資通安全網路月報（112年2月）

資通安全網路月報（112年2月）

<近期政策重點>

依資通安全責任等級分級辦法第3條規定，各機關應每2年提交自身、所屬、所管、所監督及所轄之資通安全管理法納管對象之資通安全責任等級，提報主管機關核定(或備查)，本次作業已啟動，請各機關於112年3月31日前完成提報。

<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40,678件，分析可辨識的威脅種類，第1名為入侵嘗試類(38%)，主要是嘗試入侵未經授權的主機；其次為資訊蒐集類(37%)，主要係透過掃描、探測及社交工程等攻擊手法取得資訊；以及入侵攻擊類(14%)，大多為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。

進一步彙整分析聯防情資資訊，發現駭客偽冒政府機關，透過寄送通行碼到期通知進行社交工程電子郵件攻擊。駭客在惡意郵件內文提示通行碼已到期的訊息，並直接將釣魚網頁(HTML文件)作為附檔，誘使收件人點擊附件釣魚網頁，輸入帳號通行碼並回傳至駭客端，藉此竊取收件人的敏感資訊。相關情資亦於聯防監控月報提供防護建議，提供各機關參考。

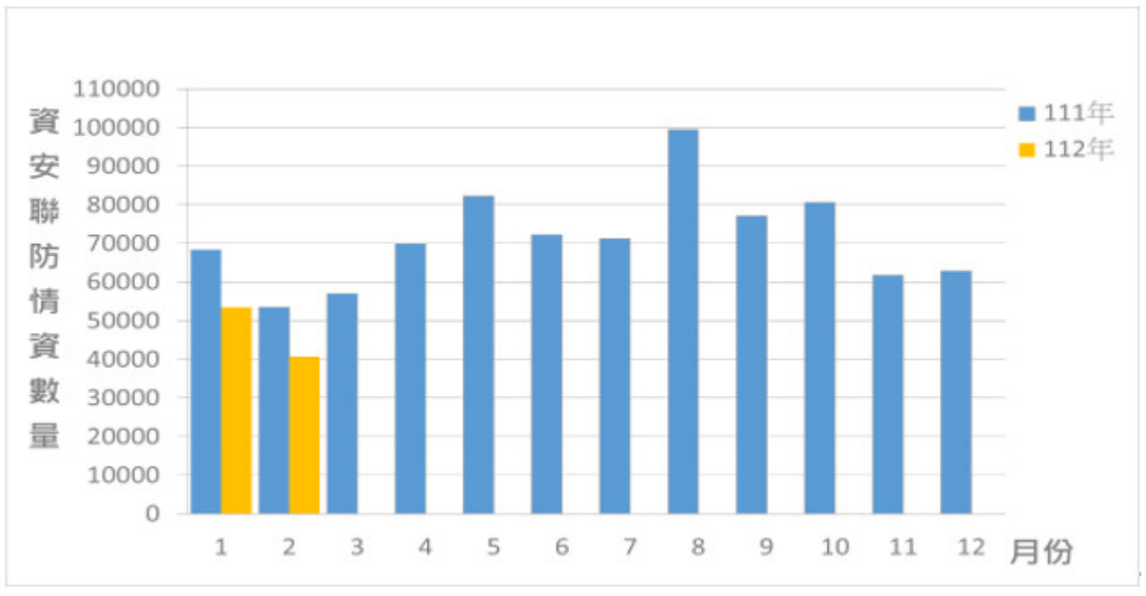

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共73件，為去年同期通報件數3.04倍，主要是國家資通安全研究院偵測發現多個機關的資訊設備，出現疑似殭屍網路(Botnet)惡意程式連線行為，占總通報數量23.29%，經調查後發現係網通設備連線異常所致(如：路由器或防火牆)。另近1年資安事件通報統計詳見圖2。

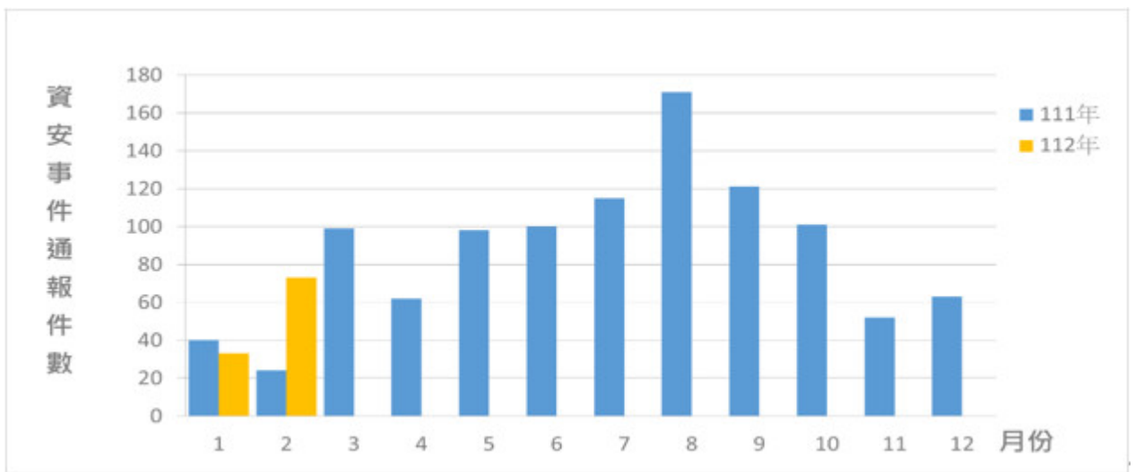

圖2 資安事件通報統計

事後資訊分享

本月發現多個公務機關對外進行殭屍網路相關異常連線行為，經調查後發現連線設備為網通設備(路由器或防火牆)，再檢視該設備發現久未進行韌體與軟體更新，推測可能是舊版本存在漏洞遭利用，目前已更新設備之軟體版本，並將原廠停止支援更新(EOS)之設備進行汰換，後續觀察確認未再觸發異常連線行為。

足資借鏡：網通設備(如路由器、防火牆及物聯網設備等)常因軟體或韌體未即時更新而容易存在資安風險，囿於設備本身容量限制，導致難以保存相關紀錄。建議機關應定期進行設備盤點，並更新韌體與軟體，以及時修補已知漏洞，同時留意產品支援版本更新情況，若產品已停止支援更新，應評估汰換或採取相關防護措施。此外，亦可建立健全的日誌保存機制，以利異常事件發生時之根因調查。

<國內外重點資安新聞>

一、汽車租賃服務業者資安事件

1月底某汽車租賃公司資料庫曝險事件被揭露，公路總局在2月9日發布公告，確認該公司未依「個人資料保護法」與「汽車運輸業個人資料檔案安全維護計畫及處理辦法」辦理，已要求再提報資訊安全相關措施。

2月初，另一家汽車租賃公司亦有用戶資料曝險問題，係因其提供的APP中，用戶查詢本身租車單據的連結頁面，公開且未加密保護所致。公路總局已請該公司依限改善，並要求提交複查報告。

(資料來源：iThome、聯合新聞網)

二、百貨業資料外洩事件

2月16日某百貨向會員發送防詐簡訊，並要用戶修改密碼，而後有人於駭客論壇BreachForums聲稱竊取了某百貨內部資料與90萬用戶個資。2月24日經濟部商業司也對此事件發出公告，由經濟部商業司、數位發展部國家資通安全研究院、資訊工業策進會及內政部警政署組成行政調查小組，要求業者完成個資防護自評、個資安全稽核檢查，以釐清事故原因並立即改善。

(資料來源：ETtoday新聞雲、中華民國經濟部官網)

<近期重要資安會議及活動>

111年行政院國家資通安全會報稽核結束會議於112年2月3日召開，由該會報副召集人唐鳳主持，並邀請年度稽核委員與會。

<資通安全長及資訊主管異動情形>

行政院原子能委員會資通安全長自112年2月3日起，原由張靜文政務副主任委員兼任，改由林立夫政務副主任委員兼任。

發布單位：資通安全署　　建立日期：2023-03-15　　更新日期：2023-03-15
