資通安全網路月報（111年11月）

資通安全網路月報（111年11月）

<近期政策重點>

數位發展部已於111年11月28日修正「各機關對危害國家資通安全產品限制使用原則」，明確增訂各機關自行或委外營運，提供公眾活動或使用之場地，不得使用危害國家資通安全產品，且機關應將限制事項納入委外契約或場地使用規定中

<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61,687件，分析可明確辨識的威脅種類，第1名為掃描刺探類(49%)，係Portsweep掃描行為；其次是入侵攻擊類(23%)，主要為網頁入侵行為；以及政策規則類(15%)，主要為單一帳號持續登入失敗。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，近期資安公司揭露Fortinet網通設備與Microsoft Exchange電子郵件系統漏洞，技服中心發現有多個政府機關使用相關設備，恐遭駭客利用漏洞進行攻擊，已發布警訊通知潛在風險機關立即進行安全性更新。相關情資亦於聯防監控月報提供防護建議供政府機關參考。

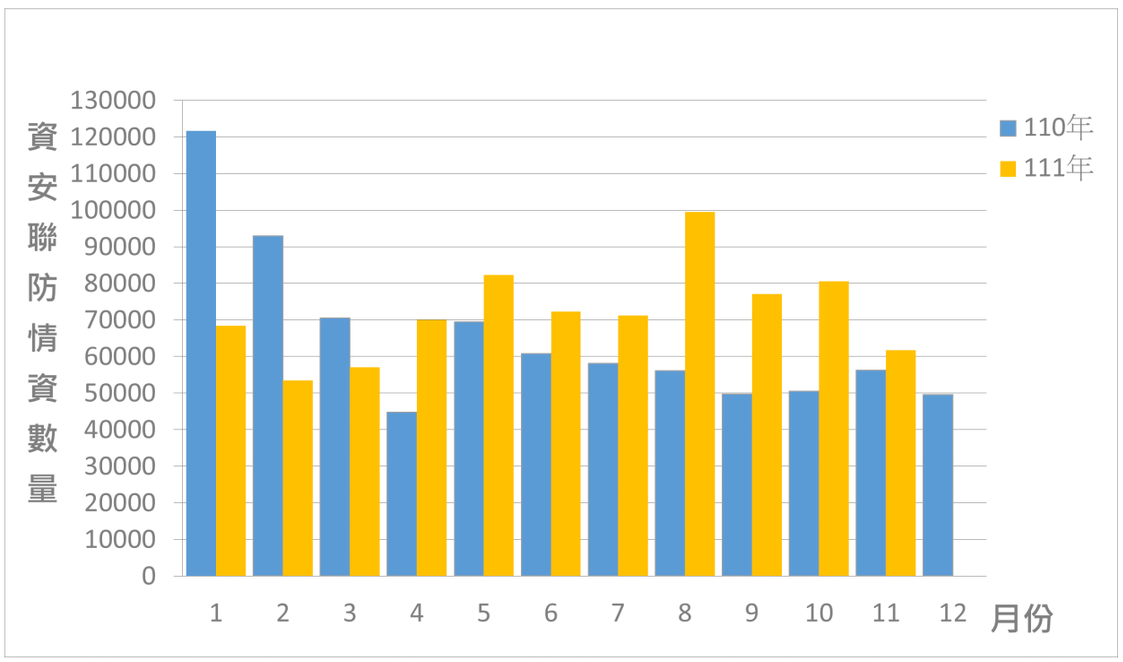

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共53件，較上個月減少47.52%，主要係上個月技服中心偵測發現多個機關監視器設備嘗試下載殭屍網路(Botnet)相關惡意程式，本月偵測殭屍網路相關事件下降71.43%，占通報事件11.32%。另近1年資安事件通報統計詳見圖2。

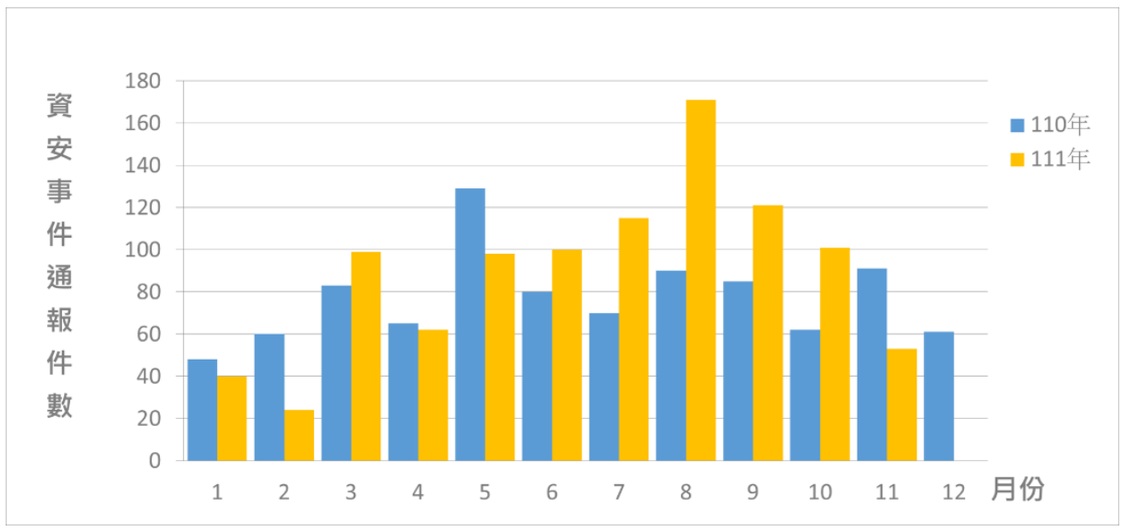

圖2 資安事件通報統計

事後資訊分享

本月發現某機關電子郵件帳號密碼外洩事件，經機關調查發現外洩帳號為業務單位早期網站客服信箱，因網站改版，業務單位申請新客服信箱，原帳號閒置且無人管理，密碼設置亦不符合機關管理原則(長度至少8碼，含英文大寫、小寫、數字及特殊符號)，遭駭客暴力破解成功，後續該機關已將帳號停用，並進行內部電子郵件帳號清查。

足資借鏡：電子郵件為現代資訊交換主要工具之一，常因資訊人員管理不當或使用者資安意識不足，遭駭客取得郵件帳號密碼成為攻擊跳板，除竊取郵件資料，亦用於發送釣魚信件。機關應落實資通安全責任等級分級辦法之附表十資通系統防護基準中對於帳號管理採取相關控制措施，建立帳號管理機制(包含停用與刪除程序)，並定期檢視帳號使用情形，以避免閒置帳號遭駭客惡意利用。

<國內外重點資安新聞>

一、TWCERT 2022台灣資安通報應變年會邁入第六屆，聚焦我國資安情勢發展
由財團法人台灣網路資訊中心(TWNIC)、台灣電腦網路危機處理暨協調中心(TWCERT/CC)主辦、數位發展部指導的TWCERT 2022台灣資安通報應變年會於11月15日舉辦。
現場邀集國內外產官學研及國際專家參與，以「資安韌性，營運永續」為題，探討全球資安重大議題，採國際座談會與專題演講形式共同交流資安聯防之實踐，關注資安威脅趨勢發展，期強化國家整體數位韌性與落實資安治理。
(資料來源：TWCERT/CC、資安人、科技新報)

二、Fortinet本月公告《2023 全球資安威脅預測》
網路資安廠商Fortinet於11月初公布《2023全球資安威脅預測》，指出5點資安威脅趨勢，包含「網路犯罪即服務(Cybercrime-as-a-Service，CaaS)」、偵查即服務(Reconnaissance-as-a-

Service)、洗錢即服務(Money Laundering-as-a-Service，LaaS)、虛擬城市內的網路犯罪、以及Wiper惡意軟體商品化。建議企業掌握網路犯罪者的動機與攻擊手法，擬定可降低資安管理複雜性之策略，即時偵測網路攻擊，阻止潛在威脅。

(資料來源：iThome、數位時代)

三、美國聯邦通訊委員會FCC宣布禁止5家中國產品進口及銷售

美國聯邦通訊委員會(Federal Communications Commission，FCC)於11月25日宣布華為、中興通訊、海能達、海康威視、大華等5家中國企業電信產品和視訊監控設備，除經特別許可，不得進口或於美國境內進行銷售。

美國聯邦傳播委員會主席Jessica Rosenworcel表示，該新令是為了確保國家安全，避免具潛在風險的網通設備於境內流通，造成國家安全上的危害與威脅。

此外，FCC也更新海底電纜執照的頒發流程，終止中國在美國提供或運營電信服務的權利，並進一步強化IoT設備及連網安全設備的安全審查。

(資料來源：FCC、iThome、科技新報)

發布單位：資通安全署　　建立日期：2022-12-15　　更新日期：2022-12-15