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
持續強化刷卡機等設備之防護措施與可視性 以利事件發生後之追查與處置

聯防監控
防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕
程式遞送控制器(ADC)成攻擊熱點

外部曝險分析
加密協定與憑證風險急遽攀升 外部曝險情勢惡化

實兵演練
實兵演練揭露驗證機制未落實密碼強度要求 致帳號遭未授權存取風險

網路巡查高風險詐騙
詐騙話術結合信任包裝與優惠誘因 降低民眾戒心導流交易

焦點文章
利用合法工具AutoIt的攻擊鏈情資分享

2026.06.04
047

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

持續強化刷卡機等設備之防護措施與可視性 以利事件發生後之追查與處置

本週總計接獲24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。本週觀察到多起事件之受害設備為刷卡機，惟機關多於發現異常後即採下架或汰換處置，致後續較難完整釐清事件原因與入侵途徑，另，相關設備普遍未設置防火牆或存取控管，亦未定期進行安全性檢查或韌體更新，增加事件追查與應變困難。

此類設備多屬嵌入式系統，部分設備可能仍使用 FTP 進行檔案傳輸、設定交換或廠商維護，一旦未妥善限制存取來源、帳號權限及可寫入路徑，即可能成為惡意程式植入入口。建議各機關除持續盤點刷卡機等設備外，亦應檢視其是否仍開放 FTP 或其他不必要服務，確認帳號密碼管理、存取來源限制及韌體更新情形，並儘可能提升設備運作紀錄與異常行為可視性，以利事件發生時及早發現、即時處置及後續追查。

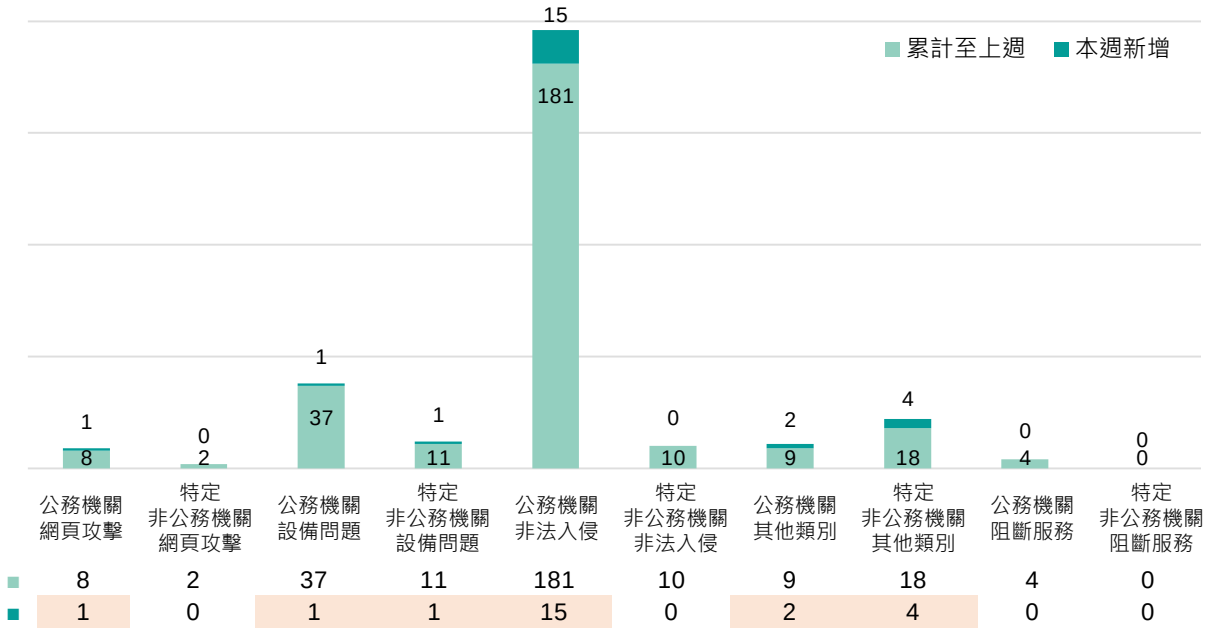

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

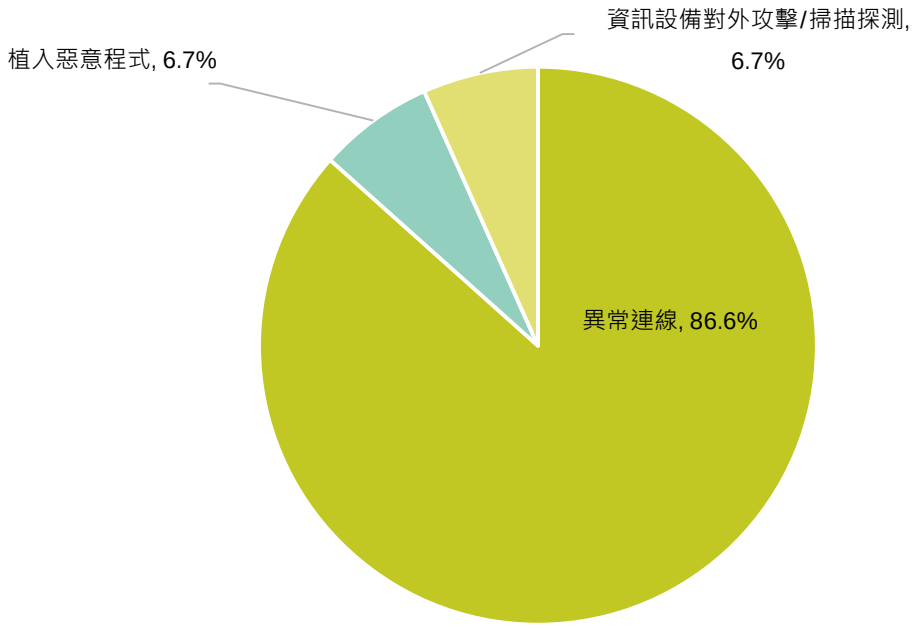

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 刷卡機開放FTP等服務且缺乏存取控管，可能成為惡意程式植入管道 ➢ 設備缺乏日誌紀錄與監控機制，事件發生後難以追查入侵途徑	➢ 定期盤點刷卡機等設備，關閉FTP及其他非必要網路服務 ➢ 強化設備帳號權限管理，限制維護來源IP與遠端存取範圍 ➢ 建立韌體更新與弱點檢查機制，降低已知漏洞遭利用風險 ➢ 啟用設備日誌留存與異常監控功能，提升事件追查與應變能力

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，產業類別為數位雲端，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
數字科技股份有限公司	115年5月26日	數字科技因進行內部活動網頁開發與測試流程，程式碼管理作業設定不當，導致部分未去識別化之測試原始碼曾短暫推送至外部平台，包含專案之會員姓名、身分證字號、電子郵件等個資。 當日資安團隊偵測發現後，已隨即啟動資安緊急應變機制，已於當日14:00完成全面下架、刪除及封鎖程序，隨後同步進行歷史紀錄清除、外部存取痕跡確認、密鑰輪替及全站程式碼安全掃描，已確認該風險路徑完全阻斷。

■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15.7%，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14.9%，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。

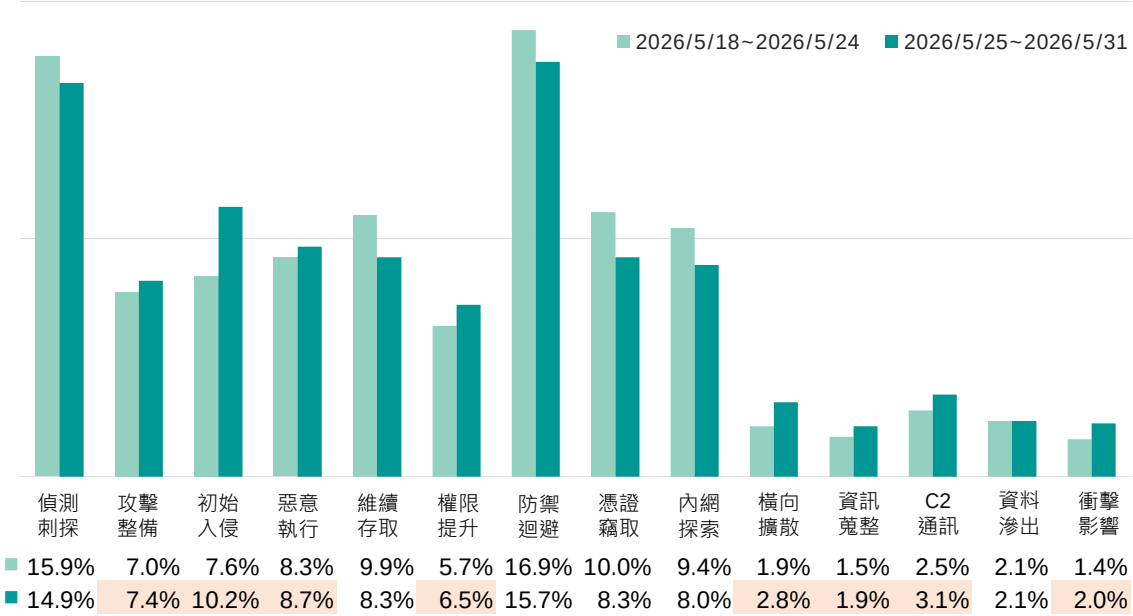

圖3 | 資安聯防監控攻擊階段統計

防護建議 **建議機關採取下列防護措施：**

防禦迴避（Defense Evasion）

- 強化端點防護（EDR/XDR），監控異常程序與命令執行行為
- 啟用並集中保存系統、PowerShell、Shell 等操作日誌，避免遭竄改或刪除
- 限制高風險系統工具（如 PowerShell、WMIC、PsExec）使用權限
- 落實最小權限原則與特權帳號管理（PAM）
- 建立異常停用防毒、刪除日誌等行為的告警機制
- 定期檢視系統設定變更及安全控制措施狀態

偵測刺探（Reconnaissance）

- 監控異常掃描流量與大量連線探測行為
- 部署 IDS/IPS 或 NDR 偵測網路偵查活動
- 定期盤點並降低對外暴露資產與服務
- 關閉非必要對外開放埠與管理介面
- 持續監控帳號探測、暴力破解與憑證填充（Credential Stuffing）行為
- 結合威脅情資（TI）封鎖已知惡意來源 IP
- 定期檢查公開資訊洩露情形，避免帳號、系統資訊暴露於網際網路

■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

程式遞送控制器(ADC)成攻擊熱點

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67.25%、「遠端控制」服務攻擊占比28.92%，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68.19%。「遠端控制」服務亦有28.82% 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服務系統比例大幅下降主因為Cisco Secure ASA軟體或Cisco Secure FTD軟體授權缺失漏洞的CVE-2025-20362，遭攻擊次數大幅下降導致。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。

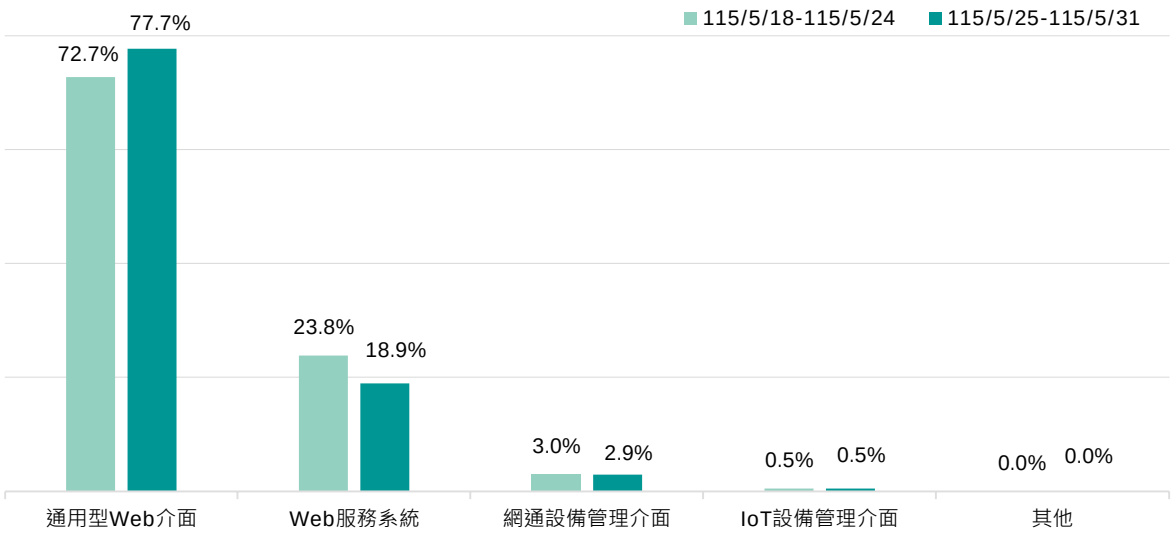

圖4 |本週網頁應用介面之誘捕攻擊比例統計

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、跨站請求偽造、授權缺失漏洞、身份驗證繞過漏洞及遠端程式碼執行漏洞，攻擊目標涵蓋程式遞送控制器(ADC)、多選下拉選單元件 、企業級網路防火牆軟體、網站主機伺服器管理系統及React 伺服器元件架構，其中 cPanel & WHM存在身分鑑別繞過之CVE-2026-41940漏洞，允許未經身份驗證的遠端攻擊者，在未經授權的情況下存取控制面板。顯示以上類型系統已成為高風險熱點。

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	⬆1	CVE-2025-5777[1]	Citrix NetScaler ADC	7.5
■	2	⬆1	CVE-2025-47204[2]	Bootstrap Multiselect	6.1
■	3	⬇2	CVE-2025-20362[3]	Cisco Secure ASA & FTD	6.5
■	4	⬆new	CVE-2026-41940[4]	cPanel & WHM	9.8
■	5	⬆new	CVE-2025-55182[5]	React Server Components	10

類型 ■ 越界讀取漏洞 ■ 跨站請求偽造 ■ 授權缺失漏洞
■ 身份驗證繞過漏洞 ■ 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 Secure Workload存在高風險漏洞(CVE-2026-20223[6])，類型為缺乏身分鑑別(Missing Authentication)，未經身分鑑別之遠端攻擊者可透過傳送特製API請求，以Site Admin權限，讀取敏感資訊或變更系統設定。
- PostgreSQL存在11個高風險安全漏洞(CVE-2026-6472至CVE-2026-6479、CVE-2026-6575、CVE-2026-6637及CVE-2026-6638[7])，類型包含堆疊型緩衝區溢位(Stack-based Buffer Overflow)、SQL注入(SQL Injection)及整數迴繞(Integer Wraparound)等，最嚴重可使取得一般權限之遠端攻擊者執行任意程式碼。

1. https://nvd.nist.gov/vuln/detail/cve-2025-5777
2. https://nvd.nist.gov/vuln/detail/CVE-2025-47204
3. https://nvd.nist.gov/vuln/detail/CVE-2025-20362
4. https://nvd.nist.gov/vuln/detail/CVE-2026-41940
5. https://nvd.nist.gov/vuln/detail/cve-2025-55182
6. https://nvd.nist.gov/vuln/detail/CVE-2026-20223
7. https://www.postgresql.org/about/news/postgresql-184-1710-1614-1518-and-1423-released-3297/

■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

加密協定與憑證風險急遽攀升 外部曝險情勢惡化

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9,419項，較上期6,760項增加2,659項，增幅約39.3%，詳見圖5。其中，「元件高風險漏洞」以4,232項居首，「過時或弱加密協定」以1,720項升至第二，「TLS憑證不受信任」以1,386項升至第三。前三項合計7,338項，占前10大風險項目總數約77.9%，顯示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。

本期整體風險上升，主要係受加密協定與憑證管理相關項目大幅增加影響。其中，「過時或弱加密協定」已增至上期約4.7倍，「TLS憑證不受信任」更增至上期約28.3倍，反映部分機關於加密通訊設定、憑證有效性及站台維運管理仍有明顯缺口。相較之下，「元件高風險漏洞」僅小幅增加，「CSP設定不當」及「未部署WAF」則略有下降，顯示本期風險惡化並非全面性擴散，而是集中於加密協定與憑證管理面向，後續宜優先強化憑證盤點、汰換及安全通訊設定檢核。

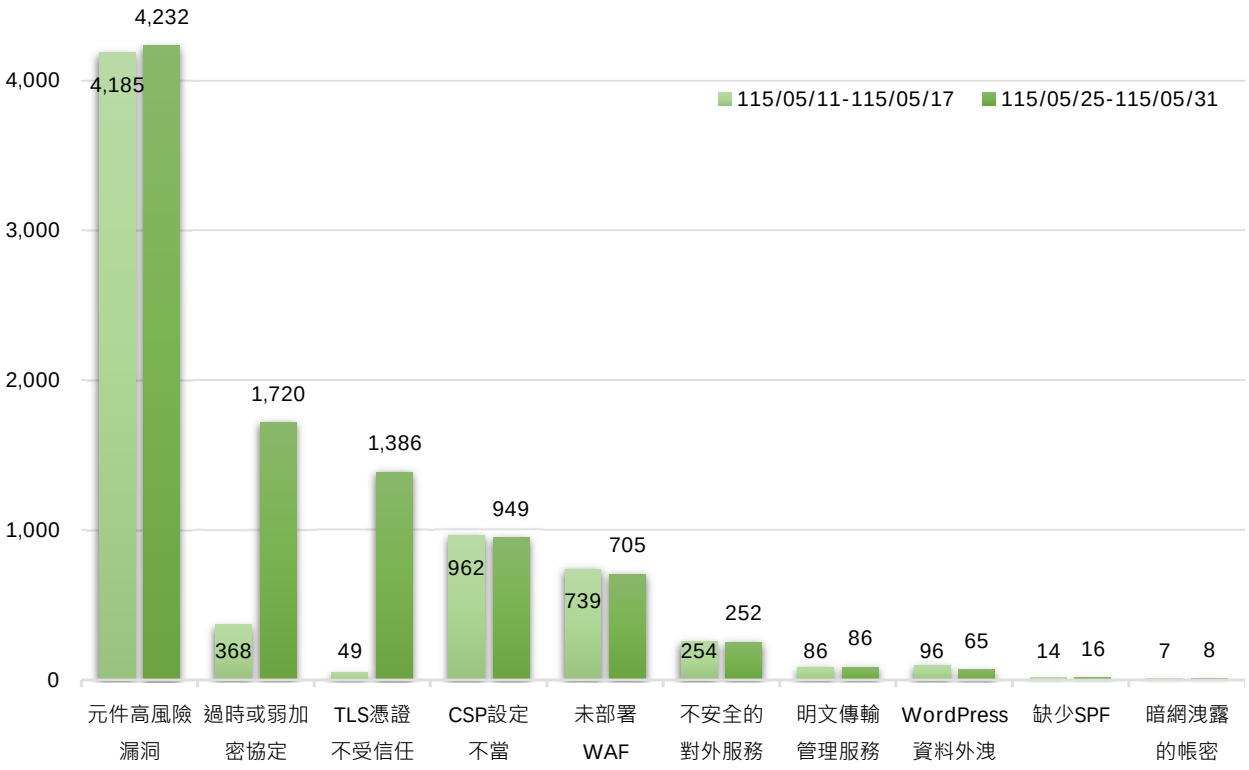

圖5 | EASM檢測結果統計(前10大風險)

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TLS1.2以上版本協定，並停用未加密或舊版加密協定 ➢ 儘速修補已知漏洞，並汰換已停止維護之軟體版本，以降低元件層級曝險風險 ➢ 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)進行存取	➢ 定期盤點並更換外洩帳號憑證，並搭配多因素驗證(MFA)，以強化存取安全 ➢ 建立弱點修補、複測與追蹤機制，確認修補後風險已確實排除 ➢ 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

實兵演練揭露驗證機制未落實密碼強度要求 致帳號遭未授權存取風險

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5/29止已累計73筆攻擊紀錄，本週新增弱點數量共11筆，分別為「驗證機制失效」4筆、「注入攻擊」3筆、「軟體供應鏈失效」2筆、「不安全的組態設定」1筆及「無效的存取控管」1筆，詳見圖6。

本週演練發現，部分系統之驗證機制未落實密碼強度要求，仍存在使用預設帳號或常見弱密碼情形，例如 admin/admin、admin/1234、guest/guest 等常見組合。攻擊者透過帳號密碼猜測方式即可成功登入，顯示驗證防護強度不足。由於此類帳號密碼組合容易被猜測成功，使驗證機制未能發揮應有之防護效果。攻擊者一旦取得登入權限，即可存取後台功能或系統資源，並進一步上傳含有惡意語法之檔案，執行注入攻擊，成功執行惡意腳本。

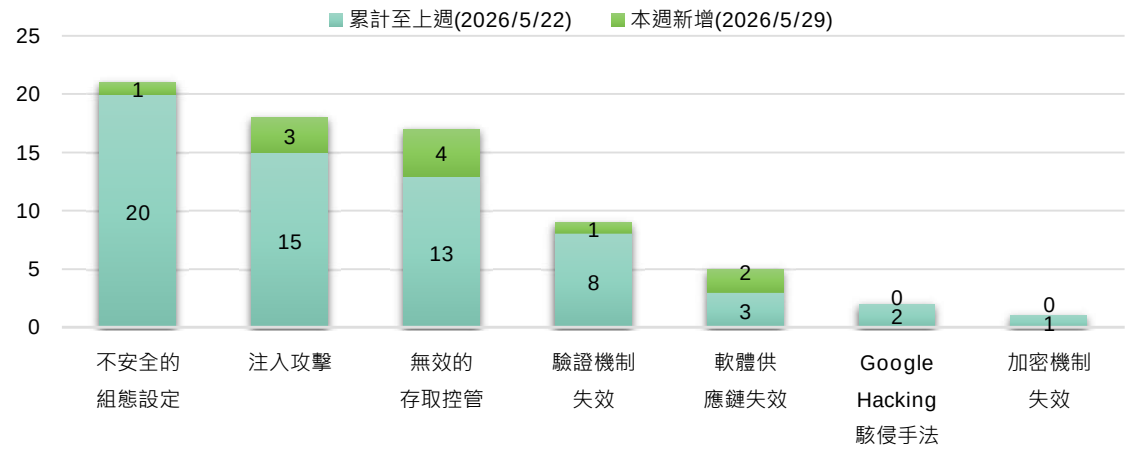

圖6 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應禁止使用預設帳號或常見弱通行碼(如 admin/admin、admin/1234、guest/guest 等)，並強制建立高強度密碼規則
- 限制登入失敗次數並啟用帳號鎖定機制，以降低暴力破解風險
- 建議導入多因素驗證(MFA)，避免僅依賴帳號密碼作為單一驗證機制
- 定期進行帳號盤點，移除或停用預設帳號與閒置帳號，減少受駭機會
- 針對 PDF 檔案應避免直接於瀏覽器中開啟，並停用PDF內嵌JavaScript等主動內容執行功能，以降低惡意程式碼執行風險

■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

詐騙話術結合信任包裝與優惠誘因 降低民眾戒心導流交易

本週高風險詐騙關鍵字分析

本週高風險詐騙訊息不只是單純販售商品，而是更明顯呈現「先吸引互動、再導入私下交易」的操作模式。從高頻關鍵字來看，「推薦」、「私訊」、「優惠」、「必備」位居前列，搭配廣告內容中常見的「截圖私訊另有優惠」、「加賴下訂有折價」、「留言 +1 拿連結」、「點擊購買」等說法，可看出詐騙訊息常先用推薦、優惠或熱銷話術建立興趣，再把民眾導往 LINE、私訊、表單或不明連結，進一步蒐集個資、財務資料或推動付款。

從「推薦」到「私訊」：先建立信任，再轉入私下流程

本週「推薦」與「私訊」同時高頻出現，相關廣告常以「閨妹推薦」、「多人推薦」等方式建立信任，再用「私訊了解」、「截圖私訊另有優惠」、「加 LINE 下訂」等話術，把民眾導向私人通訊管道。提醒民眾，凡價格、下單或付款資訊都需透過私訊、LINE 或表單取得者，應提高警覺，避免在缺乏平台保障下提供個資或付款。

「零元、免費、無經驗」降低戒心，後續才是風險重點

本週也可見「零元交車」、「全額貸」、「免費補發」、「全額退費」、「在家工作」、「無經驗可」等低門檻話術，先讓民眾覺得風險低、容易參與。但後續可能要求填寫表單、提供身分證件、帳戶、財力資料，或先繳訂金、手續費、保證金。提醒民眾，凡以免費、零元、保證、退費吸引接觸，卻要求提供個資或先付款者，應先暫停操作並查證。

把生活痛點包裝成「立即解方」，是本週常見吸引點

本週廣告大量鎖定蚊蟲、悶熱、久坐不適、代謝、喉嚨乾癢、血壓、血脂、腰酸背痛等日常痛點，再以「必備」、「神器」、「有感」、「效果」、「穩定」等字眼，宣稱可快速改善。提醒民眾，凡把健康、身體、生活或財務問題包裝成「一用就有效」、「馬上改善」、「不用治療」的簡單解方，都應審慎查證，不宜只憑廣告或留言就下單。

「台灣、日本、醫用級、專利」是本週常見可信度包裝

本週也常見「台灣研發製造」、「日本原裝進口」、「醫用級」、「專利配方」、「官方認證」等說法，用來營造來源清楚、品質可靠的印象。但若賣場缺乏公司資訊、產品標示、合法許可、檢驗文件或退換貨規範，仍可能涉及假賣場、假認證或誇大療效。提醒民

眾，看到進口、專利、醫用級、正品保證等字眼時，仍應透過官方網站、合法通路及公開客服查證。

本週防詐提醒

1. 「推薦」後接「私訊」是本週重要風險訊號。凡廣告要求私訊、加 LINE、填表單才能報價、下單或取得優惠者，應先查證商家身分與交易保障。
2. 「零元交車」、「全額貸」、「免費補發」、「無經驗可」、「全額退費」等低門檻話術，不代表沒有風險；若後續要求提供身分證件、帳戶、財力資料或先付款，應立即提高警覺。
3. 保健與身體相關商品若宣稱「一喝有感」、「快速改善」、「醫用級」、「專利配方」、「日本進口」、「調理血脂」等，應查證產品標示、合法來源及是否涉及誇大療效。
4. 夏季商品、居家用品或服飾若搭配「必備」、「神器」、「限時」、「搶完即止」、「留言 +1 拿連結」等話術，並導向短網址或不明賣場，應先確認網站及付款方式是否安全。
5. 精品、翡翠、樹苗、車貸、兼職等內容若採私訊成交、私下匯款，或缺乏清楚契約、鑑定、退換貨及售後機制，應避免倉促交易。

圖7 | 詐騙關鍵字文字雲

綜合觀察

綜合本週資料觀察，詐騙訊息已不只是單純以商品功能吸引購買，而是透過「推薦」建立信任、「優惠」製造動機、「必備」放大需求，再以「私訊」或「點擊連結」完成導流。其間搭配「台灣」、「日本」、「醫用級」、「專利」、「安心」等字眼包裝可信度，並利用「免費」、「零元」、「無經驗」、「快速有感」降低民眾戒心。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，均應先停下來查證，避免落入詐騙陷阱，詳見圖7。

焦點文章

利用合法工具AutoIt的攻擊鏈情資分享

以近期某機關執行檢測時，發現AutoIt惡意攻擊事件為例，解析駭客如何濫用合法工具規避偵測，並透過鍵盤側錄木馬竊取使用者敏感資訊

利用合法工具AutoIt的攻擊鏈情資分享

近期發現駭客利用AutoIt執行惡意腳本之攻擊案例，此事件係利用AutoIt合法工具特性，規避資安防護軟體之規則與偵測，最終目的在於電腦中潛伏執行鍵盤側錄木馬程式，以竊取使用者之敏感資訊。

從自動化工具到惡意載體：AutoIt 的雙面性

AutoIt是一款合法且免費的Windows腳本工具，原本設計用途係為系統操作與自動化模組，可模擬鍵盤輸入、滑鼠操作，以及控制視窗與程式介面等多項功能。由於AutoIt語法相對簡單、內建功能完整，因此受到許多系統管理員與資訊(IT)人員青睞，常被用於日常維運與自動化管理工作。然而，正因其具備高度自動化能力及執行彈性，近年亦逐漸成為駭客用來規避偵測與執行惡意程式的重要工具。

目前觀察到除本事件以外，不少資安事件中的惡意程式都有利用AutoIt提升惡意程式之隱蔽性與規避能力，實際案例包含遠端控制木馬（RAT）DarkGate、DarkCloud Stealer、Lumma Stealer等惡意程式。

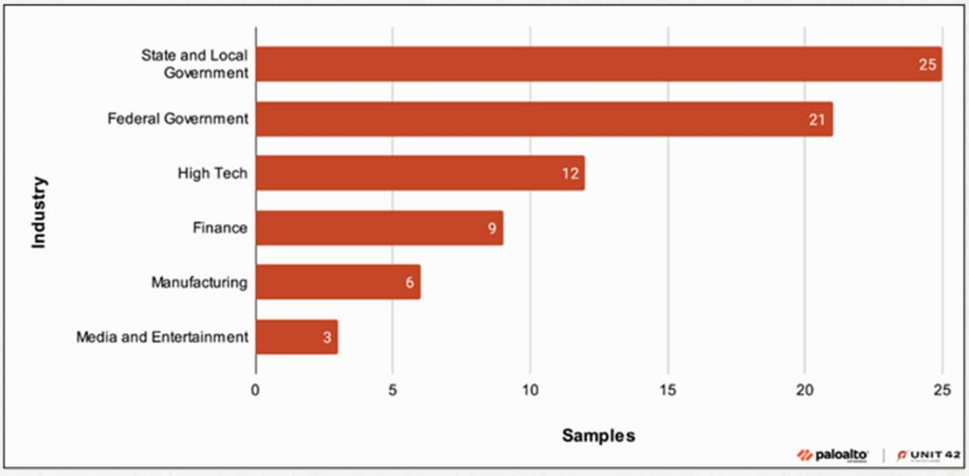

圖8 | DarkCloud Stealer 的新變種，在各產業中發現的樣本

以DarkCloud Stealer為例，網路安全公司Palo Alto Networks旗下威脅情報小組Unit 42報告中顯示各受影響產業中，觀察到之新型AutoIt型態[1]。自DarkCloud樣本數量，可看到第一

焦點文章

與第二名分別是地方政府與中央政府，其數量遠大於其他產業別，這是各政府機構須特別關注，詳見圖8。

攻擊手法

此類型之攻擊手法通常以釣魚郵件作為入侵的起始點，透過偽冒PDF檔誘使電腦使用者點擊後，植入AutoIt及經混淆加密之惡意檔案(payload)。在執行AutoIt後載入惡意檔案(payload)，可成功規避資安防護軟體偵測，進行鍵盤側錄竊取使用者敏感資訊後，再連回中繼站，詳見圖9。

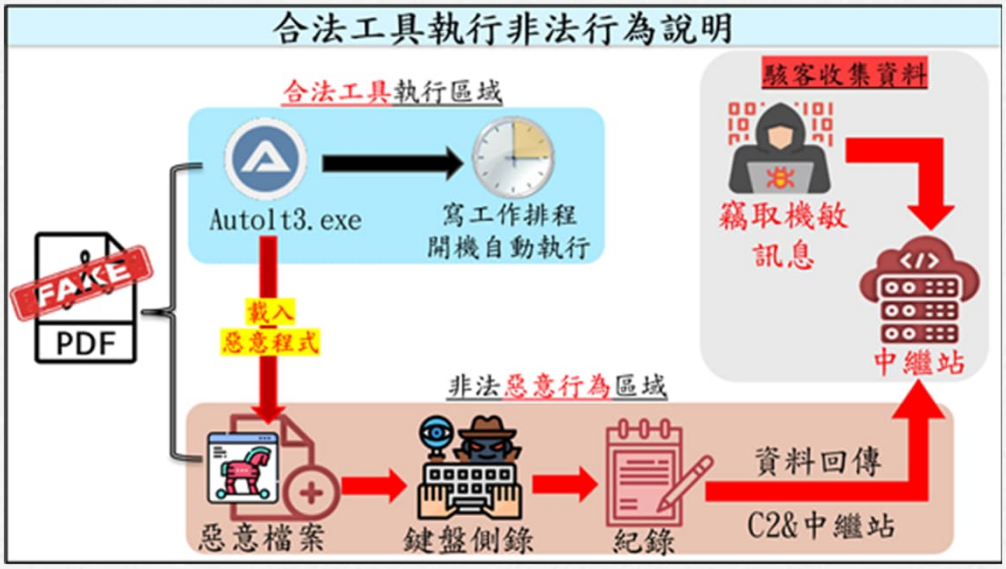

圖9 |本次攻擊事件的流程圖

駭客偏好使用AutoIt之三個主要原因：

1. 容易躲避偵測

於所發現之事件中，攻擊者利用執行正常AutoIt程式後，載入惡意檔案(payload)以隱藏自身惡意行為。傳統防毒軟體主要依靠病毒特徵碼（Signature）偵測隔離，而不是行為分析或威脅情境判斷，就更容易漏掉這類惡意活動。

2. 上手門檻低

該工具毋需具備撰寫程式的高階能力。AutoIt提供相對簡單直覺的語法，並內建大量

焦點文章

Windows自動化功能，因此，即使撰寫程式能力有限，也能快速完成鍵盤側錄、視窗操作、檔案控制或自動化流程等功能。

3. 開發速度快

AutoIt不只容易寫，也讓惡意程式之開發與更新變得更有效率。攻擊者可以利用AutoIt之模組化設計，重複使用既有程式碼，不需要每次都從頭開發。當資安防護軟體更新偵測規則後，攻擊者也能快速修改AutoIt腳本、調整規避技巧，再重新編譯成新版惡意程式。

對惡意軟體開發者來說，這種「好改、好維護、更新快」之特性，可大幅縮短開發與更新版本時間。原本這些功能是設計提供系統管理員或開發人員做合法自動化使用，但同樣也讓技術能力沒那麼高的攻擊者，更容易開發或修改惡意程式，進一步擴大潛伏在攻擊事件中之數量。

防範作為

一、因釣魚郵件係成本低廉且效果顯著之資安攻擊手法，所以諸多的攻擊常以釣魚郵件作為入侵之初始點。釣魚郵件防範我們應該要做到下列3點：

1. 加強使用者資安意識教育
   定期辦理資安宣導與社交工程演練，提升人員辨識釣魚郵件、惡意附件及可疑連結之能力。
2. 確認寄件者與郵件內容真實性
   收到郵件時應確認寄件者網域、郵件內容及附件來源，對異常或不明郵件提高警覺。
3. 避免開啟不明附件與連結
   不任意點擊郵件中之超連結或開啟未知附件。

二、以本次攻擊事件為例，如果整個組織架構下都不會使用到AutoIt進行開發或維運，那麼可以合理地假設，所有的AutoIt程序(process)都是不必要的，故可將其加入資安防護軟體黑名單中。

參考文獻

1. https://unit42.paloaltonetworks.com/darkcloud-stealer-and-obfuscated-autoit-scripting/

關鍵字：釣魚郵件、規避偵測、竊取敏感資訊

刊　　名　資安週報第 47 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