資通安全網路月報（112年10月）

資通安全網路月報(112年10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42,972件，分析可辨識的威脅種類，第1名為資訊蒐集類(49%)，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(23%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(10%)，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，發現近期某國家核廢水排放議題引起全球關注，駭客利用該國民間公司的電子郵件帳號，以核汙水爆料為由，寄送夾帶惡意壓縮檔的社交工程電子郵件，針對特定政府機關進行社交工程郵件攻擊，相關情資已提供各機關聯防監控防護建議。

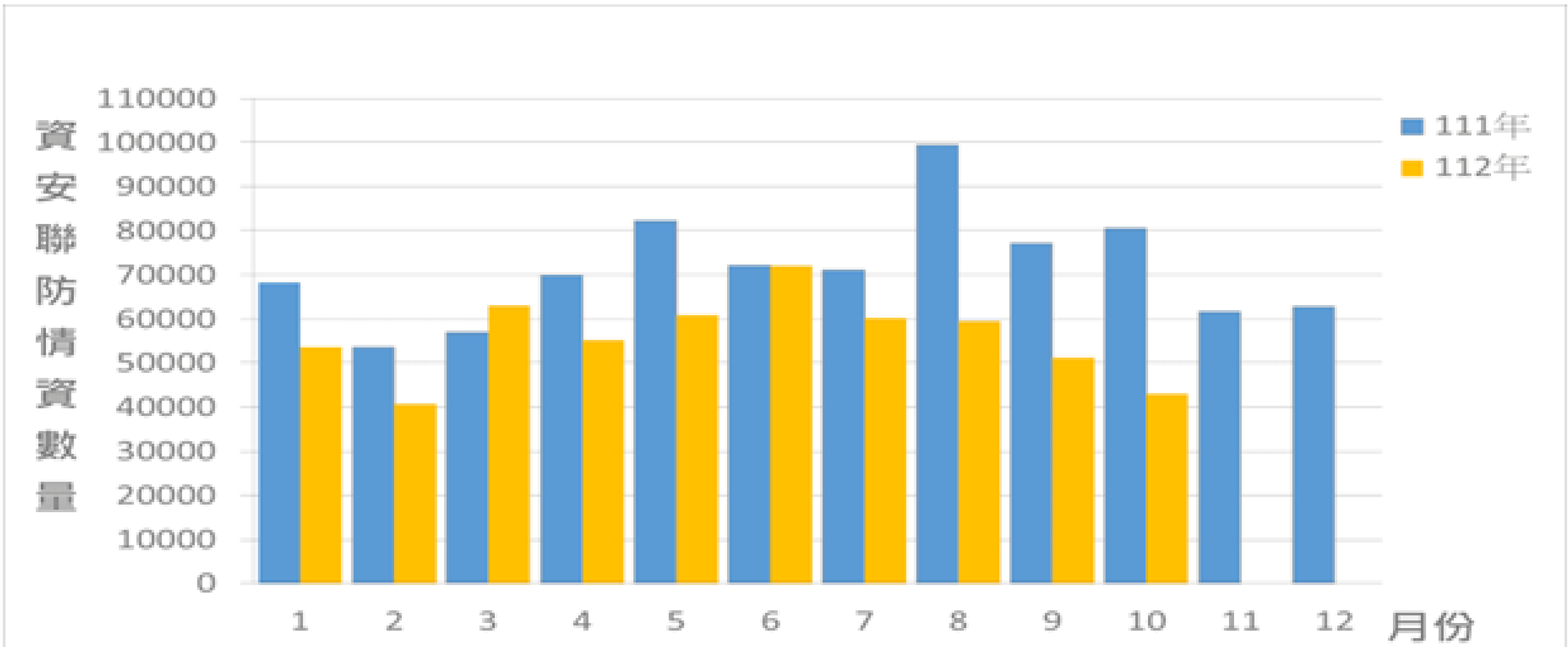

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共54件，較去年同期減少46.53%，主要是殭屍網路攻擊相關事件數量減少，較去年同期減少約80.95%。另近1年資安事件通報統計詳見圖2。

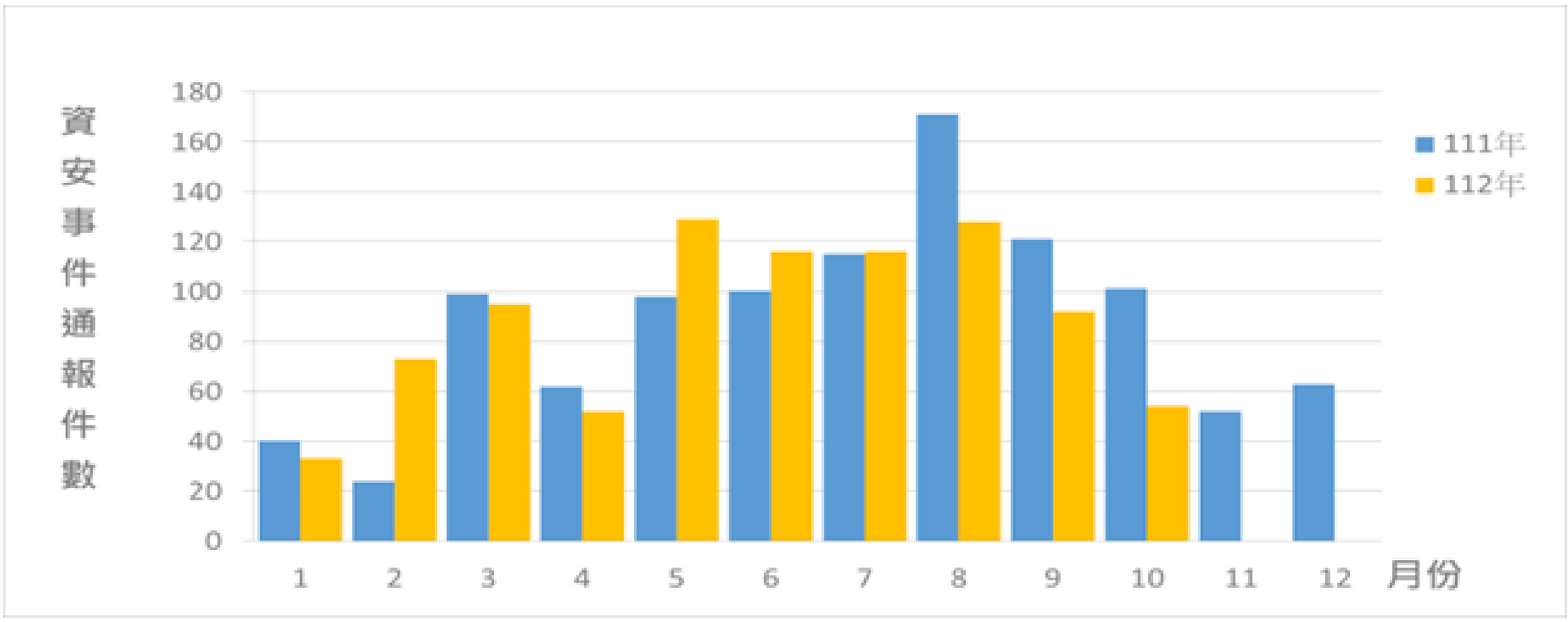

圖2 資安事件通報統計

事後資訊分享

本月國家資通安全研究院偵測發現某機關有惡意程式連線情形，經機關調查發現係同仁因業務需求，自行下載安裝通訊軟體於公務電腦，惟未於官方網站下載正式版本，導致遭植入惡意程式並對外進行連線。該機關已將受駭電腦重新建置，並加強內部資安宣導，請同仁避免在公務設備安裝非公務用軟體，如因業務需要，應於官方網站下載，以避免下載夾帶惡意程式的軟體安裝檔。

足資借鏡：

通訊軟體已成為工作溝通的主要工具，駭客亦藉此趨勢，將熱門通訊軟體夾帶惡意程式製作成安裝檔，並透過網路大量散播。使用者搜尋軟體工具時，若未多加注意檔案來源，即可能下載夾帶惡意程式的安裝檔，導致駭客成功侵入使用者電腦。機關應建立內部軟體下載與安裝相關規範及限制措施，要求人員不應於公務設備安裝非授權或非公務用的軟體，若因業務需要安裝軟體，應至該軟體的官方網站下載及安裝，以降低設備遭入侵的風險。

<國內外重點資安新聞>

1. 18國資安專家匯聚臺灣，展開跨國資安攻防演練CODE 2023，臺灣奪得冠軍

    112年10月18日至20日，數位發展部資通安全署舉辦跨國網路攻防演練(Cyber Offensive and Defensive Exercise，CODE 2023)，吸引了18個國家的資安組織參與，臺灣團隊表現出色，獲得第1名佳績。

    本次同時舉辦前瞻資安探索會議(Advanced Cybersecurity Exploration Conference)，邀集世界各地學者、業界及政府代表，聚焦兩大資安議題：關鍵基礎設施安全、新興技術風險管理，探索相關因應策略或方案，以提升國際間的資安聯防及合作。

    (資料來源：中央社，Yahoo)

2. 提升國人資安意識，數位發展部資通安全署攜手國家資通安全研究院推動資安系列競賽

    培育人才是資安精進最重要的核心，數位發展部資通安全署為擴大充實國內的資安人才庫，自95年起開始著手舉辦「資安技能金盾獎」競賽，透過高手競技的方式，提升學生對於資安領域的興趣，並提升攻防實戰的技術能力。另資安系列競賽不僅在挖掘資訊相關科系人才，更重要的是讓資安意識能廣泛深植到學子心中，讓更多人都能正視資安議題的重要性，因此還規劃了「資安海報」與「資安影片」的徵件活動，期許能讓非本科系的學生，透過集思廣益、激發創意的方式，更深入地了解資安的概念。

    (資料來源：數位時代)

3. 某公司零時差漏洞允許駭客取得最高權限

    某公司112年10月16日揭露已遭駭客攻擊的零時差漏洞(CVE-2023-20198)，該漏洞位於該公司網通設備作業系統的網頁使用者介面(Web User Interface，Web UI)，當曝露於公開網路或不可靠的網路時，就可能遭到濫用。該漏洞允許駭客存取裝置並建立新使用者帳戶，其CVSS漏洞風險評分高達10，遭成功攻擊將讓駭客取得完整管理權限，控制受駭的裝置。在未修補前揭漏洞前，建議客戶應在所有面對公開網路的系統上關閉HTTP Server功能。

    (資料來源：iThome)

<近期重要資安會議及活動>

資通安全管理法修正草案於112年9月22日公告在公共政策網路參與平臺(眾開講)，透過平臺機制公開徵詢民眾意見，並自112年10月17日起於北區辦理6場修法說明會，擴大蒐集各界意見，11月規劃有10場修法說明會分別於中、南、東區辦理，詳細簡章資料已另函送各機關(構)，歡迎踴躍報名。

112年第2次政府資通安全防護巡迴研討會112年11月20日至30日分別在北、中、南、東區共辦理8場次，請鼓勵資安專職(責)人員踴躍報名參加。

<資通安全長及資訊主管異動情形>

核能安全委員會資通安全長於112年10月5日起，原由林立夫副主任委員兼任，改由張欣副主任委員兼任。

國家科學及技術委員會資訊主管於112年10月4日起，原由薛大勇處長兼任，改由周子元處長擔任。

發布單位：資通安全署　　建立日期：2023-11-15　　更新日期：2023-11-13