資通安全網路月報（112年8月）

資通安全網路月報(112年8月)

<近期政策重點>

為因應資通安全事件，應訂定機關通報及應變機制，並請落實「國家資通安全通報應變網站」帳號盤點，以確保機關資安人員名單正確性，如有人員異動情形，應及時更新。

<整體威脅趨勢>

事前聯防監控

本月蒐整政府機關資安聯防情資共59,498件，分析可辨識的威 脅種類，第1名為資訊蒐集類(47%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(22%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(14%)，大多是系統遭未經授權存取或取得系統/使用者權限。另統計近1年情資數量分布詳圖1。

經進一步彙整分析聯防情資資訊，發現近期駭客偽冒某單位，利用與該單位業務相關主旨，寄送社交工程郵件攻擊政府機關與一般民眾。經分析，駭客竊取民眾過往與該單位來往之郵件內文做為誘餌，附上惡意附檔，大量散布惡意程式垃圾郵件(Malspam)進行社交工程攻擊，透過植入後門程式竊取個人資料，相關情資已提供各機關聯防監控防護建議。

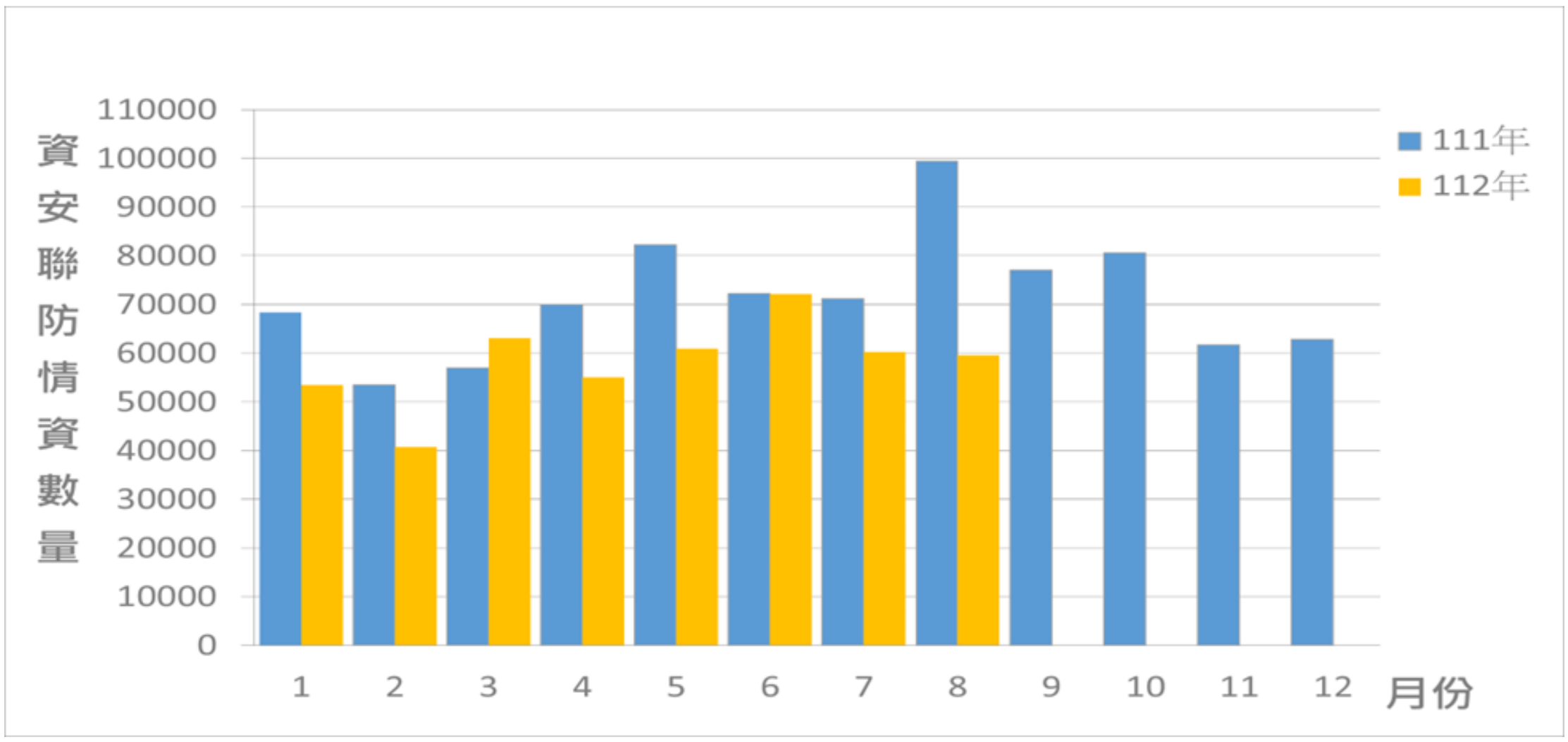

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共130件，本月通報事件較去年減少23.98%，主要係去年同期實兵演練發現多個機關使用存在弱點之第三方應用程式套件CKEdito並遭攻擊成功，今年實兵演練時各機關相關弱點已獲改善。另近1年資安事件通報統計詳圖2。

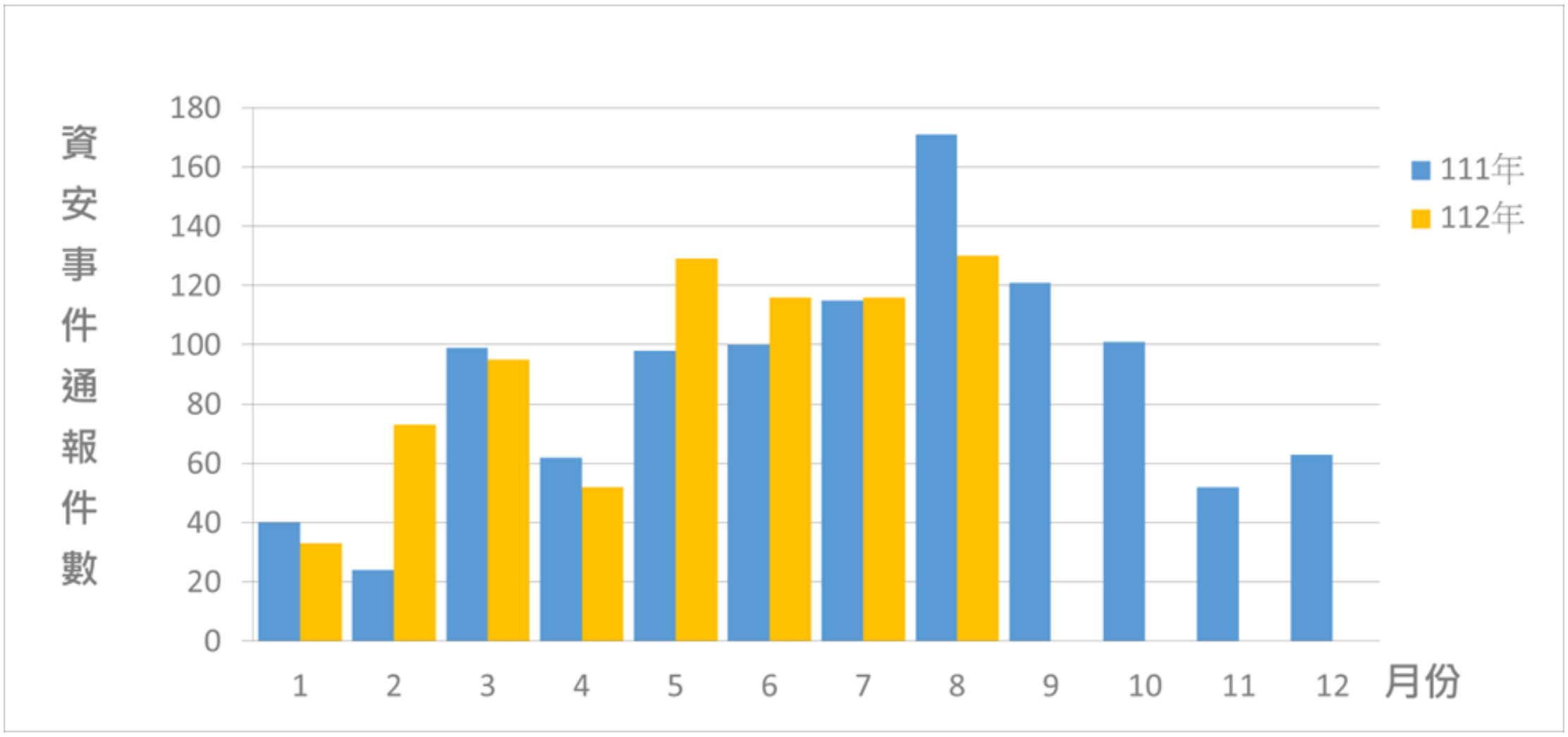

圖2 資安事件通報統計

事後資訊分享

本月接獲某機關偵測發現網站遭上傳網頁木馬程式，經調查發現該網站存有IIS目錄列舉(Microsoft IIS tilde directory enumeration)的漏洞，駭客利用前揭漏洞下載廠商存放在網站的原始碼備份檔，進而發現上傳功能無須身分驗證即可連線存取，並利用該上傳功能植入惡意程式，機關後續已修補漏洞與移除網站原始碼備份檔。

足資借鏡：

部分資訊廠商為維護網站方便性，將網站程式原始碼備份於網站主機，使其暴露於開放網路環境，駭客可利用Dirb目錄掃描等工具掃描網頁路徑進而取得檔案，並藉由分析程式碼探勘漏洞或取得金鑰等機敏資訊，進而竄改以執行未經授權的存取行為。建議對外服務系統應依內部規範，上線前完成資安檢測，定期執行弱點掃描與滲透測式，同時建立程式原始碼管理機制，例如異地備份、管制、存取稽核軌跡紀錄，並對舊版程式原始碼進行備份歸檔等，以降低資安風險。

<國內外重點資安新聞>

一、木馬程式攻擊臺灣地方政府、民間企業及美國軍方相關單位

資安業者於112年3月揭露HiatusRAT的木馬程式鎖定路由器攻擊，主要攻擊範圍為拉丁美洲及歐洲，逾百間企業受害，該木馬程式自112年6月初至8月，逾9成流量鎖定臺灣，遭到鎖定的組織包含半導體業者、化學製造廠商及地方政府，建議相關團體應有安全存取服務邊緣架構或VPN連線，並開啟安全連線以保護傳輸中的資訊。(資料來源：iThome)

二、新資料竊取惡意程式可取得Facebook商業帳號控制權

資安業者近日發現新型網路釣魚攻擊行動，其目的為散播惡意程式用於竊取資料，該程式係利用多個Facebook頁面和使用者傳遞惡意程式，誘騙受害者點選連結後下載一個包含惡意資料竊取程式。資安業者表示因Facebook的使用族群年齡層較高，容易當成攻擊目標，各單位應採取主動措施，教育所屬員工防範相關釣魚攻擊手法。(資料來源：資安人)

<近期重要資安會議及活動>

數位發展部資通安全署擬具資通安全管理法修正草案，為廣蒐各界意見及凝聚共識，已於8月17日、24日、28日及9月8日辦理北、中、南、東區共計4場次工作坊；另因應各界需求，預訂於9月下旬加開2場次，詳細資訊及簡章將另函通知，請有意報名者留意相關訊息。

數位發展部資通安全署於112年7月至11月舉辦「資安菁英人才培訓課程」，分別在臺北舉辦2期、臺南舉辦1期，每期培訓60名資安實戰人才。課程著重於培訓資安事件實戰人才，採實體授課及上機實作。第1期課程已於8月底完訓，並於9月3日辦理網路威脅防禦競賽(Cyber Blue Range Competition)，邀請結訓學員透過競技比賽驗收學習成效。另第2期課程預訂於9月23日完訓、9月24日辦理競賽；第3期課程將在臺北舉辦，報名時間為9月4日至9月18日，請把握機會踴躍報名。

<資通安全長及資訊主管異動情形>

文化部資通安全長於112年8月28日起，原由李連權常務次長兼任，改由徐宜君常務次長兼任。
行政院農業委員會於112年8月1日改制為農業部，資通安全長由陳駿季政務次長兼任，資訊主管由蕭柊瓊司長擔任。

行政院環境保護署於112年8月22日改制為環境部，資通安全長由沈志修常務次長兼任，資訊主管由謝炳輝司長擔任。

國家運輸安全調查委員會資通安全長於112年8月1日起，原由許悅玲副主任委員兼任，改由葉名山副主任委員兼任。

發布單位：資通安全署　　建立日期：2023-09-15　　更新日期：2023-09-15