資通安全網路月報（112年5月）

資通安全網路月報（112年5月）

<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60,949件，分析可辨識的威脅種類，第1名為資訊蒐集類(38%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵攻擊類(35%)，大多是系統遭未經授權存取或取得系統/使用者權限；以及入侵嘗試類(13%)，主要係嘗試入侵未經授權的主機。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，發現近期駭客使用合法電子郵件服務遞送社交工程郵件，並藉由多層式攻擊策略，規避資安防護機制，成功引誘使用者下載惡意程式。經分析，駭客首先利用第三方電子郵件服務寄送社交工程郵件，並將Google雲端硬碟下載網址與通行碼置於正常Office文件附檔，該雲端硬碟空間則存放經通行碼加密保護的壓縮檔(含惡意程式)，誘使使用者下載並以通行碼解壓縮檔案，並執行壓縮檔程式，藉由上述多層式保護機制，規避資安防護檢測，以達到駭侵目的。相關情資已提供各機關聯防監控防護建議。

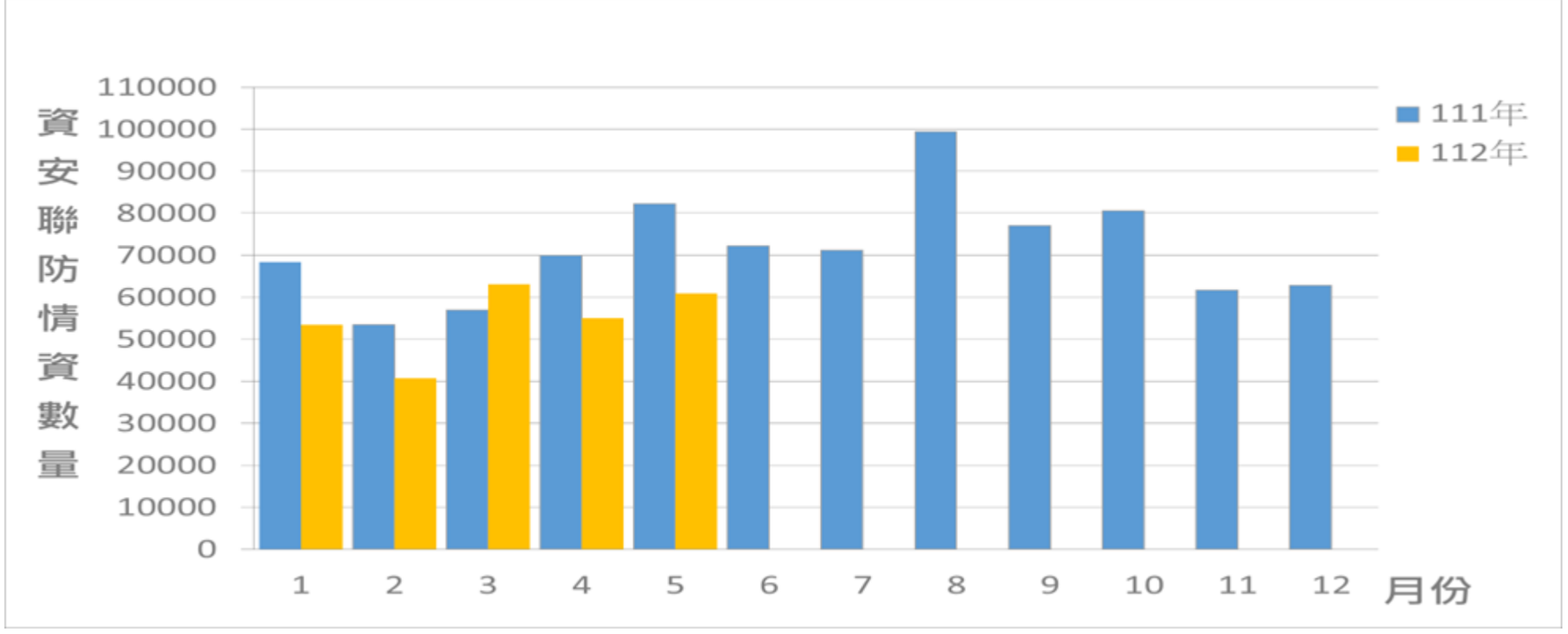

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共130件，為上個月通報事件多，主要為國家資通安全研究院偵測發現多個機關的資訊設備，嘗試下載殭屍網路(Botnet)相關惡意程式，占總通報數量28.46%，經機關調查後發現受駭設備係網通設備(如防火牆或路由器)，疑似因漏洞未及時修補而遭利用。另近1年資安事件通報統計詳圖2。

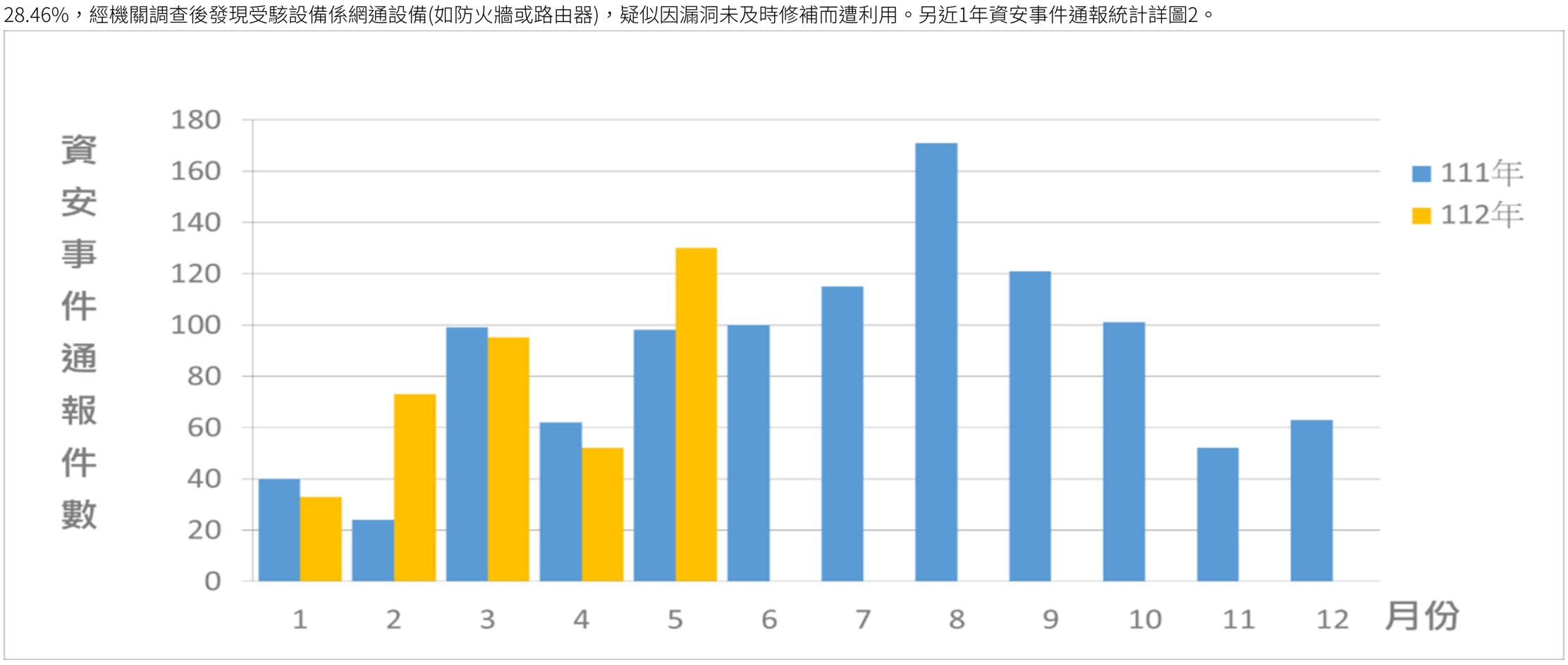

圖2 資安事件通報統計

事後資訊分享

某機關發現網站遭植入惡意程式，初步判斷是駭客利用該網站的檔案上傳頁面功能上傳惡意程式所致。該機關委請資安廠商協同系統建置商進行事件調查，發現該上傳頁面已遭移除，資安廠商進一步檢視相關紀錄，推測系統建置商疑似判斷該頁面無使用需求而逕行移除，導致無法釐清本案事件根因，該機關已重置網站並清查確保未有惡意程式殘留。
足資借鏡：
機關應遵循資通安全責任等級分級辦法之資通系統防護基準，做好「事件日誌與可歸責性」構面相關控制措施，有助於發生資安事件時釐清事件原因，除保存資通系統日誌外，亦可備份當下受駭系統環境，保留完整攻擊紀錄，以利後續事件調查。此外，執行事件調查與處理前，應與系統建置商建立良好溝通，確保彼此理解資安事件調查的需求，以有效進行事件調查與應變處置。

<國內外重點資安新聞>

- 一、網購業者個資外洩

民眾網購後接到市調電話，懷疑係該網購業者個資外洩所致。經該網購業者之主管機關，依據個人資料保護法第22條規定辦理行政檢查後，因該業者未依規定採行適當安全措施，且屆期未改善，已違反個人資料保護法第27條規定，主管機關對該業者處以10萬元罰緩及限期改正，並持續觀察，如未能改善仍將按次處罰。

(資料來源：自由時報、太報)

- 二、系統平台帳號採用共通預設密碼

某機關為民服務系統平台提供給使用者相同的初始帳密，且未強制登入後更改密碼，又因使用者帳號係可公開取得之資料，導致資料曝險。對此，該機關已立即強化該平台帳密管理機制，在使用者登入時要求修改預設密碼，並應符合密碼強度規範，降低資安風險。
(資料來源：民報、機關網站)

<近期重要資安會議及活動>

行政院於112年5月22日舉辦「行政院國家資通安全會報第41次委員會議(擴大會議)」，會議內容重點如下：

- 一、上午場次：由行政院鄭文燦副院長主持，頒發111年網路攻防演練及資安稽核績優機關(構)獎座，並邀請機關分享資安推動策略及重要工作、由駭侵案例談資安防護、機房災害之應處分享、便民服務平台帳密弱點檢討等，並提醒各機關應落實「使用預設密碼登入系統時，應於登入後要求立即變更。」之身分驗證管理控制措施，以強化國家整體資安風險管理作業。

- 二、 下午場次：由數位發展部唐鳳部長主持，邀請機關分享資安推動及防護重點、網路攻擊事件研析及資安威脅情勢分析等，並透過座談交流資安法修法方向。

<資通安全長及資訊主管異動情形>
無

發布單位：資通安全署　　建立日期：2023-06-13　　更新日期：2023-06-13