資安週報 | 試刊號第 1 期
114/7/7-114/7/13 — 7/17發布
國家資通安全研究院 National Institute of Cyber Security

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。

- 公司名稱：海華科技股份有限公司
- 發布時間：114/7/8
- 事件說明：公司偵測系統偵測到資訊系統遭受駭客攻擊，經評估對公司財務及業務並無重大影響

表1 | 本週企業重訊發布列表

本週總計1家民間企業發布重大訊息，詳見表1，產業類別屬通信網路業。

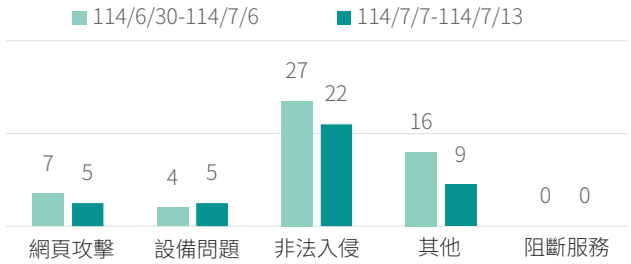

圖1 | 本週公務機關資安事件通報概況

本週總計接獲41件公務機關事件通報，詳見圖1，相較於上週，本週通報事件類型無明顯變化，非法入侵事件仍占多數，本週非法入侵事件主要為資安警訊通報事件居多，包括資訊設備產生符合冒牌軟體特徵之連線與實兵演練攻擊成功事件。建議使用者下載任何應用程式前，請先至官方網站確認其網址是否正確，以確保資訊系統安全。

■ 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。

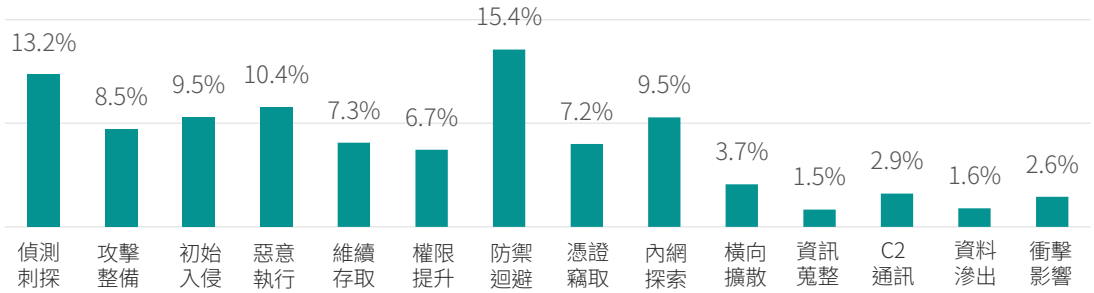

圖2 | 資安聯防監控攻擊階段統計

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，詳見圖2，防禦迴避（Defense Evasion）為最常見攻擊手法，占比15.4%，攻擊者常透過關閉或清除指令紀錄，並以系統合法工具間接執行惡意命令，以規避監控，建議導入端點防護，強化指令紀錄稽核、限制高風險工具濫用，並落實特權帳號管理，以防範攻擊者規避偵測並抹除行為痕跡。

■ **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。

「網頁應用」為國內外攻擊行為主軸；「遠端控制」次之

本週透過部署於國內外之蜜罐系統觀測攻擊態勢，已知攻擊行為主要集中於「網頁應用」服務，占比高達85.74%，顯示此類服務為威脅攻擊主軸。此外，針對「遠端控制」服務之攻擊比例亦有11.96%，反映攻擊者以公開遠端連線作為次要入侵方式。由於網頁應用是最為常見之對外服務類型，若存在已知漏洞或弱點，將面臨高風險暴露情形，易成為攻擊者入侵與滲透重要管道，須做為優先防護之項目。

類型 ■ 遠端程式碼執行漏洞 ■ 檔案上傳漏洞

		漏洞編號	受影響產品	CVSS 3.x Base Score
■	1	CVE-2021-38647	Microsoft OMI管理伺服器	9.8
■	2	CVE-2017-17215	Huawei路由器	8.8
■	3	CVE-2016-3088	Apache ActiveMQ訊息代理程式	9.8
■	4	CVE-2023-42793	TeamCity 伺服器	9.8
■	5	CVE-2024-36401	GeoServer	9.8

表2 |本週前5大攻擊使用之漏洞排行列表

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。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遠端程式碼執行與檔案上傳漏洞，攻擊目標涵蓋路由器、應用伺服器及開源套件，顯示此類系統已成為高風險熱點，建議各單位加強資安防護措施。

▲ 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：

- Fortinet FortiWeb出現1個嚴重風險資安漏洞(CVE-2025-25257)，CVSS分數達到9.8分。
- VMware ESXi、Workstation及Fusion存在沙箱逃逸(Sandbox Escape)漏洞(CVE-2025-41236、CVE-2025-41237及CVE-2025-41238) ，允許取得虛擬機一般權限之攻擊者於主機端執行任意程式碼。

前述相關漏洞，官方已釋出更新版本，建議儘速確認並進行修補。

■ 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。

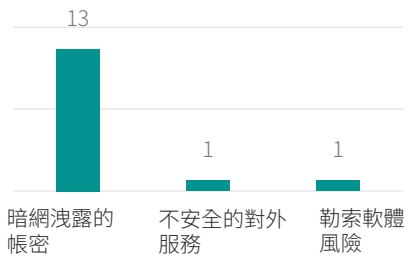

圖3 | 重大風險發現數量

本週針對55個公部門單位執行EASM資安曝險檢測，重大風險發現(Critical Finding)數量共計15個，詳見圖3，建議相關單位強化風險控管，清查並變更受影響帳號密碼，關閉不必要之對外服務，以及定期備份關鍵資料，強化端點防護與漏洞修補作業。

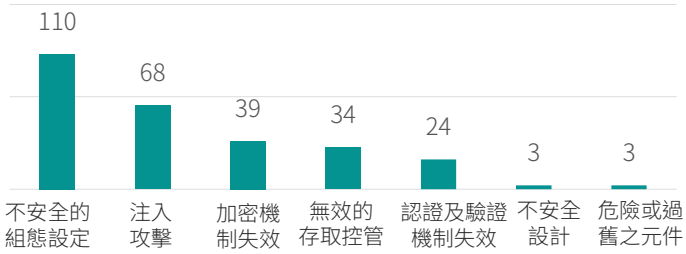

圖4 | 網路攻防演練資通系統實兵演練統計

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，並於擇定時間針對前述機關進行演練，詳見圖4，至7/12止已累計281筆攻擊紀錄，依弱點數量排名前3名依序為「不安全的組態設定」110筆、「注入攻擊」68筆及「加密機制失效」39筆，可能遭攻擊者取得系統設定檔案、Google API權限或機敏資料等影響，建議應重新檢視系統設定檔與API權限有確實進行限制，並針對網頁輸入的危險字元進行過濾或設定白名單，以及避免僅以前端頁面進行阻擋。

■ 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。

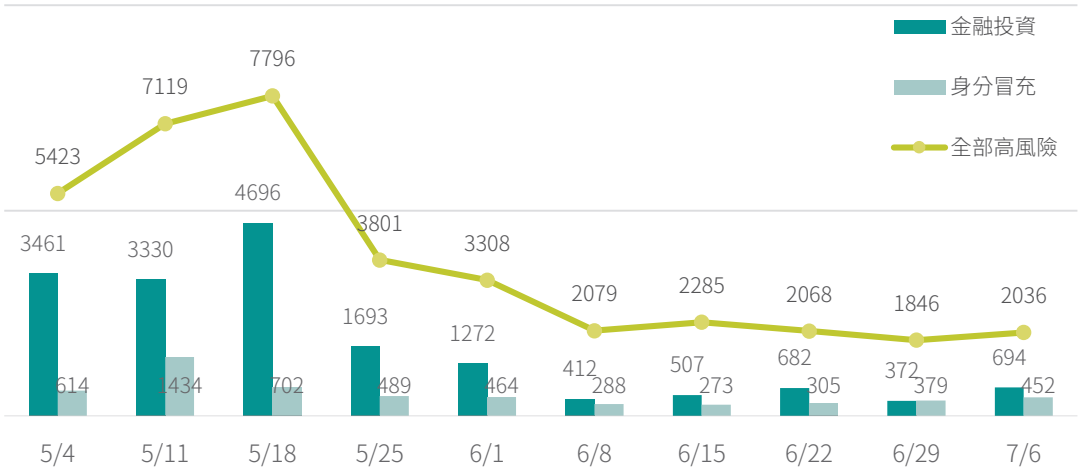

圖5 | 偵獲高風險金融投資類及身分冒充類詐騙週趨勢

本院於網路巡查偵獲之高風險詐騙總數，以及金融投資類、身分冒充類詐騙之週趨勢統計，詳見圖5。可看出詐騙數量自五月中旬起已逐步降低，原因可能與政府強力要求平台業者積極下架詐騙廣告有關，但是也必須注意是否詐騙集團針對偵測機制進行反制，導致偵獲量下降。

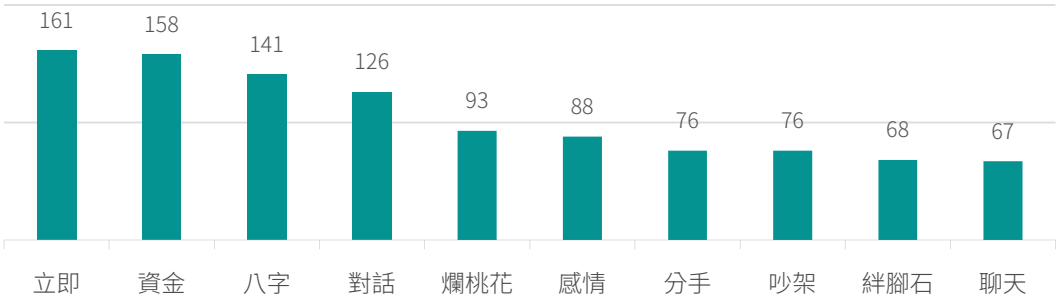

圖6 | 本週 Top10 詐騙關鍵字排名

本週的通報詐騙關鍵字統計排名前10名，詳見圖6。除了延續先前的投資理財、融資貸款、命理算命之外，還進一步出現了以感情爭吵、第三者問題、情緒操控等包裝的愛情交友詐騙。「爛桃花」、「不甘心」、「老師」等關鍵字，利用外遇問題與感情挫折，引誘受害者尋求命理風水老師協助，以進行詐騙。

焦點文章

從機制面強化產業於公私協同治理之角色

英國重組「政府資安顧問委員會」

114年6月下旬，英國《資安成長行動計畫》（Cyber Growth Action Plan）重組政府資安顧問委員會，自機制面將產業界參與資安立法與政策形成之時點前移。此轉變並非一時應急的權宜之計，而是針對資安威脅所採取的長期應對策略，相當於英國從機制設計面，擴大產業界在資安治理的實質責任與參與程度。

重組後之英國「政府資安顧問委員會」（Government Cyber Advisory Board），正式納入具全球技術與產業影響力的企業，如BAE Systems、AWS、Microsoft、Google DeepMind、Santander等。此委員會在成立後，將開始參加與英國資安相關之立法與政策討論，例如備受矚目之《資安與韌性法案》(Cyber Security and Resilience Bill）可能即是第一例。產業從原本受政府規管的對象，也就是利害關係人，轉而成為資安法制與政策制定過程中的諮詢與協力夥伴。

英國政府此規劃，一方面與產業界建立起持續性之公私對話與決策參與的機制；另一方面，則充分借助業界掌握第一線技術與風險趨勢的優勢，協助政府即時掌握威脅態勢，為公部門提供資安法制與政策建議，有利於強化國家整體資安韌性。

對我國公私治理的啟示

我國擘劃資安政策或相關立法時，素有邀集學者、專家參與討論並提供專業、客觀意見之良好做法，亦常在個別政策最終形成之前，聽取產業界等利害關係人與公眾之意見，惟自機制面上納入產業，由其常態參與，並於政策或法制形成之初，即參與提供諮詢建議之作法，則仍屬創新。參考英國相關機制，我國或亦可考慮由政府機關主導，在法律許可之前提下，邀集例如雲端、半導體、金融、AI等關鍵產業代表，結合學研界專業，以常態化方式，參與資安政策與法制研擬。透過此機制，建立產政學研共治文化，引導產業界更主動、持續投入政策形成與論辯之過程，亦有助於政府迅捷掌握產業實務需求，提升政策落實之效率。

關鍵字
公私協同治理、英國、資安成長行動計畫、政府資安顧問委員會

刊　　名　資安週報第1期　試刊號
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
讀者信箱　contactus@nics.nat.gov.tw

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

本刊所有圖文內容均受著作權法保護，未經授權，
禁止翻印、複製、轉載。