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

資安週報

Cyber Security Weekly Newsletter

2026.03.05

034

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

防範偽冒軟體風險 應以必要性與可信來源為原則 強化軟體安裝安全

本週總計接獲10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。近期觀察到偽冒軟體散布手法出現變化，除過往以偽冒通訊軟體為主外，攻擊者開始利用遊戲平台及官方模擬器名義散播惡意程式。攻擊者透過仿冒下載網站或偽裝合法安裝程式，誘使使用者下載執行，進而於端點設備植入惡意程式，並建立後續之遠端控制通道。

鑑於攻擊者偽冒軟體手法持續演變，端點防護除惡意程式偵測外，亦應涵蓋軟體下載與安裝行為控管；技術面建議限制來源不明程式執行並強化新安裝程式與異常連線監控，管理面上，應明確規範公務設備僅限安裝業務必要軟體，避免於公務設備安裝非業務用途之應用程式，以降低惡意程式透過偽冒軟體進入機關環境之風險。

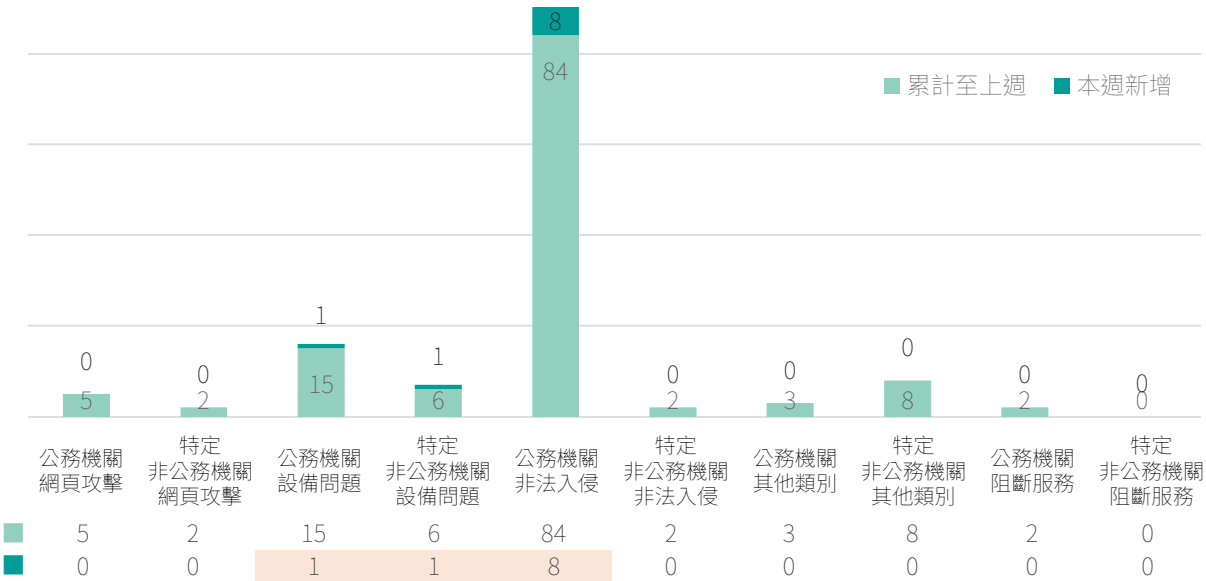

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

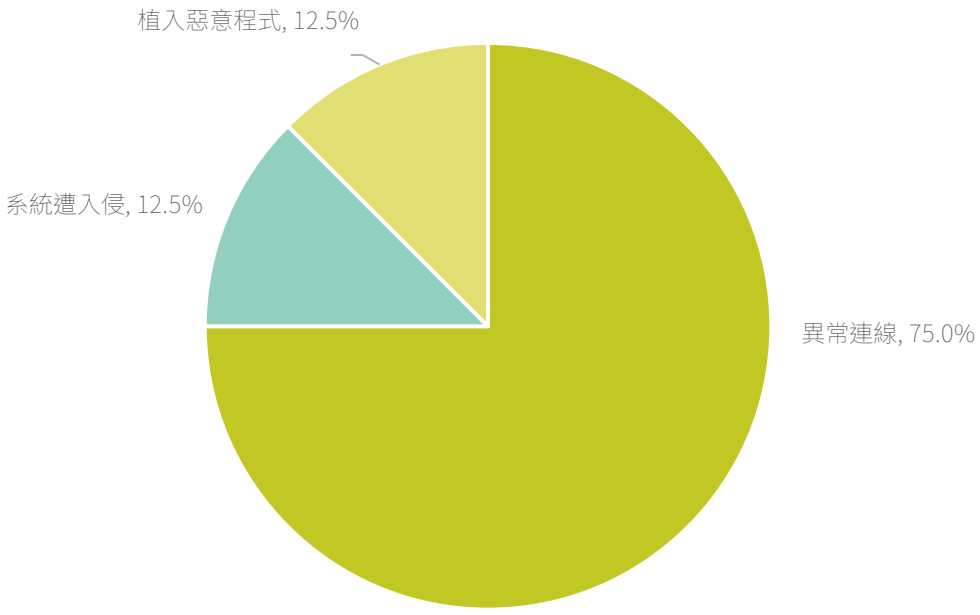

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 留意偽冒官方軟體名義誘導下載與安裝之資安風險 ➢ 警覺惡意程式植入後建立遠端控制通道之威脅	➢ 建立來源驗證機制限制未知程式執行 ➢ 強化新安裝軟體與異常行為監控機制 ➢ 落實端點對外異常連線即時告警機制 ➢ 建立公務設備軟體安裝白名單制度

◎本週無企業發布資通安全事件重大訊息。

■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

攻擊手法轉向深層滲透! 橫向擴散與C2通訊活動雙雙攀升

本週資安聯防監控顯示，整體攻擊態勢呈現多元化發展趨勢，詳見圖3。與上週相比，「偵測刺探」階段從17.2%下降至14.7%，「攻擊整備」也從13.8%降至11.1%，顯示攻擊者在初期探測階段的活動有所減緩。然而值得關注的是，「防禦迴避」仍維持最高佔比達16.2%，攻擊者持續運用關閉或清除指令紀錄、利用合法工具執行惡意命令等技術來規避偵測。其次為「偵測刺探」與「初始入侵」，後者從9.5%上升至11.3%，顯示攻擊者正積極嘗試突破防線。此外，「惡意執行」佔比11.4%位居第三，反映出成功入侵後的惡意程式執行活動頻繁。

特別需要留意的是「橫向擴散」從1.47%增加至2.44%，以及「C2通訊」從1.4%上升至2.6%，這些數據顯示部分攻擊已從初期偵測階段進入更具破壞性的內網滲透與遠端控制階段。整體而言，雖然初期探測活動減少，但攻擊者正朝向更深層的網路滲透發展，組織應提高警覺並強化縱深防禦機制。

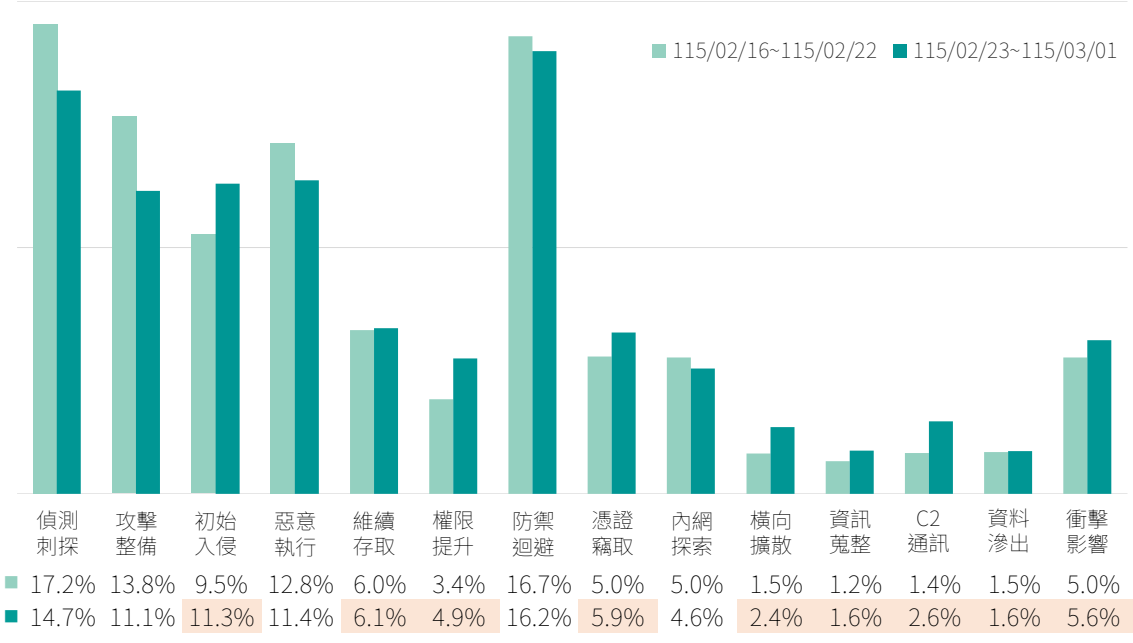

圖3 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

- 強化偵測刺探防護
  - ✓ 導入端點偵測與回應(EDR)解決方案，即時監控異常行為模式
  - ✓ 強化指令紀錄稽核機制，確保所有系統操作留有完整記錄
  - ✓ 限制高風險工具的使用權限，防止合法工具遭濫用執行惡意命令
  - ✓ 落實特權帳號管理，定期審查並限縮管理權限範圍
- 加強初始入侵防護
  - ✓ 定期更新系統與應用程式修補程式，減少可利用的漏洞
  - ✓ 實施多因素驗證機制，提高帳號安全性
  - ✓ 強化電子郵件安全閘道，過濾釣魚郵件與惡意附件
- 監控橫向擴散與C2通訊
  - ✓ 部署網路流量分析工具，偵測異常的內網通訊行為
  - ✓ 實施網路區隔，限制不同網段間的橫向移動
  - ✓ 建立威脅情資整合機制，即時阻擋已知的C2伺服器連線

■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

Citrix NetScaler ADC與Cisco IOS XE網通設備作業系統成攻擊熱點

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59.26%、「遠端控制」服務攻擊占比35.40%，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66.74%。「遠端控制」服務亦有28.96% 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下降主因為NETGEAR RAX43路由器命令注入漏洞的CVE-2021-20167，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。

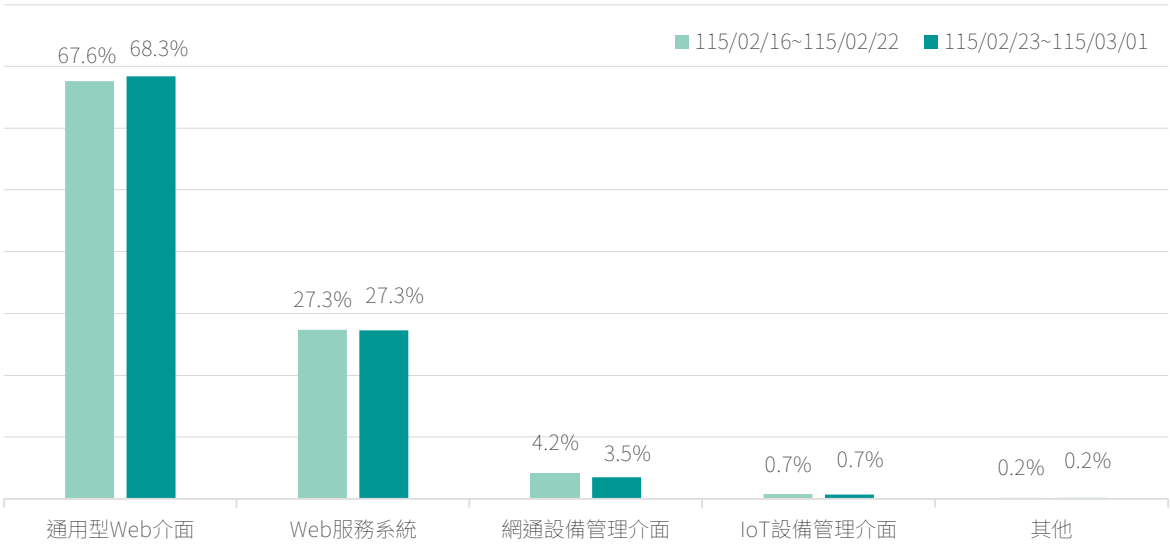

圖4 | 本週網頁應用服務之誘捕攻擊比例統計

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、特權提升、程式碼注入、遠端程式碼執行及身分驗證繞過漏洞漏洞，攻擊目標涵蓋Citrix NetScaler ADC、Cisco IOS XE網通設備作業系統、GeoServer開放源碼伺服器、PHP及ConnectWise ScreenConnect，顯示此類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-2023-20198[2]	Cisco IOS XE網通設備作業系統	10
■	3	-	CVE-2024-36401[3]	GeoServer開放源碼伺服器	9.8
■	4	-	CVE-2024-4577[4]	PHP	9.8
■	5	↑New	CVE-2024-1709[5]	ConnectWise ScreenConnect	10

類型 ■越界讀取漏洞 ■特權提升 ■程式碼注入 ■遠端程式碼執行漏洞 ■身分驗證繞過漏洞

▶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：

- Google Chrome、Microsoft Edge、Vivaldi、Brave及Opera等以Chromium為基礎之瀏覽器存在高風險安全漏洞(CVE-2026-2441[6])，類型為使用釋放後記憶體(Use After Free)，未經身分鑑別之遠端攻擊者可利用特製HTML頁面觸發記憶體錯誤，進而於瀏覽器沙箱環境執行任意程式碼。
- Cisco Catalyst SD-WAN存在高風險安全漏洞(CVE-2026-20127[7]與CVE-2026-20129[8])，類型為身分鑑別繞過(Authentication Bypass)，前者因對等連線(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，取得高權限帳號；後者因API使用者驗證機制不當，致使未經身分鑑別之遠端攻擊者可透過發送特製請求，以netadmin角色權限執行任意程式碼。
- Microsoft Windows與Office存在5個高風險安全漏洞，類型包含安全功能繞過(Security Feature Bypass)漏洞(CVE-2026-21510[9]、CVE-2026-21513[10]及CVE-2026-21514[11])與本機提權(Local Privilege Escalation)漏洞(CVE-2026-21519[12]與CVE-2026-21533[13])，前者可使未經身分鑑別之攻擊者於使用者互動情境下繞過系統安全機制；後者可使已通過身分鑑別之攻擊者在既有權限基礎上提升權限。

1. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
2. https://nvd.nist.gov/vuln/detail/cve-2023-20198
3. https://nvd.nist.gov/vuln/detail/cve-2024-36401
4. https://nvd.nist.gov/vuln/detail/cve-2024-4577
5. https://nvd.nist.gov/vuln/detail/cve-2024-1709
6. https://nvd.nist.gov/vuln/detail/CVE-2026-2441
7. https://nvd.nist.gov/vuln/detail/CVE-2026-20127
8. https://nvd.nist.gov/vuln/detail/CVE-2026-20129
9. https://nvd.nist.gov/vuln/detail/CVE-2026-21510
10. https://nvd.nist.gov/vuln/detail/CVE-2026-21513
11. https://nvd.nist.gov/vuln/detail/CVE-2026-21514
12. https://nvd.nist.gov/vuln/detail/CVE-2026-21519
13. https://nvd.nist.gov/vuln/detail/CVE-2026-21533

■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

擴大檢測範圍：93個A、B級關鍵基礎設施(CI)之外部曝險分析

本次針對93個A、B級關鍵基礎設施(CI)進行EASM檢測，經統計前10大風險項目累計達2,454項(含重大與高風險)，詳見圖5。檢測結果顯示，「過時或弱加密協定」共計793項，為最主要之資安威脅，顯示多數對外服務仍啟用舊版協定或弱加密套件，增加中間人及降級攻擊風險，恐導致傳輸中之帳密與敏感資料遭攔截或竄改。「元件高風險漏洞」共計622項，反映系統修補管理與版本控管仍有精進空間。若已知漏洞未及時修補，將大幅提高遭惡意利用與入侵之風險。「TLS憑證不受信任」共計596項，顯示憑證效期管理、信任鏈設定及維運流程需持續強化，以免影響服務可信度及連線安全性。

以上三項指標合計佔總風險項目81.9%。整體而言，受測單位在「加密傳輸、漏洞修補及憑證管理」等維運面向仍具改善空間，建議儘速採取修復與強化措施。

防護建議	
加密與憑證管理	系統元件管理
➢ 全面盤點並汰換：檢查並更新對外服務之過時加密協定 ➢ 落實憑證維運：定期驗證TLS憑證有效性與信任鏈完整性 ➢ 停用弱加密演算法：淘汰不安全之加密方法，確保傳輸安全	➢ 落實弱點修補：針對高風險元件漏洞執行即時更新與修復 ➢ 健全驗證機制：定期評估外部暴露面之安全性 ➢ 優化更新流程：建立常態化之元件版本管理與安全更新機制

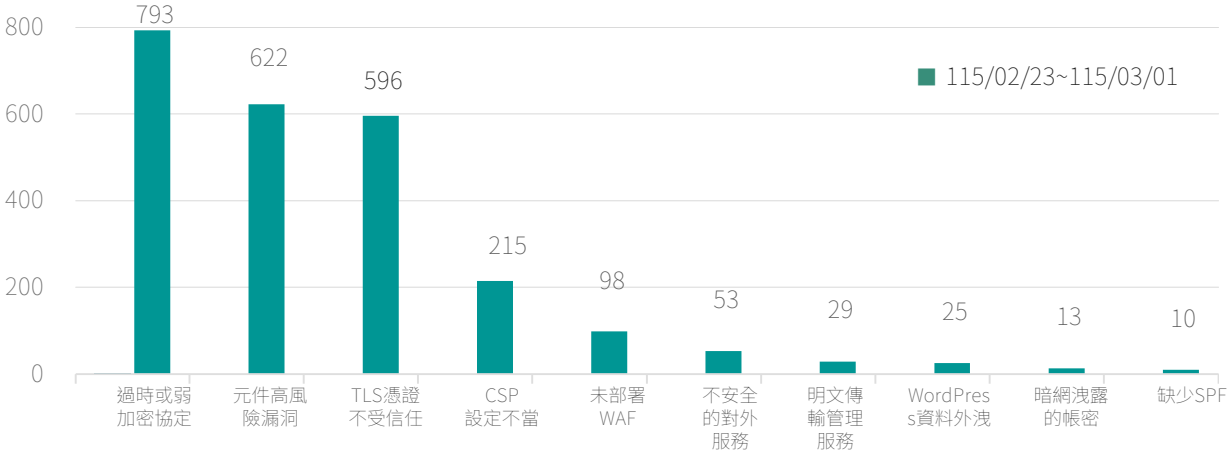

圖5| EASM檢測結果統計(前10大風險)

■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

題材輪動下整體趨勢小幅回落 「產品服務」仍居高 假客服與假投資仍需防範

整體觀察「全部高風險」總量趨勢，相較前一週(115/02/16~115/02/22)，本週(115/02/23~115/03/01)整體呈現小幅回落，顯示近期高風險詐騙的擴散動能略有收斂，詳見圖6。惟須提醒，趨勢回落不代表詐騙消失；詐騙內容常隨投放題材與社群話題更換而調整包裝，仍請民眾持續落實「先查證、再行動」，避免因一時鬆懈而受害。

從詐騙類型來看，「產品服務」依舊是最主要風險來源，且本週不減反增，顯示網購、二手交易與各式促銷情境仍容易被詐騙集團利用。常見手法包括假賣家誘導私訊下單、要求站外付款，或偽造付款/物流通知引導點擊不明連結。提醒民眾，交易資訊請以官方 App 或官網查詢為準，避免被引導改走私訊流程或站外交易。

「身分冒充」本週較前週減少，但仍持續可見「假冒親友」、「假冒公部門」、「假冒企業客服或金流客服」等情形。常見話術多以「退款/取消交易」、「帳戶異常」、「需立即驗證」等情境施壓，誘導提供驗證碼、配合操作或下載工具。提醒民眾遇到自稱官方來電或私訊時，先中止互動，再改以官方電話或官方客服管道查證，勿在原對話鏈內處理。

「金融投資」本週降幅最為明顯，顯示近期投資題材的活躍度暫時降溫。然而，此類詐騙常以「投資理財」、「虛擬貨幣」、「老師帶單」、「高報酬穩賺」等話術包裝，並透過社群群組、私訊邀請、獲利截圖或名人背書引導入金；一旦受害往往損失金額較高，仍請民眾保持高度警覺，不因短期減少而降低查證強度。

綜整而言，本週「全部高風險」整體較前週回落，但三大類型呈現分化:其中「產品服務」增加且仍為主要風險來源；「身分冒充」略有收斂但手法仍在；「金融投資」明顯降溫但屬高損失風險類型，後續仍需持續宣導與防範。

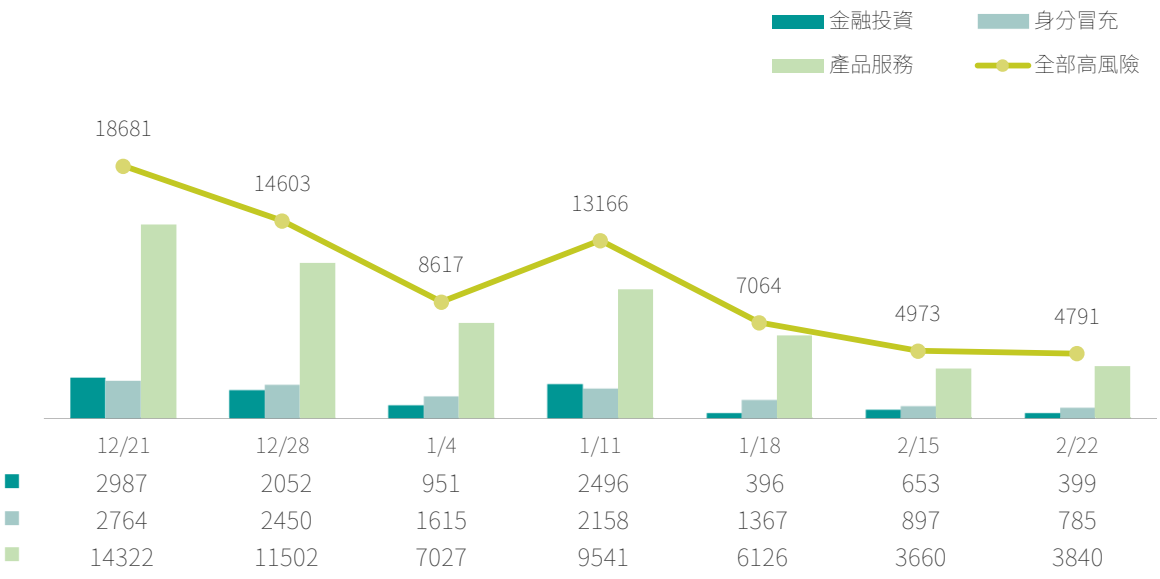

圖6 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙週趨勢

高風險詐騙偵測趨勢分析與提醒

提升多平台風險警覺

- ✓ 涉及購物、票券、二手交易或促銷訊息，若出現不明連結、短網址、要求私訊下單、要求改用站外付款或「限時、倒數、名額」等催促話術，請先停止並回到官方 App 或官網核對。
- ✓ 遇到投資相關廣告或社群邀請(帶單、老師、群組)，務必先查證對方身分與合法性；凡宣稱「保證獲利、穩賺不賠」者，請一律提高警覺並避免匆忙入金。
- ✓ 任何要求下載指定 App、安裝遠端工具、提供驗證碼或「配合操作」者，均屬高風險警訊，請立即中止互動。

強化身分驗證與求證習慣

- ✓ 親友以訊息表示急需匯款或代付，請改用電話或影音再次確認，避免僅以文字往返。
- ✓ 自稱公部門、金融機構、電商或物流客服者，如要求提供帳戶資料、協助解除分期、退款驗證或資金檢核，請先掛斷並改撥官方電話查證。
- ✓ 建議開啟多重驗證(2FA)並定期檢查登入紀錄與綁定裝置，降低帳號遭盜用後被冒名聯繫的風險。

善用官方資訊與檢舉機制

- ✓ 遇到疑似詐騙內容，請立即通報「165 反詐騙專線」或平台客服，並保留對話、連結、帳戶與交易資訊等證據。
- ✓ 請持續關注政府與金融機構發布之最新手法警示，特別留意「假客服」與「假投資」常見誘導步驟。
- ✓ 建議企業與平台持續更新偵測與攔截規則，針對「假促銷導流」、「偽造金流/物流通知」、「假客服施壓誘導操作」等樣態加強風險控管與提醒曝光。

本次「網路巡查高風險詐騙-詐騙關鍵字排名」顯示，排名較前之關鍵字以「台灣」、「設計」、「必備」、「推薦」、「優惠」為主要特徵，並搭配「神器」、「免費」等誘因型字眼，呈現出以在地化包裝+強促銷話術吸引點閱的趨勢，詳見圖7。常見手法為先以「台灣限定/登台」、「專業設計/量身規劃」、「必備神器/限時優惠」建立可信情境，進而引導民眾點擊短網址或站外連結，轉入外部頁面完成下單、填寫資料或加入聯繫管道，後續可能衍生蒐集個資、誘導付款、要求匯款或綁定付款方式等風險。

就整體內容觀察，「台灣」與「必備/神器/優惠」等關鍵字組合，常出現在團購、居家清潔、生活小物等商品宣傳，並以「限時、限量、買贈、加碼」等方式催促立即下單。此類貼文多伴隨短網址或多層跳轉連結，風險包含導向仿冒購物頁、釣魚頁面或非正式收款管道，亦可能以「加購、升級、保留名額」名義誘導追加付款。提醒民眾，對於來源不明之購物連結，切勿輸入信用卡、網銀或身分證件等敏感資訊，並應先查核賣家基本資料、退換貨規則、客服聯繫方式及付款安全機制後再決定是否交易。

另就「設計」與「推薦」等用語觀察，常被用於營造「專業背書、客製服務」之可信氛圍，並搭配「有問題」「可諮詢」等互動措辭，引導民眾進一步點擊連結或改以私下管道洽詢，以取得報價、方案或領取方式。此類情境可能將費用、合約條款、退費規則等重要資訊置於站外或私下溝通，並在後續以訂金、方案費、材料費等名目要求先付款。建議民眾，凡涉付款或合約事項，務必要求提供完整書面資料並審閱條款；若對方以「立即決定」「名額有限」催促付款，請提高警覺並先行查證。

此外，「健康」與「配方」等關鍵字亦位於前段，顯示健康相關商品、保健宣稱或寵物健康等情境仍為高風險類型之一。此類內容常以「配方升級、效果明顯、顧健康」等措辭吸引注意，並可能搭配「免費諮詢」作為入口，引導填寫個資、留下聯絡方式或導向特定收款頁面。提醒民眾，對於涉及療效、健康改善之宣稱應保持審慎，避免因誇大話術而急於下單；亦請勿在不明頁面提供身分資料、付款資訊或下載安裝來源不明之應用程式。

綜合上述，本次高風險訊息多呈現「在地化包裝(台灣)→ 可信化措辭(設計/推薦)→ 促銷催促(必備/神器/優惠)→ 導流站外(短網址/外部頁面)→ 交易或資料蒐集(付款、個資、付款綁定)」之常見路徑。提醒民眾:凡要求先點不明連結、先填寫資料、或以優惠與贈送為由要求先付款/提供帳戶與身分資料者，請立即停止操作並先行查證；建議優先透過官方網站與公開客服管道確認真偽，並保留相關連結、對話及交易資訊，以降低受騙風險。

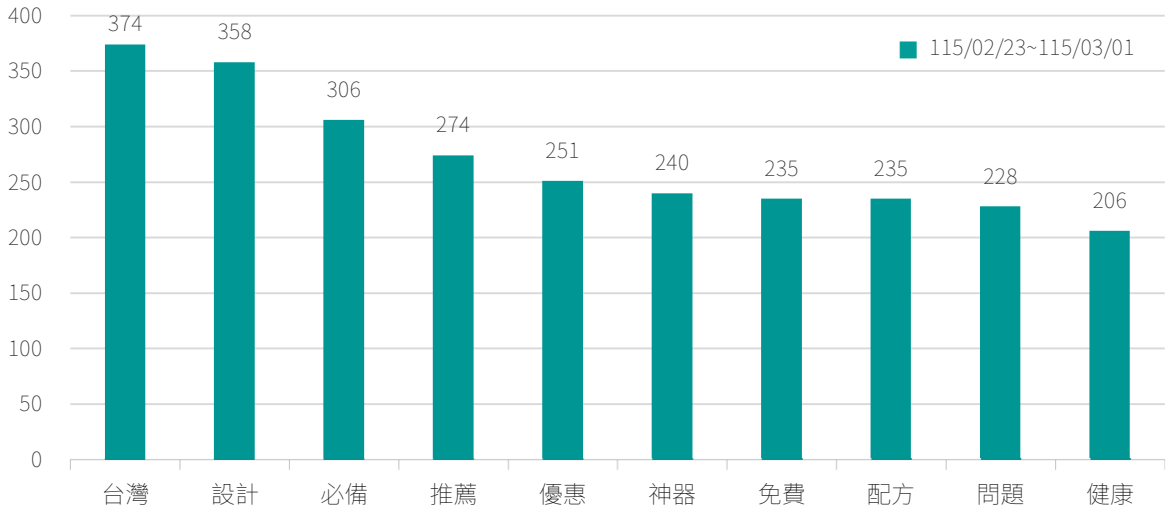

圖7 | 本週代表性詐騙關鍵字 Top 10

焦點文章

邊界設備風險升溫：VPN 重大漏洞、利用趨勢與防禦建議

為何 VPN 威脅日益嚴峻

近年各類邊界設備(Edge Devices)相關威脅持續升溫，核心原因在於：攻擊者越來越常把「利用已知漏洞」作為入侵的起點，而 VPN 等遠端存取服務因長期對外曝露、且直接連接內部網路，往往成為最先被掃描與嘗試利用的目標。

Verizon《2025 DBIR》指出，在「已知漏洞利用」這條攻擊路徑中，以 VPN 等邊界設備為目標的比例達 22%，顯示攻擊者對這類關鍵節點的高度興趣。同時，防守端也很難以傳統修補節奏追上攻擊速度，即使企業組織越來越重視邊界漏洞修補，全年仍僅約 54% 能完成修補。在「攻擊者可大量自動化掃描、利用門檻降低」與「修補需要停機、重啟、跨部門協調」的落差下，VPN 不再只是遠端連線工具，而是駭客最有利可圖、也最容易被規模化利用的入侵入口之一[1]。

VPN相關威脅與趨勢分析

資安院整理近一年 VPN 產品相關漏洞資訊，歸納出以下四類常見攻擊情境。這些情境的共同特徵是：一旦邊界設備失守，攻擊者往往可更快速地向內網橫向移動，並在短時間內造成重大損害(例如勒索加密、資料外洩、或服務全面中斷)。

漏洞類別一：遠端代碼執行（RCE）與記憶體安全威脅

由於許多邊界設備為了高效地處理網路封包，核心功能模組往往採用編譯型語言(如C/C++)開發，隨著程式碼逐代累積，若在緩衝區與記憶體邊界檢查上出現疏漏，就可能形成溢位等高風險弱點，形成駭客持續嘗試攻擊的目標。攻擊者一旦能透過對外服務(如VPN/Portal)發送特製封包或請求，便可能讓設備在未經授權的狀況下執行指令，使設備轉變為攻擊者進入內網、部署後門與橫向移動的快速通道。

焦點文章

漏洞類別二：身分驗證繞過與權限提升

相較於「直接打穿」的 RCE，這類漏洞如同「門禁規則設計有漏洞」，駭客可能利用認證流程、授權判斷、路徑解析或協議邏輯的瑕疵，繞過原本驗證方式，或把低權限身分「升級」成管理者。這種漏洞特別常出現在管理平面、Web 介面、或跨系統整合機制上；一旦被利用，駭客未必需要植入複雜惡意程式，只要取得管理控制權，就能改設定、建帳號、開後門，並把整個網路環境變成「可遠端操控」的狀態。

漏洞類別三：XSS、釣魚與憑據竊取

就算設備上不存在高風險 RCE ，駭客也可把「人」作為突破口。利用 VPN或登入頁面的 XSS 等前端漏洞，把惡意腳本藏在看似正常的連結裡，一旦使用者點擊，腳本就可能導致登入資訊、Session(已登入狀態)被竊取，或被導向高度相似的釣魚頁面。此類攻擊結合了「官方入口的可信感」與「使用者操作行為」，使攻擊者更容易取得合法身分，進而繞過部分防護機制。

漏洞類別四：服務可用性(DoS)與雲端管理風險

當駭客無法攻入，也可採用「讓你用不了」的策略。例如利用邏輯錯誤漏洞，造成設備反覆崩潰、進入維護模式，直接讓遠端辦公或對外服務中斷；或是從雲端管理平台、備份機制、API 等供應鏈環節下手，進而拿到設定檔與備份資料。由於備份檔可能包含帳號資訊、連線設定或其他敏感配置，一旦外洩，往往會進一步放大後續入侵與復原成本。

結論與企業組織應對策略

面對現今漏洞快速被武器化與規模化掃描的現實，邊界安全的重點應思考從「單點修補」走向「風險管理與架構調整」，有以下做法建議：

- 持續關注更新訊息：建立明確的更新告示與修補流程，當供應商發布安全更新或修補建議時，應評估影響並盡快完成更新，降低被已知漏洞鎖定的機率。

焦點文章

- 減少公網暴露： 考量 VPN 需要對外提供服務，難以完全避免公網存取，但應避免將管理介面直接曝露於公網。對外入口建議加上來源限制(如允許清單)、多因素認證、以及必要的登入防護(如嘗試次數限制/風險式登入)，以縮小可被攻擊面。
- 持續監控設備狀態： 強化設備日誌、狀態與異常行為的監控(例如異常重啟、設定變更、帳號新增、登入失敗暴增等)，並搭配帳號權限管理與定期稽核，以便及早發現入侵跡象或配置被竄改的情形。
- 架構轉型： 鑑於現在大多設備採用SSL-VPN 架構，而 SSL-VPN 建構於 Web 應用層，容易受到 Web 相關漏洞影響，企業可評估採用 IPsec 架構 VPN、或導入零信任存取控制(Zero Trust / ZTNA)等方式，降低單一入口失守所造成的橫向擴散風險。

引用資料

1. Verizion 2025 Data Breach Investigations Report，https://www.verizon.com/business/resources/T16f/reports/2025-dbir-data-breach-investigations-report.pdf

關鍵字：漏洞研析、邊界設備、VPN

刊　　名　資安週報第 34 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