資通安全網路月報（112年11月）

資通安全網路月報(112年11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49,099件，經分析可辨識的威脅種類前3名，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(27%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(11%)，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，發現近期駭客寄送夾帶點擊追蹤連結與惡意短網址的社交工程電子郵件，藉由貼近業務的主旨，誘騙承辦人開啟可疑連結並下載惡意檔案，對政府機關進行社交工程電子郵件攻擊。相關情資已提供各機關聯防監控防護建議。

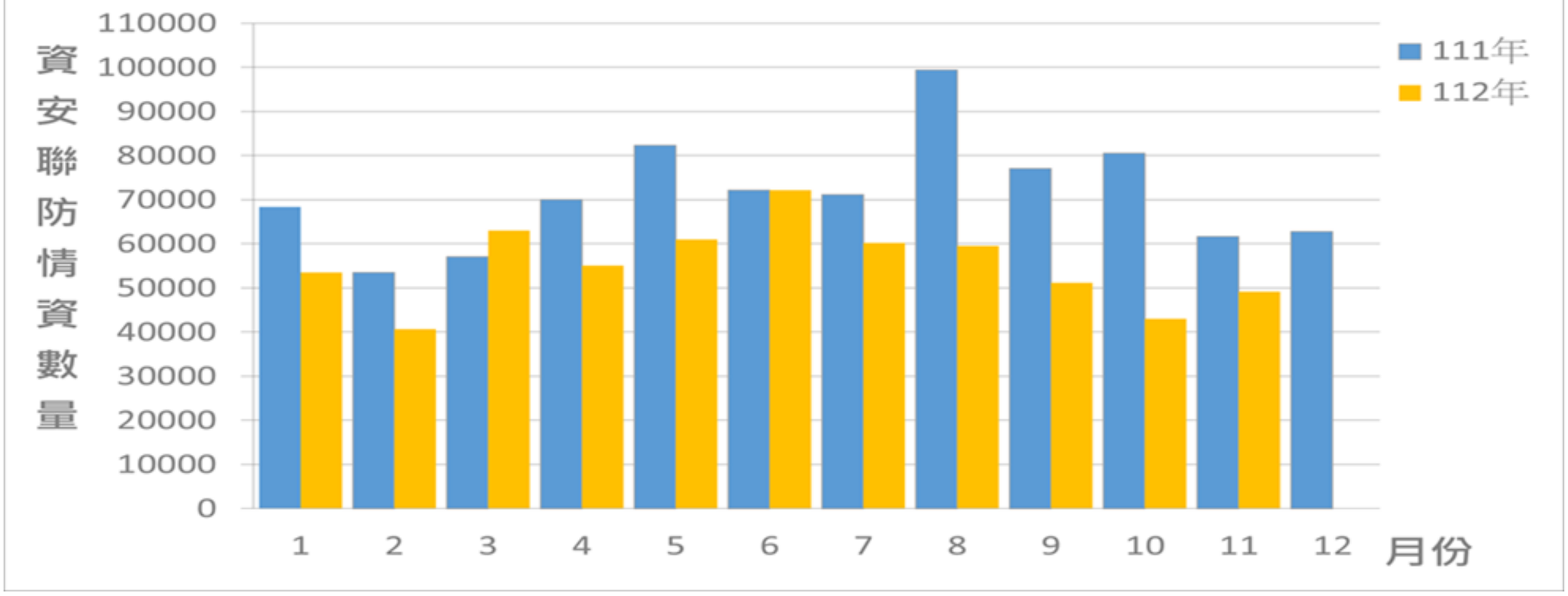

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共86件，較去年增加65.38%，國家資通安全研究院偵測發現部分機關資訊設備，嘗試下載惡意程式或產生符合惡意程式行為的連線，占總通報數量39.53%，經前揭機關調查後發現異常連線為監視器設備。另近1年資安事件通報統計詳圖2。

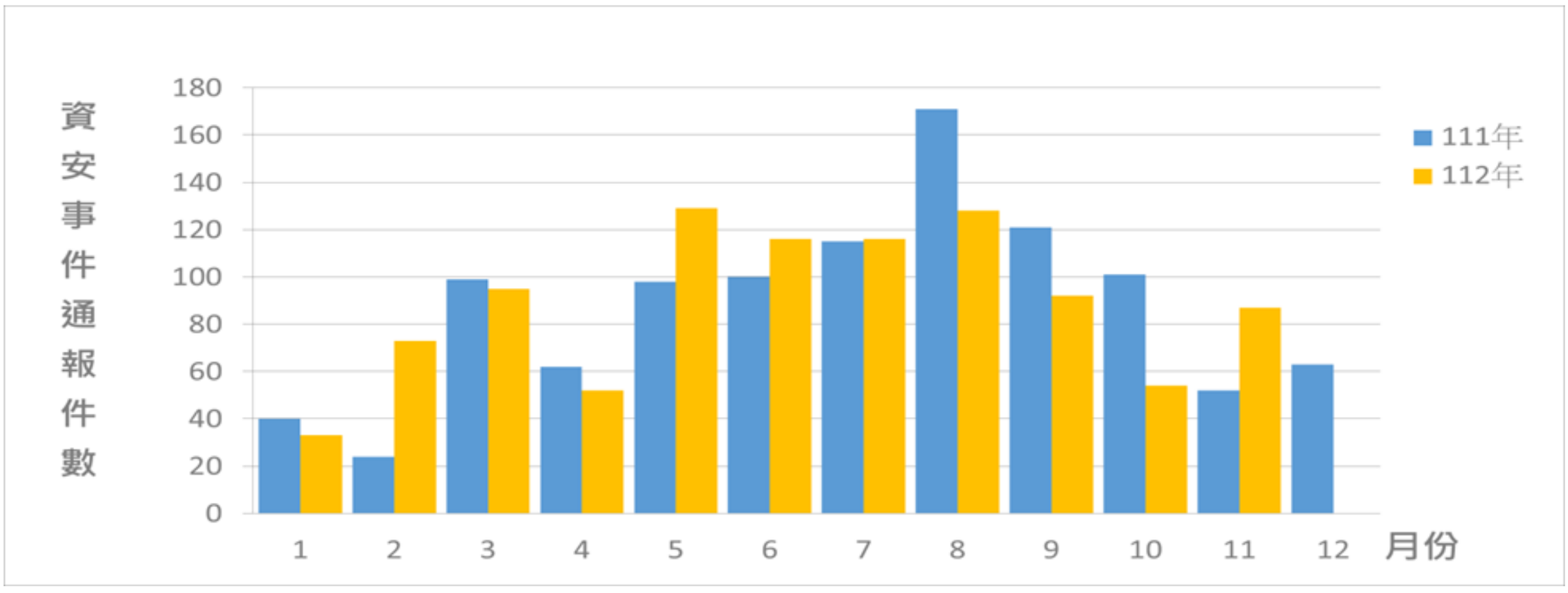

圖2 資安事件通報統計

事後資訊分享

本月偵測發現某機關公文系統曾連線下載惡意xml檔案，經國家資通安全研究院研究人員檢測後，研判與Apache ActiveMQ於10月揭露的重大漏洞(CVE-2023-46604，CVSS Score 10)相關，隨即發布資安警訊通知該機關。該機關原表示受駭系統未使用前揭軟體，惟經維護廠商進一步檢視發現該系統的功能模組確實有使用ActiveMQ元件，且其版本屬重大漏洞影響範圍，已協助機關進行版本更新作業。

足資借鏡：

機關網站常見透過第三方套件與軟體開發系統功能或服務，以縮短網站建置時間，惟第三方套件或軟體亦可能存在資安漏洞。建議機關應盤點及注意網站使用的套件或軟體，並透過定期檢視與弱點掃描等安全性檢測，掌握系統版本更新與安全狀態，及時完成漏洞修補作業，若因故無法及時修補漏洞(如原廠尚未釋出更新版)，應即採取相關防護措施，降低弱點遭利用導致網站遭入侵的風險。

<國內外重點資安新聞>

1. 某銀行驚傳1.4萬客戶資料外洩，金融監督管理委員會(簡稱金管會)公布調查結果列4大缺失，依銀行法重罰1千萬

    某銀行經金管會查核指出未明訂定期變更電腦密碼、未訂定可攜式設備管控規範、未留存個人資料使用軌跡及未監控出資安軟體漏洞並確認其軌跡執行情形等4項重大缺失。金管會對該銀行缺失開罰1千萬，重點在於未確實執行內部控制制度，且事後缺乏相關資訊可追查。

    此外，金管會亦提出全面檢討本案所涉當責人員及主管責任、盤點全行涉及個資的各類電腦系統是否均建置留存個資使用稽核軌跡、建置各類應用系統測試稽核機制及充實稽核人員資訊系統稽核能力並委託會計師辦理全行個資保護專案查核等4項監理要求。

    (資料來源：iThome，資安人)

2. 某公司遭駭客攻擊！顧客資料恐被利用於詐騙示警

    某公司11月29日於臺灣證券交易所發布重大訊息，表示其遭受網路駭客攻擊，並說明已全面啟動相關防禦機制，以及委請外部資安公司技術專家共同處理，依法通報相關部門，並持續加強資通安全管理。該公司同時透過官網、簡訊、電子郵件及其他必要方式加強並提醒旅客反詐騙警語，持續強化網路資訊與資安管控，以確保資料安全。

    (資料來源：iThome，Yahoo)

3. 某公司遭遇網路攻擊，44萬用戶、合作夥伴、員工個資恐外洩，臺灣也有用戶資料曝險

    某通訊軟體公司臺灣用戶眾多，此事故引起國內各界關注。該公司11月27日向資安主管機關說明，並依法通報個資外洩。目前尚未發現個人或群組的通訊內容，以及信用卡、銀行帳號等金融資料外洩的情形。

    該公司已強制重設員工內部系統密碼及二階段認證機制(Two-Factor Authentication)，並發出訊息通知相關當事人。數位發展部數位產業署也要求該公司配合行政檢查，持續強化資通安全。

    (資料來源：iThome,Yahoo)

<近期重要資安會議及活動>

資通安全管理法修正草案於11月20日完成預告，數位發展部資通安全署刻正彙整公共政策網路參與平臺(眾開講)及修法說明會獲得的回饋意見，並依各界意見調修法案內容，後續將送數位發展部及行政院進行法案審查後，送請立法院審議。

<資通安全長及資訊主管異動情形>

本月無。

發布單位：資通安全署　　建立日期：2023-12-15　　更新日期：2023-12-15