVE-2026-13368)[3]。當Mobile User VPN使用IKEv2協定且設定使用外部LDAP驗證伺服器時，未經身分鑑別之遠端攻擊者可利用此漏洞於iked程序執行任意程式碼。

1. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604
2. https://www.postgresql.org/about/news/pgadmin-4-v916-released-3324/
3. https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00023

■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

元件高風險漏洞大幅下降 帶動整體曝險風險減少

本次針對曝險程度較高之100個A、B級公務機關進行EASM資安曝險檢測，前10大風險項目共計9,630項。其中，「元件高風險漏洞」以4,050項居首，「過時或弱加密協定」1,989項次之，「TLS憑證不受信任」1,525項位居第三。前三項合計7,564項，占前10大風險項目總數約78.5%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密協定與憑證管理等議題。相較上期10,636項，本期整體風險數量減少1,006項，降幅約9.5%，詳見圖5。

進一步分析主要風險變化情形，「元件高風險漏洞」仍為最大宗風險，數量由上期5,008項減至本期4,050項，降幅約19.1%。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍為主要風險來源；Drupal核心相關弱點(CVE-2020-13671)已見減少，惟本期新增Archive_Tar相關弱點(CVE-2020-28949)。其他主要風險項目亦呈下降趨勢，「過時或弱加密協定」由2,016項減至1,989項，降幅約1.3%；「TLS憑證不受信任」由1,531項減至1,525項，降幅約0.4%。另「未部署WAF」由759項減至689項，降幅約9.2%。整體而言，本期外部曝險風險下降，主要來自元件高風險漏洞數量的大幅減少；惟部分元件仍持續出現新增弱點，受測機關仍須落實元件盤點、版本更新及弱點修補作業。

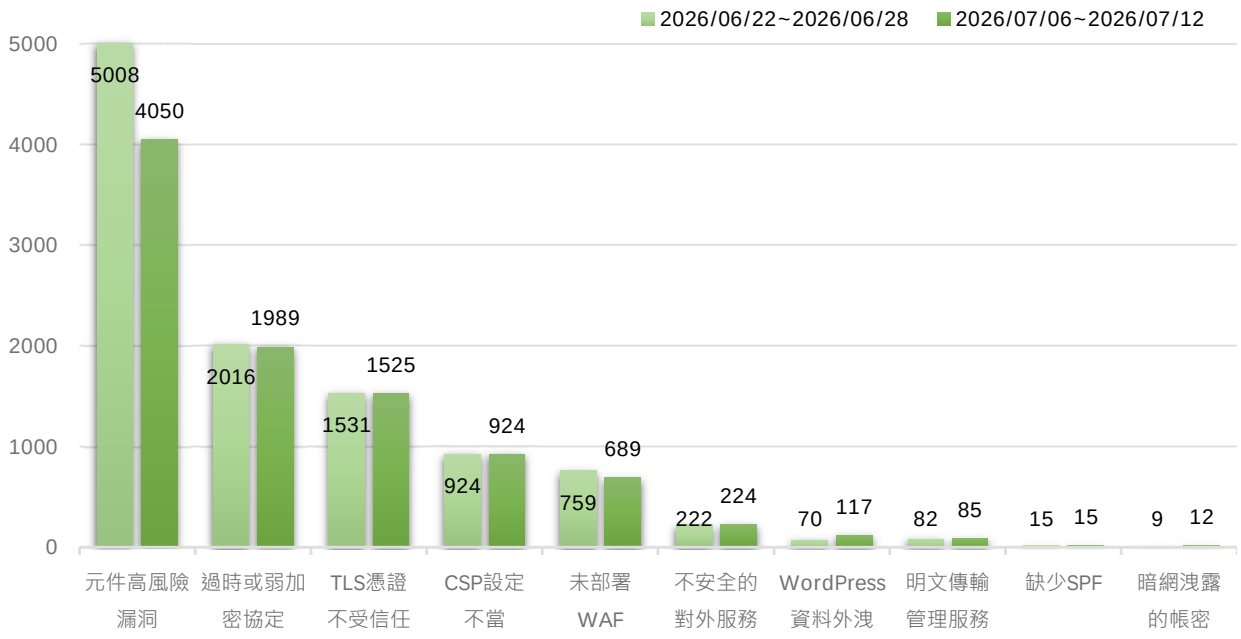

圖5 | EASM檢測結果統計(前10大風險)

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，並淘汰已停止維護之軟體版本 ➢ 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

實兵演練揭露加密機制失效 文件遮蔽不當致敏感資訊外洩風險

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7/9止已累計213筆攻擊紀錄，本週新增弱點數量共14筆，分別為「無效的存取控管」4筆、「不安全的組態設定」3筆、「軟體供應鏈失效」3筆、「加密機制失效」2筆及「驗證機制失效」2筆，詳見圖6。

本週演練發現，影響程度較高之弱點為「加密機制失效」。攻擊者於公開文件中發現已遮蔽之個人資料，進一步使用 LibreOffice Draw 開啟目標文件，移除覆蓋於內容上的遮蔽物件後，即可還原原始內容，取得個人資料。經檢視，該文件雖已於視覺上遮蔽敏感資訊，惟遮蔽物件僅覆蓋於原始內容之上，並未將原始資料自文件中實際覆蓋，因此仍可透過具備文件編輯功能之工具還原遭遮蔽內容。

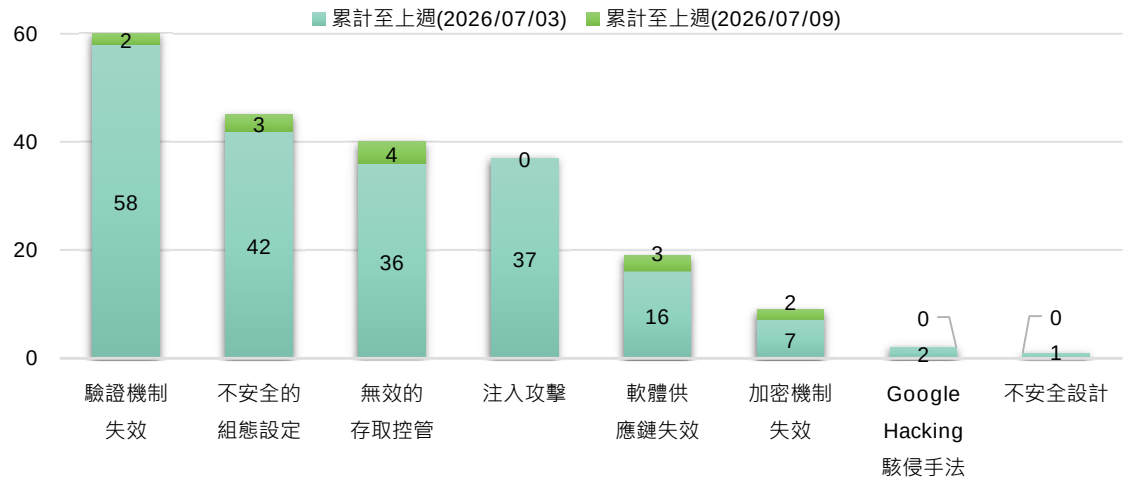

圖6 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 使用具備永久移除內容功能之文件去識別化工具，或是遮蔽後重新另存圖片，避免僅以圖形、色塊或文字方塊遮蔽敏感資訊
- 建立文件公開前審查機制，對外公開文件前，應重新檢視文件內容、圖層及遮蔽物件，確認敏感資訊已完全移除，並以不同文件檢視或編輯工具進行驗證
- 定期宣導人員正確執行文件去識別化作業，以避免機敏資訊因處理不當而外洩

■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

高風險廣告話術與導流手法觀察

本週高風險廣告多以「優惠」、「免費」、「健康」及賽事預測等話術吸引點擊，再導向LINE、私人群組或不明網站，要求民眾付款或提供個人資料，詳見圖7。

優惠與免費話術催促操作

「限時優惠」、「免費諮詢」、「買一送一」、「免費試用」及「立即領取」等說法，容易降低民眾戒心。提醒民眾，免費可能附帶運費、訂閱或個資蒐集；限時、限量及貨到付款，也不代表交易安全。

賽事分析宣稱準確比分

相關廣告常以大數據、專業分析及正確比分為名，誘導加入LINE群組、購買牌單或前往博弈平台。任何人均無法保證比賽結果，遇到要求匯款儲值或下載不明程式者，應立即停止操作。

健康商品誇大檢測效果

免扎針血糖手錶、手機健康檢測、腰椎器材及快速改善膚況等廣告，可能利用健康焦慮促銷。穿戴裝置及手機程式不能取代醫療診斷；凡宣稱快速治療、精準測量或名人專業推薦者，應查證產品許可與廣告真實性。

投資、副業及貸款廣告須提高警覺

投資與AI課程常以被動收入、快速創業或高額月收入招攬學員；貸款廣告則標榜免聯徵、免保人及低利率。投資及副業不能保證獲利，合法貸款也會進行必要審核。切勿預付保證金、寄送提款卡或提供驗證碼。

網購與私訊交易風險

翡翠、日本代購、服飾、生活用品及健康商品，常搭配原裝進口、限量供應或誇大功效，再要求加LINE或私訊下單。購買前應查核賣家、檢驗標示及退換貨規範，避免脫離原平台交易。

本週防詐提醒

1. 免費、限時及限量是常見催促話術。
2. 正確比分、保證獲利及快速見效均不可信。
3. 不加入不明LINE群組或點選陌生連結。
4. 不提供帳戶、提款卡、信用卡及驗證碼。
5. 遇到可疑廣告，先停止操作並撥打165查證。

綜合觀察

本週高風險廣告普遍採取「優惠吸引—私訊導流—要求付款或提供資料」的模式。凡遇到資訊不完整、過度宣稱效果或催促立即交易的廣告，均應提高警覺。

圖7 | 詐騙關鍵字文字雲

焦點文章

雙刃劍的暗面：生成式 AI 在網路攻擊與精準釣魚的演進與防禦

AI 浪潮下的網路安全新挑戰

隨著生成式人工智慧（Generative AI）與大型語言模型（LLM）的爆發式成長，這項技術不僅轉型了全球的商業生產力，也無可避免地成為網路犯罪份子的新興軍火。傳統的網路釣魚（Phishing）與社交工程（Social Engineering）多依賴人工撰寫，常因拙劣的語法、不自然的語氣或明顯的拼字錯誤而被資安防護系統或警覺的用戶識破。

然而，現今的威脅者已將 AI 深度融入攻擊生命週期。從自動化情報搜集到幾秒內生成毫無破綻的誘騙內容，AI 正在將網路攻擊的門檻「平民化」，同時將攻擊規模與精準度提升至前所未有的高度。本篇資安焦點文章將全面拆解 AI 武器化的核心手法、關鍵威脅數據及企業防禦之實務指南。

一、AI 驅動的攻擊與釣魚四大核心手法

1. 消除語言與文化壁壘的「超完美釣魚郵件」

   傳統釣魚郵件常因非母語者撰寫而顯得生硬。如今，攻擊者利用 AI 工具（甚至包括在暗網販售的惡意 AI 模型如 WormGPT 與 FraudGPT），能夠在數秒內生成符合特定企業文化、專業術語且語法完全無瑕疵的郵件。這使得傳統依賴「尋找錯字」或「檢視生硬中文」的員工資安意識培訓逐漸失效。

2. 精準自動化的「魚叉式釣魚」（Spear-Phishing）

   過去，針對高階主管或關鍵財務人員的魚叉式釣魚需要耗費數周人工搜集情報。現在，AI 惡意腳本能自動爬取目標在 LinkedIn、社群媒體及企業官網的公開資料，快速分析其人際網絡、近期參與專案與過往說話風格。AI 在建立這種個性化漏洞檔案的準確度極高，並能據此量身打造極具說服力的客製化誘騙內容。

3. 多模態威脅：深偽技術（Deepfake）與語音複製

   AI 釣魚已不再局限於文字。多模態 AI 的成熟讓「商務電子郵件詐騙（BEC）」演變為「深偽視訊/語音詐騙」。攻擊者只需取得高階主管數秒的公開演講音檔（如 YouTube 影片或公開研討會音訊），即可完美複製其聲音，並在電話中要求財務人員緊急匯款。更甚者，利用即時深偽濾鏡在視訊會議中冒充高層，已在全球造成數起重大的企業實質損失。

焦點文章

4. 變種惡意軟體與自動化規避偵測

除了前端的社交工程溝通，攻擊者亦利用 AI 自動修改惡意代碼特徵（Polymorphic Malware）。AI 能針對現有的資安防禦機制（如安全郵件閘道器 SEG）進行對抗式測試，微調郵件中的隱喻、結構、超連結跳轉或代碼特徵，藉此繞過傳統基於特徵碼（Signature-based）的靜態攔截過濾系統。

二、 驚人的關鍵數據（最新威脅態勢）

根據多間國際知名資安機構與微軟威脅情報（Microsoft Threat Intelligence）的最新統計，AI 帶來的威脅呈現指數型成長：

1. 攻擊量暴增：2025 年末至 2026 年初，AI 生成與輔助之釣魚攻擊在短時間內出現了高達 14 倍的驚人激增。
2. 點擊率與速度：在 AI 輔助的網路攻防戰中，平均漏洞偵測與攻擊發動時間顯著縮短；而含有精準上下文脈絡的 AI 釣魚郵件，其受害者點擊率提升了近 50%。
3. 新興媒介崛起：伴隨 AI 釣魚而來的，還有結合 QR Code 的「掃碼釣魚（QRishing）」與繞過驗證的 CAPTCHA 釣魚。單在 2026 年第一季，微軟偵測到的 QR Code 釣魚郵件便在短短三個月內激增 146%，顯示攻擊者正利用 AI 大規模多管道佈局。

三、 企業與個人應如何防禦 AI 時代的釣魚攻擊？

面對精明、快速且無孔不入的 AI 威脅，傳統的「見招拆招」防禦已不敷使用，企業必須邁向主動式、零信任（Zero Trust）的防禦架構：

1. 「以 AI 對抗 AI」：導入整合機器學習與行為分析的次世代郵件安全解決方案。不只檢查寄件者 IP 或網域，更要透過 AI 審查郵件的「行為意圖」、上下文語境與情感施壓特徵是否異常。
2. 推動防釣魚多因素驗證（MFA）：傳統的簡訊或 App 驗證碼容易被 AI 生成的即時假網站中間人攔截（AitM）。企業應全面升級為基於 FIDO2 規範、具備網域綁定能力的防釣魚 MFA（如 FIDO2 硬體密鑰或 Passkeys）。

焦點文章

3. 重新定義「安全控制流程」：建立嚴格的雙管道驗證機制。凡涉及財務匯款、重要權限變更或敏感資料調閱，即便是「執行長或高階主管在視訊或電話中親自交辦」，也必須透過第二個獨立的內部認證管道確認，徹底防範深偽（Deepfake）詐騙。
4. 資安意識培訓升級：員工培訓必須從單純的「找拼字與語法錯誤」轉向「識別異常行為、利益誘惑與急迫性暗示」（例如：突然要求繞過正常簽核程序、營造極大的時間壓力等）。

結論

AI 被用於網路攻擊與釣魚活動，標誌著網路犯罪已進入「自動化、規模化與工業化」的新紀元。在這場硬核的技術攻防戰中，資安防禦者不能再依賴傳統肉眼與靜態規則。唯有建立全面零信任的防禦思維，並積極導入 AI 資安偵測工具，才能在 AI 武器化的暗潮中，有效守住企業與個人的核心數位資產防線。

參考文獻 (References)

1. Hoxhunt. (2026). 2026 Phishing Trends Report. Retrieved from Hoxhunt Research Insights. (指出 AI 生成之釣魚攻擊在近期出現 14 倍的爆發性成長，且每次釣魚事件平均造成極高的企業損失)。
2. Microsoft Threat Intelligence. (2026, April 30). Email threat landscape: Q1 2026 trends and insights. Microsoft Security Blog. (詳細揭露 2026 年第一季高達 83 億次郵件威脅，以及結合 AI 與 QR Code、CAPTCHA 的新型態複合釣魚激增數據)。
3. Zensec. (2026, March). Phishing statistics 2025 - 2026: The numbers you need to know. (統計指出高達 82.6% 的釣魚郵件含有 AI 協作痕跡，且 AI 釣魚郵件的點擊率顯著提升)。
4. SQ Magazine & Cybersecurity Analytics. (2026). AI Cyber Attacks Statistics 2026: How Attacks, Deepfakes & Ransomware Have Escalated. (提供 AI 魚叉式釣魚建立漏洞檔案具備 88% 準確度，以及深偽語音/視訊商務電子郵件詐騙增加之關鍵數據)。
5. Kymatio Cybersecurity. (2025, July). Phishing Trends 2026: AI-Phishing, QRishing & Voice Deepfakes. (探討生成式 AI 如何抹平語言壁壘，並融合多模態技術進行高階主管冒充之手法)。

關鍵字：釣魚郵件、Deepfake、惡意軟體

刊　　名　資安週報第 53 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