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

建議持續強化資安管理能力 逐步由預設信任轉向最小權限與行為可追溯之機制

聯防監控

防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕

通用型Web介面攻擊增加

外部曝險分析

整體風險數量下降9.8% 惟元件高風險漏洞增加

網路巡查高風險詐騙

高風險內容持續包裝成日常購物資訊 近期須留意穿搭、保健與售後流程混用情形

焦點文章

帳號外洩的真正原因？認識持續活躍的資訊竊取程式

2026.04.16
040

資安儀表板

事件通報、聯防監控、蜜罐誘捕、外部曝險分析及網路巡查高風險詐騙等五類量化指標

■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

建議持續強化資安管理能力 逐步由預設信任轉向最小權限與行為可追溯之機制

本週總計接獲4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。本週通報案件均涉及個人電腦遭惡意程式感染，包含安裝來源不明之軟體，或透過 USB 裝置進行惡意程式傳播，並由共用設備(如會議室電腦)擴散至其他個人電腦。相關事件多非利用系統漏洞，而係透過使用行為與設備使用情境形成入侵機會，且因來源不明與設備共用等因素，常導致事件來源難以追溯，增加釐清與應變之困難。

針對此類風險，關鍵在於補強終端設備之信任邊界與可視性，避免透過不明軟體或USB裝置帶入未經控管之程式或內容，造成防護機制失效。治理上應由「預設信任」轉向「最小權限與可追溯性」，並透過技術與管理並行強化控管，包括限制非授權軟體安裝(應用程式白名單)、加強USB使用控管、納管共用設備並落實使用限制；同時導入端點偵測(EDR)與集中式日誌機制，以提升行為監控與事件追溯能力，降低非漏洞型入侵風險。

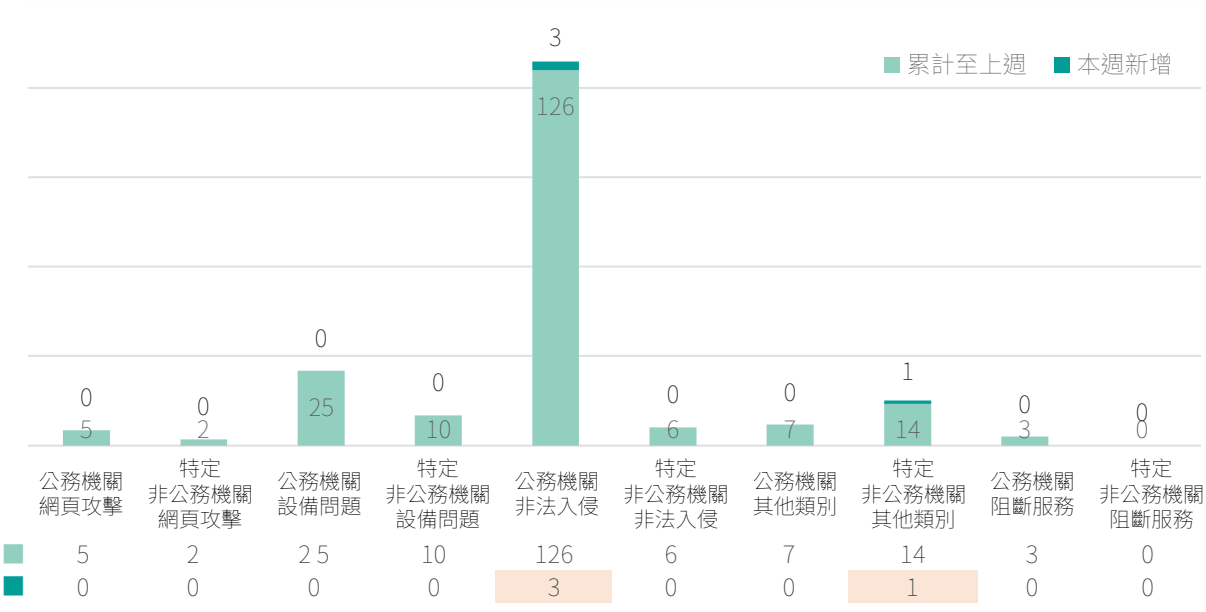

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

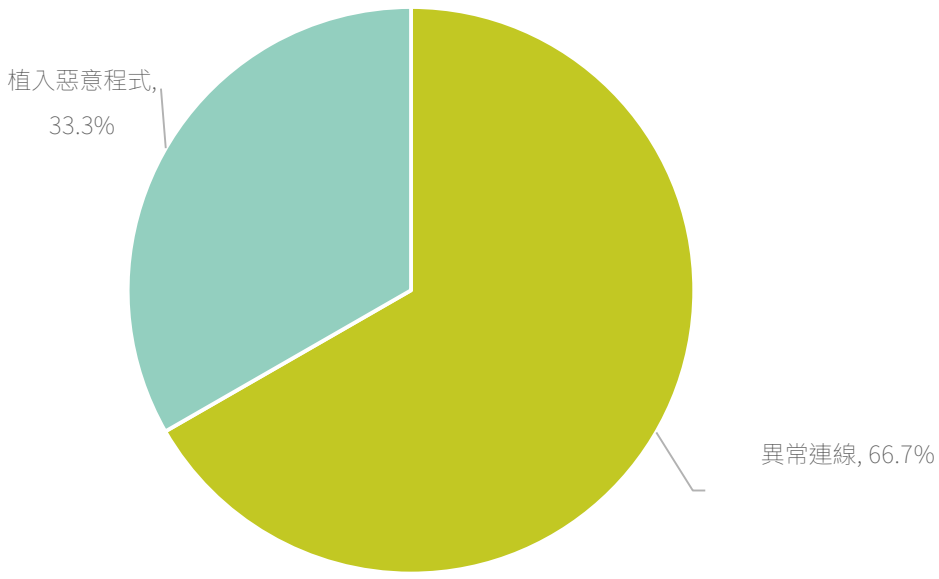

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 惡意程式透過USB裝置擴散感染多台電腦 ➢ 安裝不明軟體導致後門程式長期潛伏	➢ 建立應用程式白名單機制，限制未授權軟體安裝與執行行為 ➢ 強化USB裝置使用控管機制，避免未經授權設備連接主機 ➢ 導入端點偵測與回應機制，即時掌握異常行為與感染狀況 ➢ 納管共用設備使用規範，落實帳號控管與操作行為紀錄機制

5間民間企業揭露重大資安訊息

本週5家民間企業發布重大訊息，產業類別分為生技醫療業、鋼鐵工業、其他電子業、半導體業及觀光餐旅業。

■ 公司名稱	健喬信元醫藥生技股份有限公司
■ 發布時間	115年4月7日
■ 事件說明	健喬公司資訊系統偵測異常後，立即啟動資安應變機制及系統復原程序，進行系統隔離與清查；相關資料已陸續恢復中，同時委請外部資安專業機構與技術專家協助調查及處理。經評估後，本事件對公司營運無重大影響，後續將持續密切監控，全面性檢視系統安全，加強系統的監控與防護，強化資安保護及資訊安全，提升整體資訊安全管理，以降低類似事件發生之風險。
■ 公司名稱	豐達科技股份有限公司
■ 發布時間	115年4月8日
■ 事件說明	豐達科公司部分資訊系統遭受駭客網路攻擊時，立即啟動相關防禦機制。目前評估尚無個資、機密或重要文件資料外洩等情事發生，對公司營運無重大影響。後續將持續檢視與強化提升網路與資訊基礎架構之安全控管，以確保資料安全與完整性。
■ 公司名稱	弘塑科技股份有限公司
■ 發布時間	115年4月10日
■ 事件說明	弘塑公司資訊系統遭受勒索病毒攻擊，於第一時間偵測到資訊系統異常情形，已立即啟動資安應變機制，包括系統隔離、防護強化及資料復原作業，目前仍持續搶救中。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，並導入更完善資安控管措施，以降低未來風險。
■ 公司名稱	政美應用股份有限公司
■ 發布時間	115年4月12日
■ 事件說明	政美應用公司資訊系統遭受勒索病毒攻擊，已立即啟動資安應變機制，包括系統隔離、防護強化及資料復原作業，目前仍持續搶救中。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。

5間民間企業揭露重大資安訊息

本週5家民間企業發布重大訊息，產業類別分為生技醫療業、鋼鐵工業、其他電子業、半導體業及觀光餐旅業。

■ 公司名稱	饗樂餐飲實業股份有限公司
■ 發布時間	115年4月12日
■ 事件說明	Q Burger公司偵測到部分內部資訊系統發生異常，經初步研判為網路攻擊事件，已於第一時間啟動資安應變機制，進行系統隔離及相關防護措施，並委請外部資安專業機構協助進行鑑識分析與復原作業，同時已向主管機關通報並向刑事警察機關報案。本事件影響範圍主要局限於部分行政系統，核心營運相關系統運作正常，故對公司整體營運無重大影響。後續將持續提升網路與資訊基礎架構之安全控管，並持續密切監控，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

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14.6%，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12.9%，為本週占比次高的攻擊階段，顯示攻擊者持續強化對目標環境的前期偵查與情報蒐集行動。觀察到的主要手法包括主動式掃描、IP 區段掃描、以及DNS與被動式 DNS 情資蒐集。攻擊者透過自動化工具大規模掃描外部網段，以識別可存取服務與潛在攻擊入口，並結合被動式 DNS 資料分析，掌握目標組織之網域架構、子網域分佈及歷史解析關聯，進一步描繪完整攻擊面。此類行為融合主動與被動偵查技術，具低互動性與高隱蔽特性，能有效提升後續攻擊的精準度與成功率。建議加強對異常掃描流量的即時監控與阻擋機制，定期盤點對外資產與DNS資訊曝光情形，並結合威脅情資進行來源分析，以提前識別潛在攻擊準備活動。

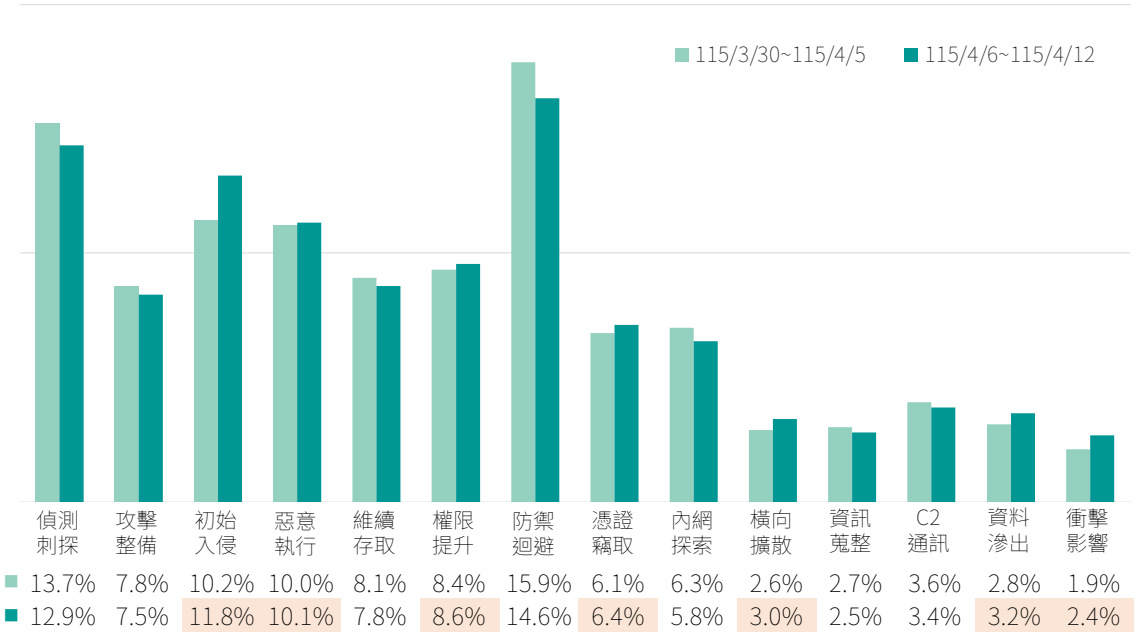

圖3 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

- 強化端點防護（EDR / XDR），監控異常指令與行為鏈
- 啟用並集中管理指令紀錄（如 PowerShell、CMD、Shell logging）
- 防止日誌被刪除或竄改（啟用防竄改機制、集中式 SIEM）
- 限制高風險系統工具使用（如 PowerShell、WMI、PsExec）
- 實施最小權限原則（Least Privilege），降低濫用風險
- 強化特權帳號管理（PAM、MFA、帳號行為監控）

防禦迴避（Defense Evasion）

- 建立異常掃描流量偵測與阻擋機制（IPS / WAF / Firewall）
- 對外服務加上存取控制（IP allowlist / rate limiting）
- 定期盤點與縮減外部攻擊面（開放服務、Port、API）
- 管理與清查 DNS 暴露資訊（子網域、歷史解析紀錄）
- 導入被動 DNS 與威脅情資比對來源可疑性

偵測刺探（Reconnaissance）

■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

通用型Web介面攻擊增加

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74.88%、「遠端控制」服務攻擊占比21.53%，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73.64%。「遠端控制」服務亦有23.06% 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。

而網通設備管理介面比例大幅下降，主因為CVE-2017-17215遠端程式碼執行漏洞相關攻擊次數明顯減少。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。

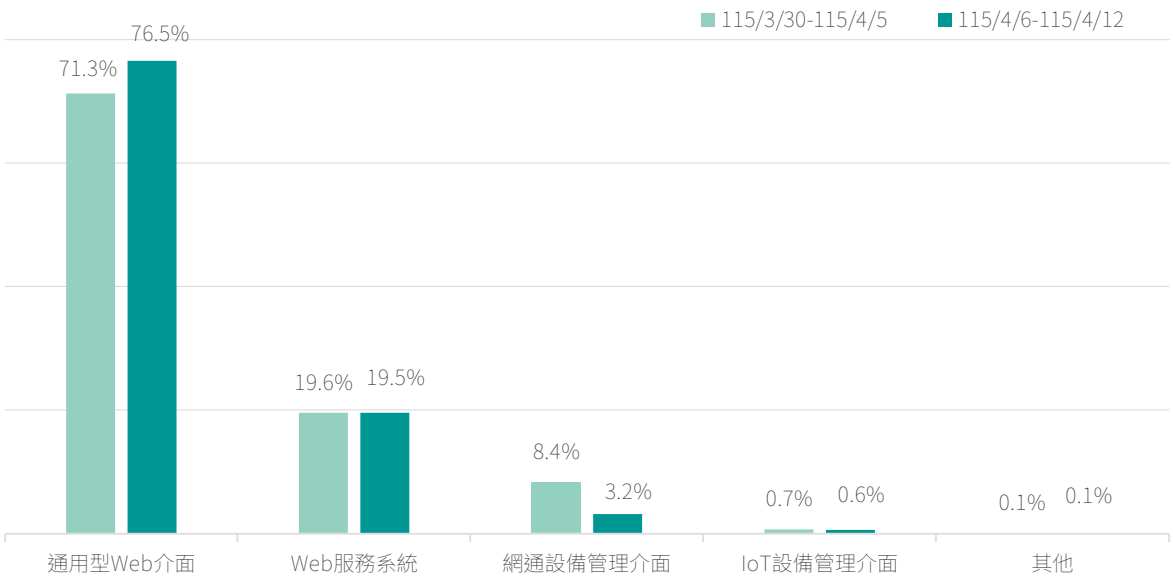

圖4 |本週網頁應用介面之誘捕攻擊比例統計

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1。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越界讀取漏洞、遠端程式碼執行漏洞、目錄遍歷漏洞及程式碼注入漏洞，攻擊目標涵蓋應用程式遞送控制器(ADC)、PHP伺服器端腳本語言、 知識管理與團隊協作系統、VPN Gateway及行動裝置管理系統。

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1 | 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-2025-5777[1]	Citrix NetScaler ADC	7.5
■	2	-	CVE-2024-4577[2]	PHP	9.8
■	3	↑New	CVE-2024-21683[3]	Atlassian Confluence Server	8.8
■	4	↓1	CVE-2024-24919[4]	Check Point VPN Gateway	8.6
■	5	↓1	CVE-2025-4428[5]	Ivanti Endpoint Manager Mobile	7.2

類型 ■越界讀取漏洞 ■遠端程式碼執行漏洞 ■目錄遍歷漏洞 ■程式碼注入漏洞

▶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 Integrated Management Controller存在2項高風險安全漏洞(CVE-2026-20093[6]與CVE-2026-20094[7])，類型分別為身分鑑別繞過(Authentication Bypass)與指令注入(Command Injection)。
  - ✓ CVE-2026-20093可使未經身分鑑別之遠端攻擊者，透過發送特製HTTP請求繞過驗證機制，修改系統任意使用者(含Admin)通行碼，進而以該使用者身分存取系統。
  - ✓ CVE-2026-20094可使通過身分鑑別且僅具唯讀權限之遠端攻擊者，透過發送特製指令，以root權限於受影響系統底層作業系統執行任意指令。
- Cisco Smart Software Manager On-Prem存在高風險安全漏洞(CVE-2026-20160[8])，類型為執行任意程式碼(RCE)，未經身分鑑別之遠端攻擊者可透過發送特製請求，以root權限於受影響主機上執行任意指令。
- GNU Inetutils Telnetd存在高風險安全漏洞(CVE-2026-32746[9])，類型為緩衝區溢位(Buffer Overflow)，未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼。
- Juniper Networks Support Insights (JSI) Virtual Lightweight Collector (vLWC)與Junos OS MX系列路由器存在高風險安全漏洞(CVE-2026-33784[10]與CVE-2026-33785[11])，類型分別為使用預設密碼(Use of Default Password)與授權檢查不足(Missing Authorization)。
  - ✓ CVE-2026-33784由於系統未強制變更高權限帳號之預設密碼，可使未經身分鑑別之遠端攻擊者透過使用預設帳密登入系統，進而取得設備完整控制權。
  - ✓ CVE-2026-33785於採用Connected Security Distributed Services (CSDS)之MX路由器，因具備Juniper Device Manager (JDM)套件，可使低權限本機端使用者於未授權之情況下執行高權限CLI指令(request csds)，進而影響由該設備所管理之系統與服務。

1. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
2. https://nvd.nist.gov/vuln/detail/cve-2024-4577
3. https://nvd.nist.gov/vuln/detail/cve-2024-21683
4. https://nvd.nist.gov/vuln/detail/cve-2024-24919
5. https://nvd.nist.gov/vuln/detail/cve-2025-4428
6. https://nvd.nist.gov/vuln/detail/CVE-2026-20093
7. https://nvd.nist.gov/vuln/detail/CVE-2026-20094
8. https://nvd.nist.gov/vuln/detail/CVE-2026-20160
9. https://nvd.nist.gov/vuln/detail/CVE-2026-32746
10. https://nvd.nist.gov/vuln/detail/CVE-2026-33784
11. https://nvd.nist.gov/vuln/detail/CVE-2026-33785

■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

整體風險數量下降9.8% 惟元件高風險漏洞增加

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1,849項，詳見圖5。其中，「元件高風險漏洞」以676項居首，「過時或弱加密協定」416項次之，「TLS憑證不受信任」261項位居第三。前三項合計1,353項，占前10大風險項目總數約73.2%，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。相較上期2,049項，整體風險數量減少200項，降幅約9.8%，顯示相關機關於接獲警訊通知後，已陸續採取改善措施，整體曝險情勢已有所改善。

進一步分析主要風險變化情形，「元件高風險漏洞」由630項增至676項，增加46項，增幅約7.3%；「TLS憑證不受信任」由376項降至261項，減少115項，降幅約30.6%；「過時或弱加密協定」由532項降至416項，減少116項，降幅約21.8%；「CSP設定不當」由240項微降至238項，減少2項，降幅約0.8%；「未部署 WAF」由136項微降至129項，減少7項，降幅約5.1%。整體而言，除元件高風險漏洞增加外，其餘主要風險項目多呈下降趨勢，惟部分對外網站在WAF部署及應用層攻擊防護方面仍有待強化。

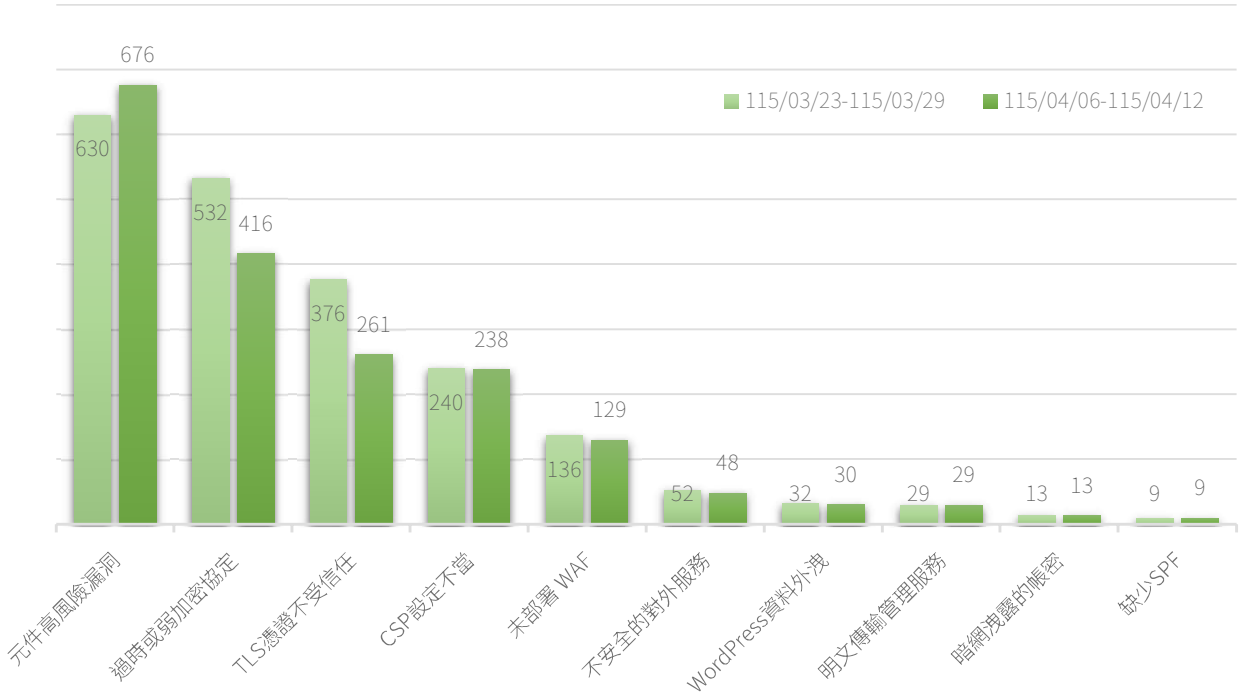

圖5 | EASM檢測結果統計(前10大風險)

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，停用未加密或舊版加密協定 ➢ 儘速完成已知漏洞修補，並汰換已停止維護或不再支援之軟體版本 ➢ 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 ➢ 關閉非必要對外服務；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)進行管理	➢ 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、驗證及追蹤機制，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、加密設定及服務配置之安全意識

■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

高風險內容持續包裝成日常購物資訊 近期須留意穿搭、保健與售後流程混用情形

綜整本週資料觀察，高風險詐騙內容的整體結構並無明顯改變，仍以「產品服務」類型為主，明顯高於「身分冒充」與「金融投資」等其他類型，詳見圖6。顯示近期高風險內容仍持續混入一般消費、購物與生活資訊之中，並以貼近日常需求的商品題材作為主要包裝外觀。

從本期關鍵字分布來看，高頻詞集中於「必備、設計、神器、配方、台灣、推薦、優惠、安心、問題、效果」等字眼，呈現出明顯的商品行銷語境，詳見圖7。相關內容多以穿搭服飾、草本保健、護理矯姿、居家用品、廚房器具、汽機車周邊、農用工具等題材出現，並搭配「台灣設計」「日本推薦」「草本配方」「現貨供應」「快速有感」「限量補貨」等說法，強化產品可信度與即時下單氛圍，使高風險訊息外觀更接近一般促銷貼文。

另從風險類型交錯情形觀察，「身分冒充」雖非表面主題，但仍常出現在後續互動或交易流程中，例如以客服、賣家、貸款窗口、物流通知或售後協助等名義銜接，將原本看似單純的商品訊息延伸為私訊聯繫、點擊連結、填寫表單或轉往站外洽談等行為；「金融投資」類型雖非本期主軸，但仍可見貸款、債務整合、手機貸款與分期條件等金融性話術穿插在消費情境中，增加辨識上的模糊性。

整體而言，本期高風險內容仍以「商品型包裝」為核心樣態，並持續與售前促銷、售後客服、貸款諮詢及交易導流機制結合。詐騙訊息不再只以明顯異常的形式出現，而是更頻繁地嵌入日常購物語境，透過商品描述、效果宣稱、優惠語句與客服話術逐步降低民眾戒心，風險辨識門檻持續提高。

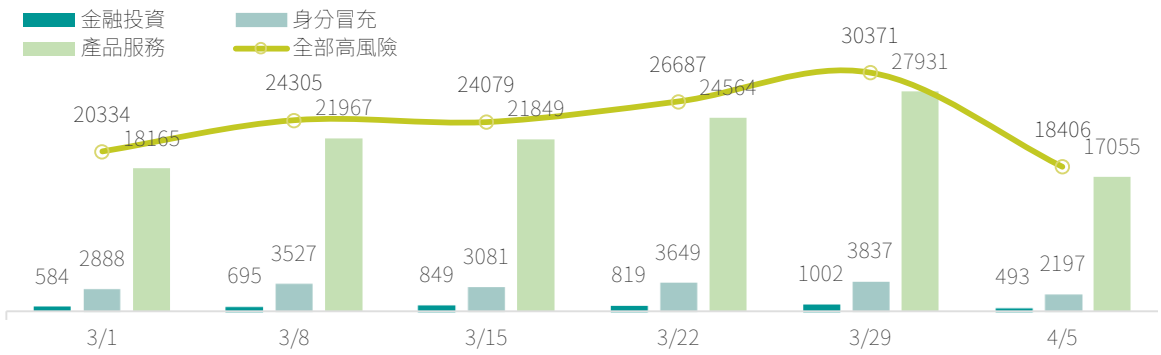

圖6 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙週趨勢

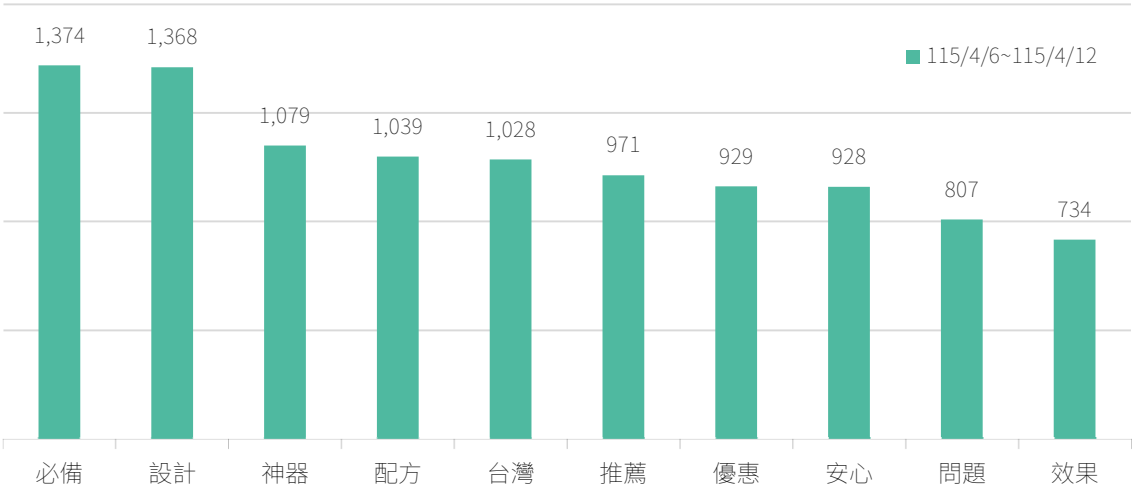

圖7 | 本週代表性詐騙關鍵字 Top 10

近期高風險手法辨識重點

商品型包裝仍為主要外觀，且題材更貼近日常生活需求

本期高風險內容多以服飾穿搭、保健護理、居家廚房、汽車周邊與農用工具等日常商品作為主要切入點，常見表述聚焦於實用性、舒適度、外觀設計、產地來源與使用效果。此類內容與一般電商促銷貼文高度相似，表面上多為商品介紹，實際上則可能進一步導向其他高風險互動行為。

效果宣稱與專業背書並行，形成較強的真實感包裝

從「配方、安心、健康、調理、提升、有感、品質」等關鍵字可見，本期不少內容結合健康改善、草本修護、專業推薦、檢驗認證或在地／進口來源等元素，透過功能性敘述與背書語言增加說服力。此類手法常見於保健護理、矯姿用品與個人保養題材，容易讓高風險內容看起來更像一般商品宣傳或口碑分享。

私訊、點擊與站外洽談仍是高風險轉折點

本期關鍵字中「私訊」「點擊」「限時」「優惠」持續居前，顯示高風險內容仍高度依賴導流式操作。前段多以促銷、清倉、限量、福利價等語句吸引注意，後段再銜接私訊詢價、表單填寫、外部連結、貸款諮詢或客服聯繫，使風險並非完全顯現在貼文本身，而是逐步出現在後續互動與交易流程之中。

焦點文章

帳號外洩的真正原因？認識持續活躍的資訊竊取程式

什麼是資訊竊取程式

資訊竊取程式（Infostealer）為專門用來竊取使用者資料之惡意程式。當使用者下載並執行惡意檔案後，程式會自電腦中竊取瀏覽器儲存之帳號密碼、Cookies、信用卡資料或加密貨幣錢包等資訊，並利用於個資販賣或詐騙等犯罪活動。研究顯示全球因資訊竊取程式外洩之帳密數量正快速增加，已成為近年最常見之網路威脅。

常見攻擊流程

攻擊者經常偽冒軟體下載網站、破解程式或透過惡意廣告散播，誘導使用者下載被惡意汙染之檔案程式，一旦於電腦端執行後，即觸發資訊竊取程式蒐集瀏覽器與系統之帳密或個人機敏資料，被竊取之資料通常會被整理成「stealer logs」，並傳送到由攻擊者控制之伺服器。攻擊者會將竊取資料透過地下論壇進行販售，成為後續帳號盜用、詐騙甚至勒索攻擊之來源。

常見之資訊竊取程式

- Lumma Stealer

  Lumma Stealer為近年成長最快之資訊竊取惡意程式之一，採用「Malware-as-a-Service」模式，攻擊者只需付費就能使用。主要鎖定Windows作業系統之個人電腦，竊取瀏覽器帳密、加密貨幣錢包與各種登入憑證。114年Microsoft跨國聯合執法機構及資安業者，關閉約2300個相關網域並試圖阻止其運作，惟該惡意程式仍持續遭犯罪集團使用。研究人員指出，Lumma於114年短短兩個月內感染了約39萬台Windows電腦，其擴散速度相當驚人。

- RedLine Stealer

  RedLine Stealer為近年廣為人知之資訊竊取程式之一，最早於109年被發現。同樣以「Malware-as-a-Service」模式在地下論壇販售，因此攻擊門檻相對較低。RedLine能竊取瀏覽器密碼、Autofill資料、FTP帳密及加密貨幣錢包資訊等。112年曾被發現以ChatGPT、Google Bard安裝程式為誘餌進行散布。

焦點文章

■ Vidar Stealer

Vidar為另一個長期活躍之資訊竊取程式，具模組化架構，除了竊取瀏覽器資料與系統資訊外，也能下載其他惡意程式。114年10月出現 Vidar 2.0，據稱其效能、躲避偵測及整體功能皆有提升。近年研究人員發現，攻擊者利用搜尋引擎優化（SEO）操作讓惡意網站於搜尋結果中排名靠前，當使用者下載看似正常之AI工具或軟體時，實際上安裝了Vidar資訊竊取程式。

我國受害情形

資安院觀測外部資安情資，自114年1月初至115年2月底統計臺灣有2,569台主機受到資訊竊取程式感染，主要為Lumma與其變種程式，顯示資訊竊取程式仍潛伏在不被注意到的環境中，持續洩漏機敏或個人資訊，國人應多加注意與防範，詳見圖8。

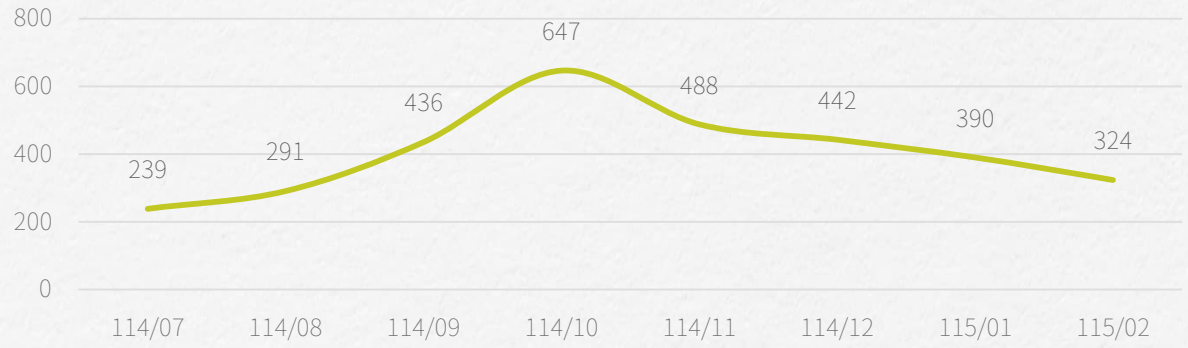

圖8 |遭資訊竊取程式感染之主機數量(單月統計)

如何防範

為降低資訊竊取程式感染風險，建議使用者落實資安防護意識：

- 避免下載破解軟體或來源不明之應用程式
- 判讀網路搜尋引擎所提供之查詢結果，識別關鍵字廣告或偽冒網站
- 優先透過官方網站取得軟體

此外，為重要帳號或網路服務啟用多因子驗證（MFA）、定期更換密碼並檢查帳號登入紀錄，也能有效降低帳密被盜用的風險。養成良好下載習慣與保護帳號安全，是防範資訊竊取程式最有效之方法。

焦點文章

引用資料

1. Microsoft Digital Defense Report 2025, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf
2. 快速、廣泛、難以偵測：Vidar Stealer 2.0 資訊竊取程式做了哪些升級，https://www.trendmicro.com/zh_tw/research/25/j/how-vidar-stealer-2-upgrades-infostealer-capabilities.html
3. Vidar 竊資軟體：更深入的了解，https://www.kaspersky.com.tw/resource-center/threats/vidar-stealer

關鍵字：資訊竊取程式、Infostealer、Lumma、RedLine、Vidar

刊　　名　資安週報第 40 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