



國家資通安全研究院

National Institute of Cyber Security

# 資安週報

Cyber Security Weekly Newsletter

## 外部曝險分析

外部曝險微幅上升 憑證管理與加密通訊仍待加強

## 重大漏洞

Gitea與GitLab高風險漏洞應盡速修補

## 實兵演練

實兵演練揭露登入功能SQL Injection弱點與敏感資訊外洩風險

## 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 & Gateway)及視覺化工作流程自動化工具  
成為攻擊熱點

## 事件通報

妥善控管錯誤訊息 避免洩漏系統資訊

## 網路巡查高風險詐騙

金融投資占比續升 廣告主打選股名單與課程

## 焦點文章

慎防真假難辨的惡意網站

2026.10.01

064

## 資安儀表板

外部曝險分析、重大漏洞、實兵演練、聯防監控、蜜罐誘捕、事件通報及網路巡查高風險詐騙等七類量化指標

### ■ 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

#### 外部曝險微幅上升 憑證管理與加密通訊仍待加強

本次針對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2,795項。其中，「元件高風險漏洞」以884項居首，「過時或弱加密協定」732項次之，「TLS憑證不受信任」694項位居第三。前三項合計2,310項，占前10大風險項目總數約82.6%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密協定及憑證管理等議題。相較上期2,758項，本期整體風險數量增加37項，增幅約1.3%，詳見圖1。

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888項微降至本期884項，降幅約0.5%。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍為主要風險來源，該弱點可能造成原始碼洩漏或程式碼執行風險，建議升級至2.4.60以上之已修補版本。「過時或弱加密協定」由725項增至732項，增幅約1.0%；「TLS憑證不受信任」由641項增至694項，增幅約8.3%。另「CSP設定不當」由235項增至240項，增幅約2.1%；「未部署WAF」由131項降至107項，降幅約18.3%。

整體而言，本期外部曝險呈現微幅上升，主要以「TLS憑證不受信任」增幅最為明顯，「過時或弱加密協定」及「CSP設定不當」亦較上期增加，顯示加密通訊、憑證管理及網站安全設定仍有持續強化空間；另一方面，「元件高風險漏洞」及「未部署WAF」則較上期減少，反映部分機關於元件修補及網站應用程式防護方面已有改善。建議持續落實高風險元件漏洞修補與版本更新，優先檢視TLS憑證有效性及信任鏈設定，並逐步汰除過時或弱加密協定，同時強化CSP設定及WAF防護機制，以降低外部資產遭受攻擊及曝險之風險。

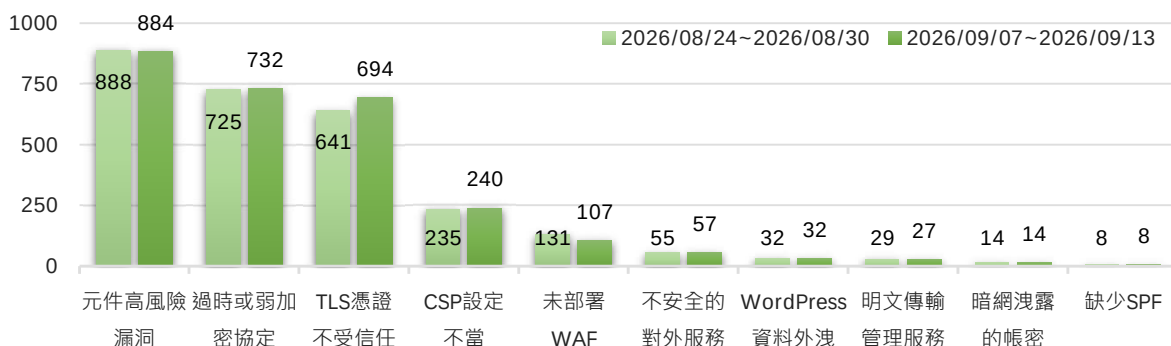


圖1 | EASM檢測結果統計(前10大風險)

## 防護建議

### 建議受測單位採取下列防護措施

- 優先修補對外服務所使用元件之高風險漏洞，並依原廠安全公告更新至已修補版本；如短期內無法完成升級，應採取WAF、虛擬修補、來源存取限制或網路區隔等補償性措施，以降低漏洞遭利用之風險
- 依據IETF RFC 10015，檢視TLS 1.2所使用之金鑰交換機制，停用較舊或安全性較低之方式，並優先採用ECDHE等具前向保密性之安全機制，以強化加密通訊安全
- 強化TLS憑證管理，定期檢視憑證有效期限、信任鏈及憑證狀態，並建立到期通知及自動續期機制，避免因憑證失效造成服務異常或安全風險
- 定期檢視網站CSP及WAF等防護設定，並依系統功能及實際業務需求調整安全政策，以降低跨網站腳本、惡意請求及其他

### Web攻擊風險

### 建議受測單位採取下列管理措施

- 建立並定期維護對外資產清冊，納管IP、網域、系統元件及憑證等資訊，以掌握各項資產之用途、版本及使用情形
- 建立高風險漏洞之修補、追蹤及複測機制，依漏洞嚴重程度訂定修補期限，並於完成修補後進行複測，確認改善措施有效落實
- 定期盤點系統所使用之軟體及第三方元件版本，持續追蹤原廠安全公告及CVE弱點資訊，並適時進行版本更新，降低使用已停止支援或存在已知弱點元件之風險
- 將漏洞修補、憑證更新、安全設定調整及後續複測等要求納入委外維運管理，明確訂定處理時限、責任分工及追蹤方式，以確保各項改善措施確實執行

## ■ 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

### Gitea與GitLab高風險漏洞應盡速修補

- Gitea存在程式碼注入(Code Injection)漏洞(CVE-2026-60004)[1][2]，未經身分鑑別之遠端攻擊者可藉由重複提交相同修補檔以製造合併衝突，將可執行之Git鉤子(Hook)程式寫入儲存庫根目錄，進而以Gitea服務帳號權限執行任意指令，該漏洞已遭駭客濫用。
- GitLab存在多項高風險安全漏洞(CVE-2026-85706與CVE-2026-87719)[3]，類型包含路徑遍歷(Path Traversal)與不安全之反序列化(Insecure Deserialization)，其中，CVE-2026-85706已遭駭客濫用。
  - CVE-2026-85706：未經身分鑑別之遠端攻擊者，可利用儲存庫提交應用程式介面(Repository Commits API)存在路徑限制不當與未強制執行身分鑑別之缺失，讀取伺服器上之任意檔案，導致機敏資訊外洩。
  - CVE-2026-87719：已通過身分鑑別之遠端攻擊者可藉由特製之GraphQL訂閱參數，繞過序列化處理並進行伺服器端物件查找，進而取得Advanced Search之執行個體設定與敏感憑證。

[1] <https://github.com/go-gitea/gitea/security/advisories/GHSA-rcr6-4jqh-j84m>

[2] <https://blog.gitea.com/release-of-1.27.1/>

[3] <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/>

## ■ 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

## 實兵演練揭露登入功能SQL Injection弱點與敏感資訊外洩風險

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9/24止已累計389筆攻擊紀錄，本週新增弱點數量共8筆，分別為「無效的存取控管」5筆、「驗證機制失效」1筆、「不安全的組態設定」1筆及「注入攻擊」1筆，詳見圖2。

本週演練發現，高風險弱點為「注入攻擊」。攻擊者於系統網頁中發現「請輸入學校代碼」欄位，並透過公開資訊取得有效學校代碼後，成功進入系統登入頁面。攻擊者於登入頁面輸入帳號與密碼建立登入請求，並透過Burp Suite工具攔截系統請求後存成檔案，使用SQLMap工具進行弱點驗證，確認系統登入功能存在SQL Injection弱點，並可取得系統資料庫名稱、資料表名稱及資料表欄位內容，進一步發現資料表中包含資通系統帳號與密碼，造成系統敏感資訊遭未授權存取之風險。

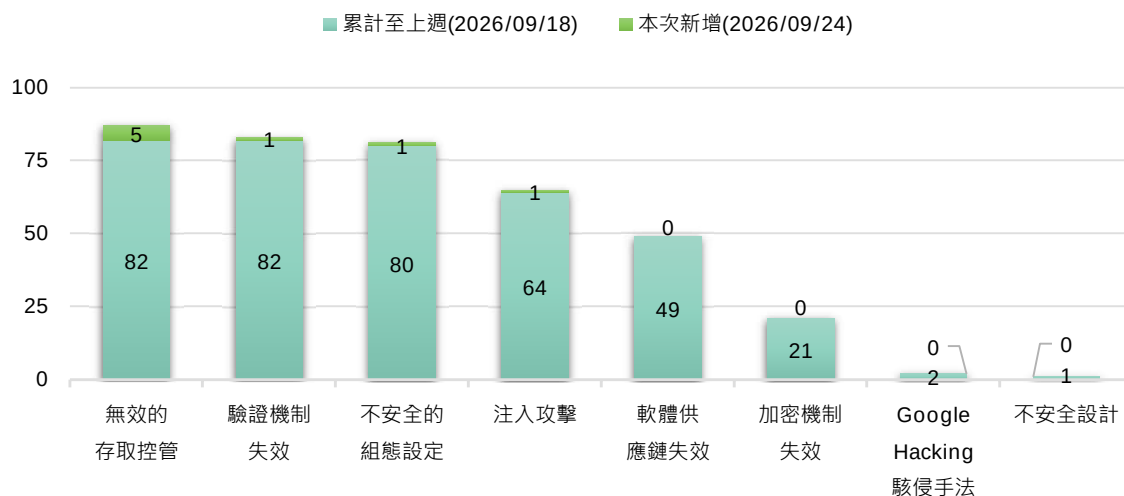


圖2 | 網路攻防演練資通系統實兵演練統計

## 建議機關及關鍵基礎設施提供者，採取下列防護措施

- 學校代碼不應作為唯一之存取驗證機制，並應強化相關功能之身分驗證與存取控管，避免透過公開資訊取得代碼後進一步存取系統
- 系統登入功能之輸入參數應進行適當之輸入驗證，並採用參數化查詢(Parameterized Query)或預備語句(Prepared Statement)，避免輸入內容遭利用進行SQL Injection攻擊
- 資料庫帳號應依最小權限原則設定存取權限，限制應用程式僅能存取必要之資料庫與資料表，避免透過系統弱點取得非必要資料

## ■ 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14.3%，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12.3%，為本週占比次高的攻擊階段，顯示攻擊者持續針對目標環境進行前期偵查與網路資訊蒐集，以掌握對外暴露資產及潛在攻擊入口。觀察到的主要手法包括主動式掃描、IP 區段掃描、以及DNS / 被動式 DNS資訊蒐集。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，以識別可存取主機、開放埠及服務資訊，並結合 DNS 與被動式 DNS 資料，蒐集目標網域、子網域及歷史解析關聯，進一步掌握目標組織的網路架構與資產分布。此類活動結合主動與被動偵查方式，可協助攻擊者建立較完整的攻擊面資訊，作為後續漏洞探測及初始入侵的重要依據。建議機關持續監控異常掃描流量與可疑來源，定期盤點對外暴露資產及 DNS 資訊，並結合威脅情資進行來源分析與阻擋，以提前辨識潛在偵查活動並降低後續入侵風險。

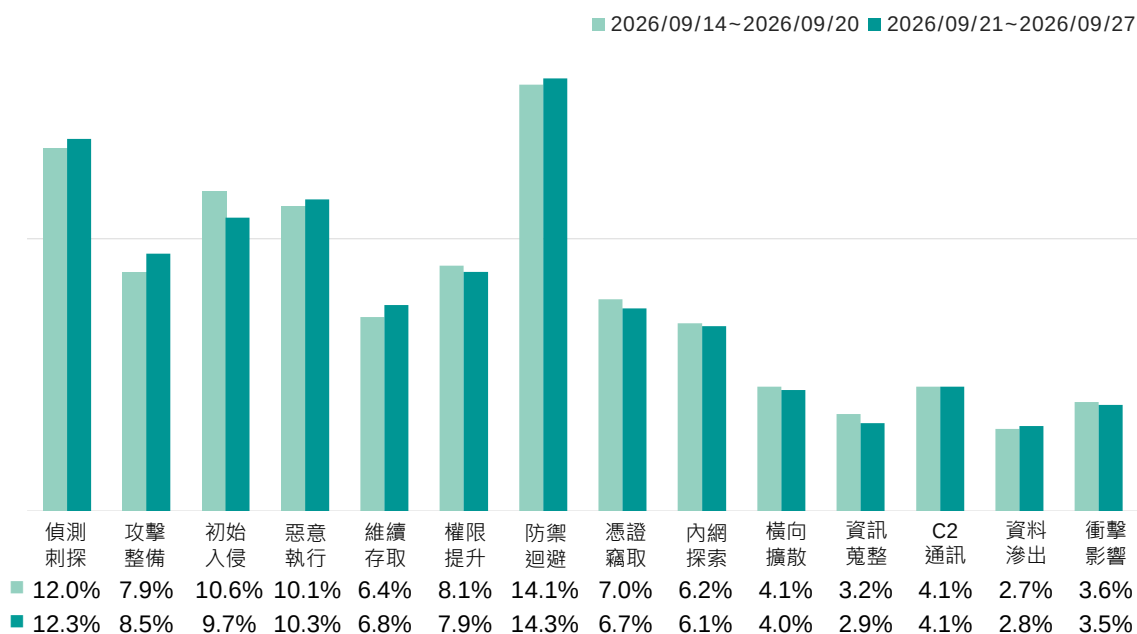


圖3 | 資安聯防監控攻擊階段統計



## 防護建議

建議機關採取下列防護措施



## 防禦迴避 (Defense Evasion)



強化端點防護與異常行為偵測



加強 PowerShell、Shell 等指令執行與操作紀錄稽核



限制高風險系統工具與管理工具的使用權限



強化特權帳號管理，避免攻擊者利用合法權限規避偵測



集中保存系統與安全日誌，降低紀錄遭刪除或竄改的影響



## 偵測刺探 (Reconnaissance)



持續監控異常掃描、IP 區段探測及大量連線行為



定期盤點對外暴露的主機、服務、開放埠及網路資產



檢視 DNS / 子網域資訊暴露情形，減少不必要的公開資訊



結合威脅情資識別惡意掃描來源，適時進行封鎖或限制



定期執行外部曝險面與弱點檢視，優先修補高風險對外服務

## ■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 & Gateway)及視覺化工作流程自動化工具成為攻擊熱點

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75.95%、「遠端控制」服務攻擊占比21.13%，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68.64%。「遠端控制」服務亦有26.08%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服務系統比例大幅上升主因為Cisco Secure ASA & FTD 缺少授權漏洞之CVE-2025-20362，遭攻擊次數上升導致。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。

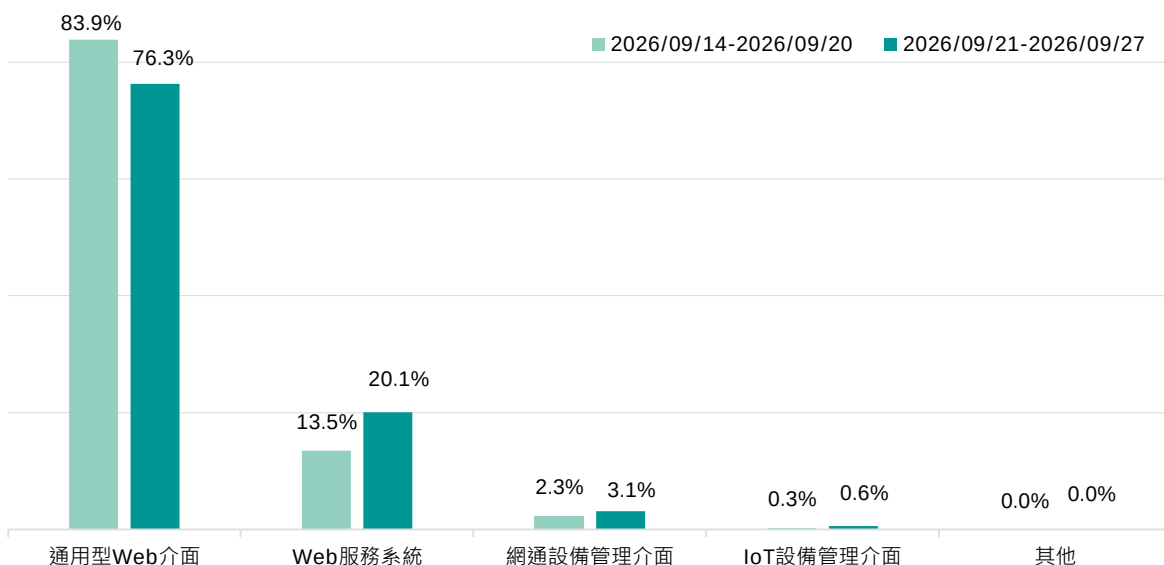


圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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1。近1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、輸入驗證不當漏洞、身分驗證繞過漏洞及指令注入漏洞，攻擊目標涵蓋程式遞送控制器(ADC & Gateway)、視覺化工作流程自動化工具、網站主機伺服器管理系統、大模型API統一介面與代理伺服器工具及企業級的終端裝置管理與資安防護系統。

### 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1年漏洞排行列表

| 排名 |   |       | 漏洞編號                        | 受影響產品                   | CVSS 3.x Base Score | 已知遭利用漏洞 (KEV) |
|----|---|-------|-----------------------------|-------------------------|---------------------|---------------|
| ■  | 1 | -     | CVE-2026-3055 <sup>1</sup>  | NetScaler ADC & Gateway | 9.8                 | ✓             |
| ■  | 2 | ↑ new | CVE-2026-21858 <sup>2</sup> | n8n                     | 10                  |               |
| ■  | 3 | -     | CVE-2026-41940 <sup>3</sup> | cPanel & WHM            | 9.8                 | ✓             |
| ■  | 4 | ↓ 2   | CVE-2026-42271 <sup>4</sup> | LiteLLM                 | 8.8                 | ✓             |
| ■  | 5 | ↑ new | CVE-2026-1603 <sup>5</sup>  | Ivanti Endpoint Manager | 8.6                 | ✓             |

類型 ■ 越界讀取漏洞

■ 輸入驗證不當漏洞

■ 身分驗證繞過漏洞

■ 指令注入漏洞

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-3055>

2. <https://nvd.nist.gov/vuln/detail/CVE-2026-21858>

3. <https://nvd.nist.gov/vuln/detail/CVE-2026-41940>

4. <https://nvd.nist.gov/vuln/detail/CVE-2026-42271>

5. <https://nvd.nist.gov/vuln/detail/CVE-2026-1603>

## ■ 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

## 妥善控管錯誤訊息 避免洩漏系統資訊

本週總計接獲26件公務機關與特定非公務機關事件通報，詳見圖5，公務機關非法入侵事件中以異常連線占多數，詳見圖6。本週發現機關網站API發生伺服器錯誤時，回傳內容揭露後端服務設定，其中包含資料庫錯誤訊息及程式檔案路徑。相關資訊可能使攻擊者進一步掌握系統作業流程、後端服務位置及使用技術，縮小後續探測範圍，並提高針對特定服務或弱點進行攻擊的可能性。

建議機關建立統一的錯誤處理機制，系統發生異常時，對外僅回傳必要之錯誤代碼及不涉及內部實作細節的訊息，詳細的系統設定、程式路徑及診斷資訊等則應留存於伺服器端日誌。另應透過參數缺漏、格式錯誤及其他異常輸入等情境進行測試，確認錯誤回應不會揭露內部系統資訊或敏感設定。

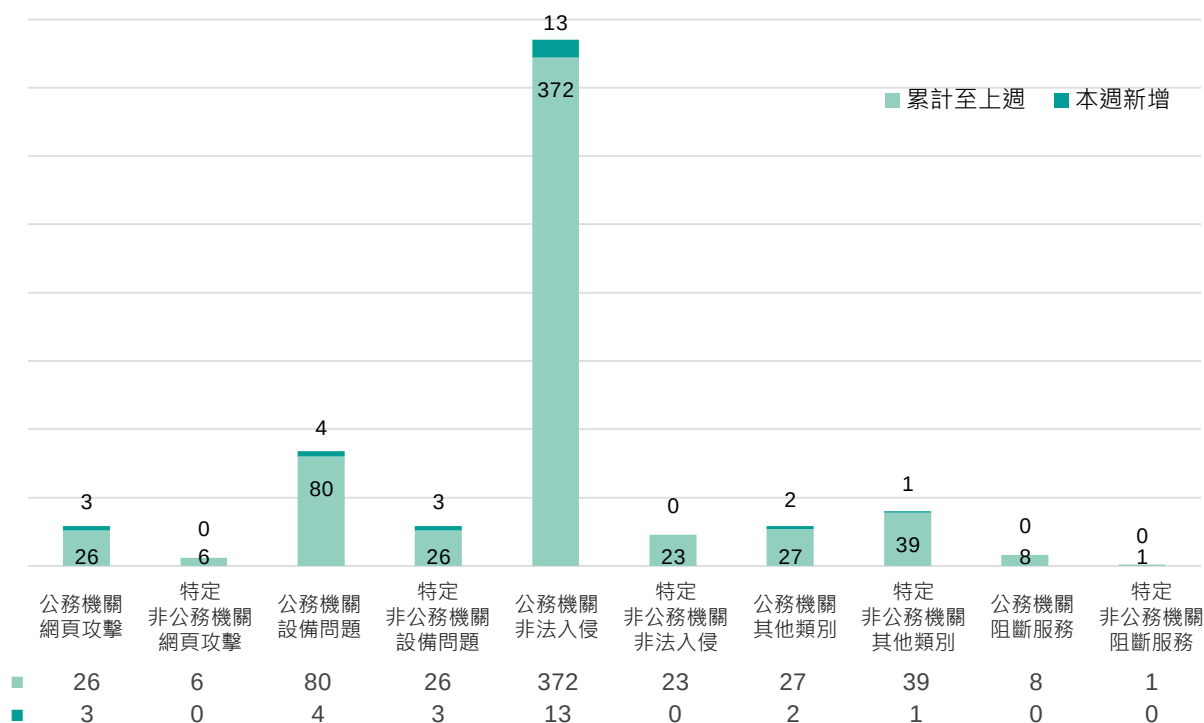


圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

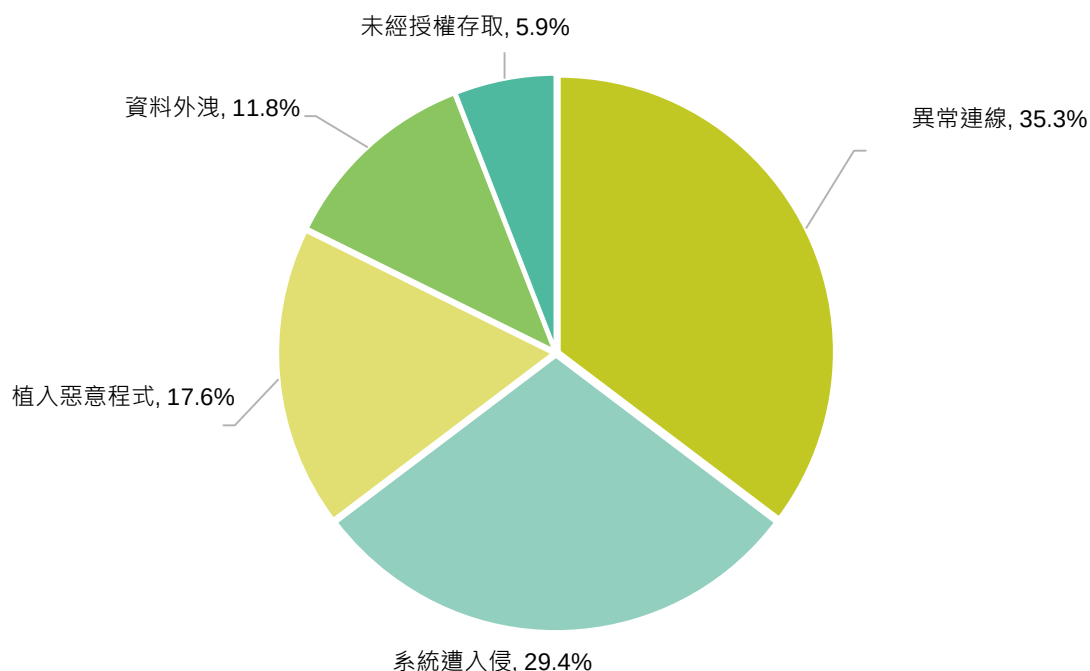


圖6 | 本週公務機關非法入侵事件類型占比

## 防護建議

除修補漏洞外，應：

## 以攻擊為出發評估潛在風險

- 錯誤訊息揭露系統路徑與後端資訊協助攻擊者探測弱點
- 攻擊者利用技術與服務資訊縮小範圍發動針對性攻擊

## 針對潛在風險執行相應改善

- 建立統一錯誤處理機制，對外僅回傳必要錯誤代碼及一般性訊息
- 禁止API回傳程式路徑、資料庫錯誤及後端服務等內部系統資訊
- 詳細錯誤與診斷資訊僅留存伺服器端日誌，並限制存取與妥善保存
- 定期以參數缺漏及異常輸入進行測試，確認錯誤回應未揭露敏感資訊

### 1間民間企業揭露重大資安訊息

本週1間民間企業發布重大訊息，產業類別為運動休閒業，詳見表2。

表2 | 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                                                                                                                                |
|--------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 柏文健康事業股份有限公司 | 2026年09月23日 | 柏文公司接獲系統委外廠商通知對外服務系統遭自動化攻擊，並對客戶資料表分頁擷取，其中部分涉及本公司員工及會員個資，已依個資事故通報及處理流程啟動應變會議，並採取必要防護措施降低影響。目前評估對公司營運無重大影響，且要求系統委外廠商重新檢視造成資安疑慮因子加以防範。 |

## ■ 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

## 金融投資占比續升 廣告主打選股名單與課程

## 詐騙類型趨勢

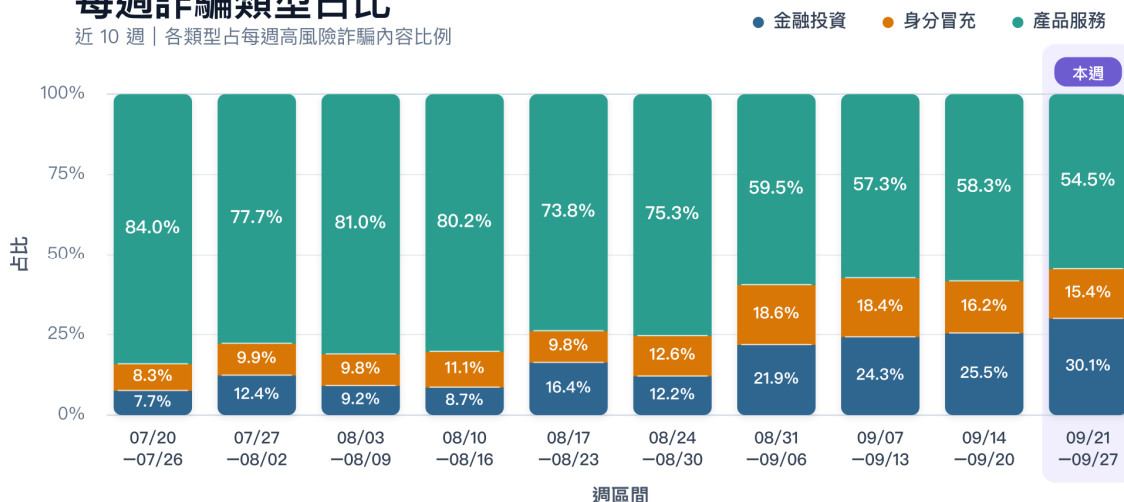
金融投資型占比續升，詳見圖7，本週在三類中排名第二。選股廣告以免費領取「黑馬名單」招攬民眾，宣稱現在可低價進場，並以錯過就得再等數月的說法製造急迫感。另有短線選股社群強調不收費、不分成，聲稱盤前提供操作策略、盤中就能看見效果，邀請民眾加入。

身分冒充型在三類中占比最低，本週較前週回落。例如，有保養品廣告藉醫師名義宣稱商品能淡化細紋，再以「假一賠十」的承諾減輕民眾對商品真偽的疑慮。

產品服務型占比較前週下降，但仍居本週首位。其中，有廣告主打免費贈送小型神像，供民眾擺放在家中或車內，宣稱能護佑平安，再以數量有限、先到先得催促民眾私訊預留。

## 每週詐騙類型占比

近 10 週 | 各類型占每週高風險詐騙內容比例



註：各週三類占比合計為 100%；本週以淡色區塊標示。

資料期間：2026/07/20—09/27

圖7 | 每週詐騙類型占比

## 關鍵字趨勢

「投資」升至本週首位，詳見圖8，「市場」從前週第 20 名升至第 3 名。「投資」相關廣告主打美股模擬交易，邀請民眾練習下單與設定停損，並引導民眾留言，進一步了解模擬交易帳號的申請方式。「市場」相關的投資課程廣告則宣稱提供高勝率模型，邀請想提高操盤績效的民眾參加體驗課，學習判讀市場。

「免費」與「優惠」分別退至第 2、第 4 名，「點擊」升至第 6 名。以「免費」為例，貸款廣告主打免費諮詢與額度試算，並宣稱前半年可享優惠利率；購車廣告以優惠車價和全額貸款吸引買家。二手商品廣告則要求先點擊聯繫、了解選購詳情，才能領取可折抵消費金額的優惠卡。

「團購」從前週第 29 名升至第 9 名，進入本週前 10 名。前週的「團購」廣告以免囤貨招募批發主，本週則宣稱能協助品牌尋找帶貨網紅、自動對帳，再以限時招募催促有意合作的業者填表。從本週前十大關鍵字來看，廣告同時瞄準想學投資、節省開銷的民眾，以及尋找銷售合作的業者。

## 詐騙關鍵字占比週比變化

以本週為主 | 完整顯示本週 Top 10

○ 前週 9/14-9/20 ● 本週 9/21-9/27

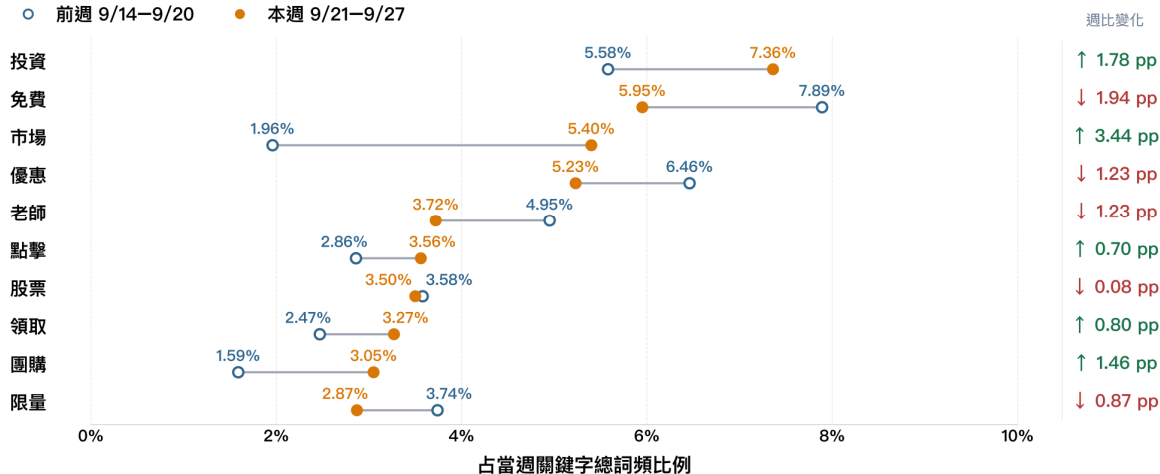


圖8 | 詐騙關鍵字占比週比變化

## 焦點文章

## 慎防真假難辨的惡意網站

### 當AI應用使惡意網域越來越像真實服務

#### 惡意網域生成技術演進

近年生成式人工智慧(Generative AI)與大型語言模型(Large Language Model, LLM)快速發展，使惡意網域的生成方式逐漸由傳統隨機或規則式的域名生成演算法(Domain Generation Algorithm, DGA)，朝向具備語意合理性、品牌關聯性或攻擊情境的生成模式發展。相較於傳統 DGA 所產生的高隨機性字串，AI 輔助生成網域在字詞結構、語意與命名邏輯上可更接近正常網域，進而提高舊有威脅偵測模型辨識惡意網域之難度。

回顧去年底由資安威脅風險管理組織所發布之2026展望報告[1]，部分研究與產業觀察認為，生成式 AI 可能進一步降低域名攻擊在技術、人力與時間上的門檻。攻擊者可利用 LLM 快速產生大量與目標品牌、服務或業務情境相近之混淆域名，並網站生成、自動化內容製作及網頁部署工具，在短時間內建立外觀、文案風格及服務情境與真實企業高度相似的偽冒網站。此類能力使網域生成不再只是大量產生名稱，而是逐漸與品牌仿冒、社交工程及釣魚內容生成整合。

國家資通安全研究院觀測外部資安威脅情資，比對被國際資安組織通報之惡意網域威脅指標，發現其網域名稱疑似為仿冒或相似混淆變體之數量，於今(115)年第一季約一千一百萬筆，至第二季已持續增加至一千四百萬筆，詳見圖9。

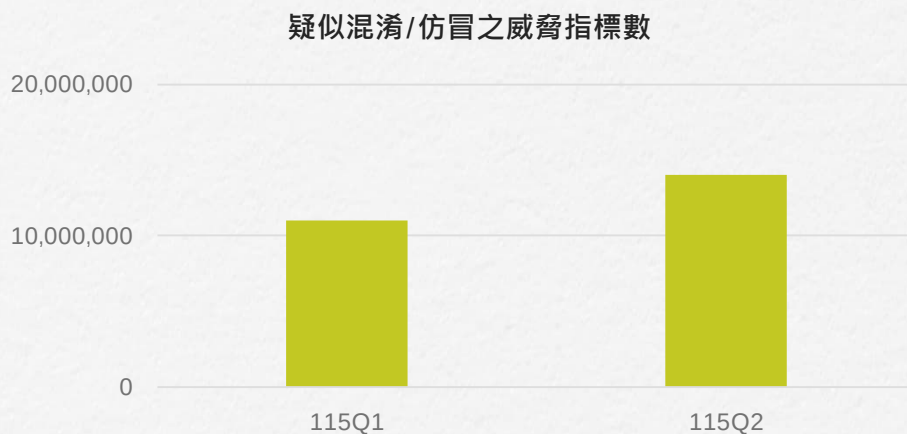


圖9 | 威脅指標數

## 焦點文章

隨著代理式人工智慧(Agentic AI)進一步發展，AI 在網路攻擊流程中的角色也由單純「輔助工具」逐步朝向具備較高自主性之任務執行機制發展。透過 LLM 與自動化腳本、API 及其他網路工具整合，部分攻擊流程可進一步串聯目標資訊蒐集、候選網域產生、網域註冊、TLS 憑證申請、網站內容生成及釣魚頁面部署等工作。此外，透過代理服務、跳板或區域規避機制，攻擊者亦可降低地理限制與基礎設施封鎖所造成的影響，使惡意網域及釣魚基礎設施的建立、替換與重新部署速度進一步提高。[2]

### 現況與未來趨勢

生成式 AI 對於惡意網域威脅所帶來的影響，將不僅限於傳統域名生成演算法(DGA)之濫用，更值得關注的是 LLM 的語意理解與內容生成能力。攻擊者可依據目標組織的業務屬性、品牌名稱、服務內容或特定攻擊情境，產生在語法、語意及命名邏輯上更具合理性的惡意網域，使其更容易融入正常網路環境，並降低僅依賴字串亂度、關鍵字或簡單規則進行偵測之有效性。

此外，生成式 AI 的跨語言能力也可能進一步降低過去因語言、文化及在地用語所形成的攻擊門檻。LLM 不僅能進行字面翻譯，也能依據特定地區的語言習慣、文化背景與使用情境重新生成內容，使攻擊者更容易建立符合不同國家或市場特性的網域名稱與釣魚內容。相關研究亦顯示，在魚叉式釣魚攻擊情境中，LLM 可利用少量公開社群資訊擷取目標的興趣、情境及溝通風格等特徵，並據此自動產生具有高度個人化與情境相關性的釣魚內容。[3]

整體而言，目前尚缺乏足夠實證資料證明真實惡意網域已由 LLM 進行大規模自動化生成。然而，從生成式 AI 在內容生成、品牌仿冒、跨語言溝通、個人化社交工程及自動化工作流程上的快速發展來看，未來惡意網域攻擊很可能逐步由單純的大量生成，轉向更強調語意合理性、情境適配性、品牌相似性與自動化部署的攻擊模式，AI 與釣魚攻擊、域名註冊及網路基礎設施自動化的整合，將成為後續惡意網域研究與威脅偵測之重要趨勢。

## 焦點文章

---

### 參考文獻

- [1] Panorays (The Future of Domain-Based Threats and AI-Driven Cyber Hygiene: 2026 Outlook), <https://panorays.com/blog/domain-threats-ai-cyber-hygiene/>
- [2] Check Point Research (AI Security Report 2026), <https://research.checkpoint.com/2026/ai-security-report-2026/>
- [3] Context-Aware Spear Phishing: Generative AI-Enabled Attacks Against Individuals via Public Social Media Data, <https://arxiv.org/html/2605.11268v1>

關鍵字：惡意網域、AI網路釣魚

刊 名 資安週報第 64 期  
發 行 人 國家資通安全研究院 龔化中院長  
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](http://www.nics.nat.gov.tw)  
訂閱網址 [www.nics.nat.gov.tw/newsletter/](http://www.nics.nat.gov.tw/newsletter/)  
讀者信箱 [www.nics.nat.gov.tw/mail2center/](http://www.nics.nat.gov.tw/mail2center/)



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