資通安全網路月報（112年7月）

資通安全網路月報（112年7月）

<近期政策重點>

一、資通安全責任等級A、B級公務機關應於本(112)年8月23日導入端點偵測及應變機制(EDR)，另依「政府領域聯防監控作業規範」，應即時回傳資安監控及情資分析資料，並於每月5日前回傳上個月之相關設備狀況，請各機關注意辦理。

二、資通安全責任等級C級納管機關應於本年8月23日前導入資通安全弱點通報系統(VANS)，並請注意以下作業重點：

(一) 導入範圍應包含機關內支持核心業務持續運作之資通系統主機與電腦；關鍵基礎設施提供者導入範圍，至少應涵蓋關鍵資訊基礎設施及營運持續運作必要之相關資通系統。

(二) 有關資訊資產上傳頻率，除重大弱點通報或大量資產異動外，建議每月至少定期上傳1次，如採系統化介接方式可增加上傳頻率；並應針對發現弱點設定修補期限，未修補前應加強防護及異常偵測，以確保弱點管理之即時性及有效性。

三、為協助機關強化委外資通系統資安控管作業，行政院於111年5月26日訂頒「資通系統籌獲各階段資安強化措施」試行1年，資安署已函請各機關於112年9月1日前提供修正意見，以利完善相關規定及實務運作。

<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60,203件，分析可辨識的威脅種類，第1名為資訊蒐集類(45%)，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(26%)，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(17%)，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，發現近期二維條碼網路釣魚(Quishing)攻擊活動漸增，駭客使用圖像的二維條碼(QR Code)進行社交工程電子郵件攻擊，藉以躲避機關資安偵測，提升攻擊成功率。駭客偽冒政府機關內部郵件，利用「智慧手機移動端系統上線」等主旨，引誘收件人以行動裝置掃描惡意二維條碼後，連線至登入頁面要求收件人輸入帳號與通行碼，進而達到竊取收件人機敏資訊的目的，相關情資已提供各機關聯防監控防護建議。

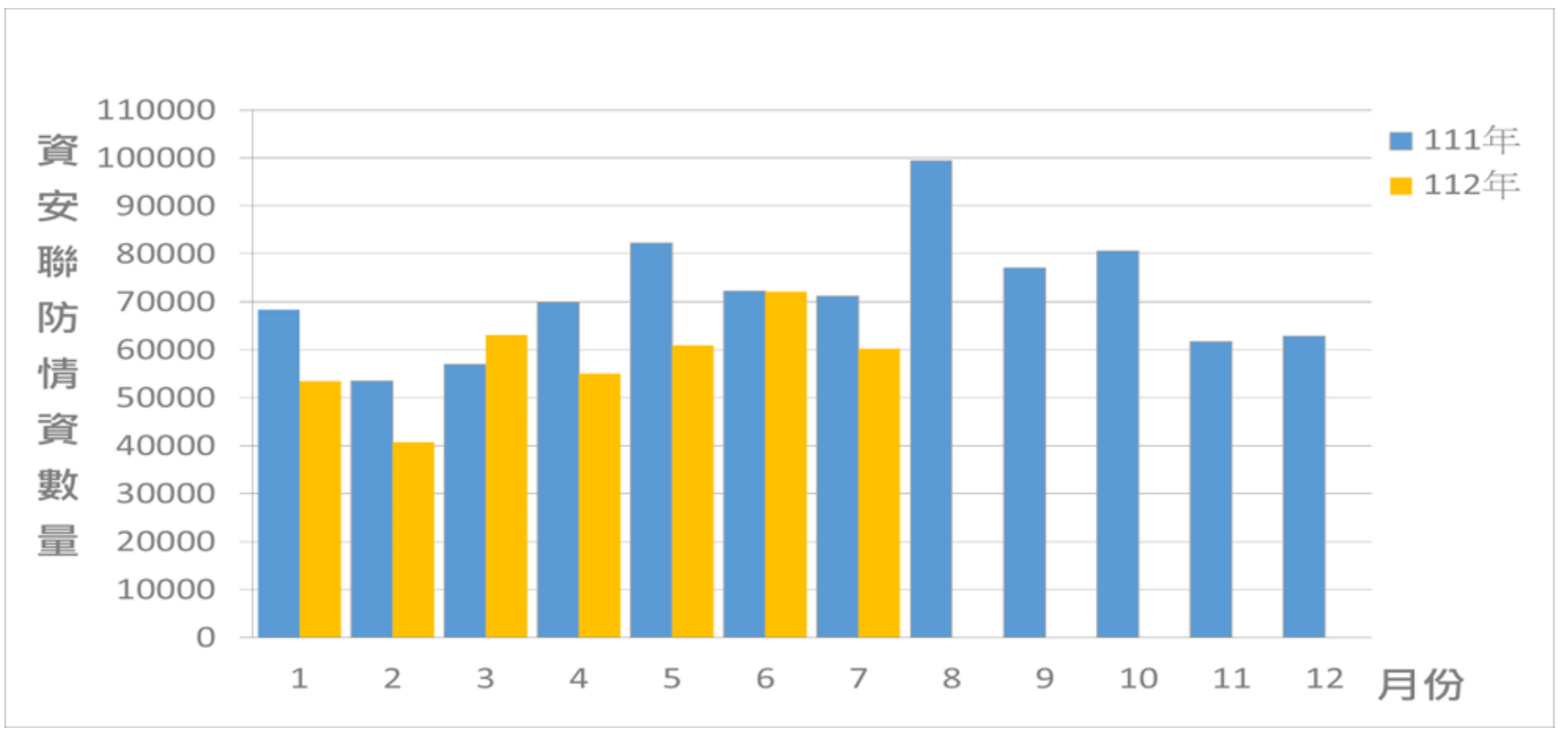

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共117件，其中因網際網路服務供應商(ISP)業者問題造成機關對外網路中斷事件，占「設備問題」事件類型數量25%。另近1年資安事件通報統計詳圖2。

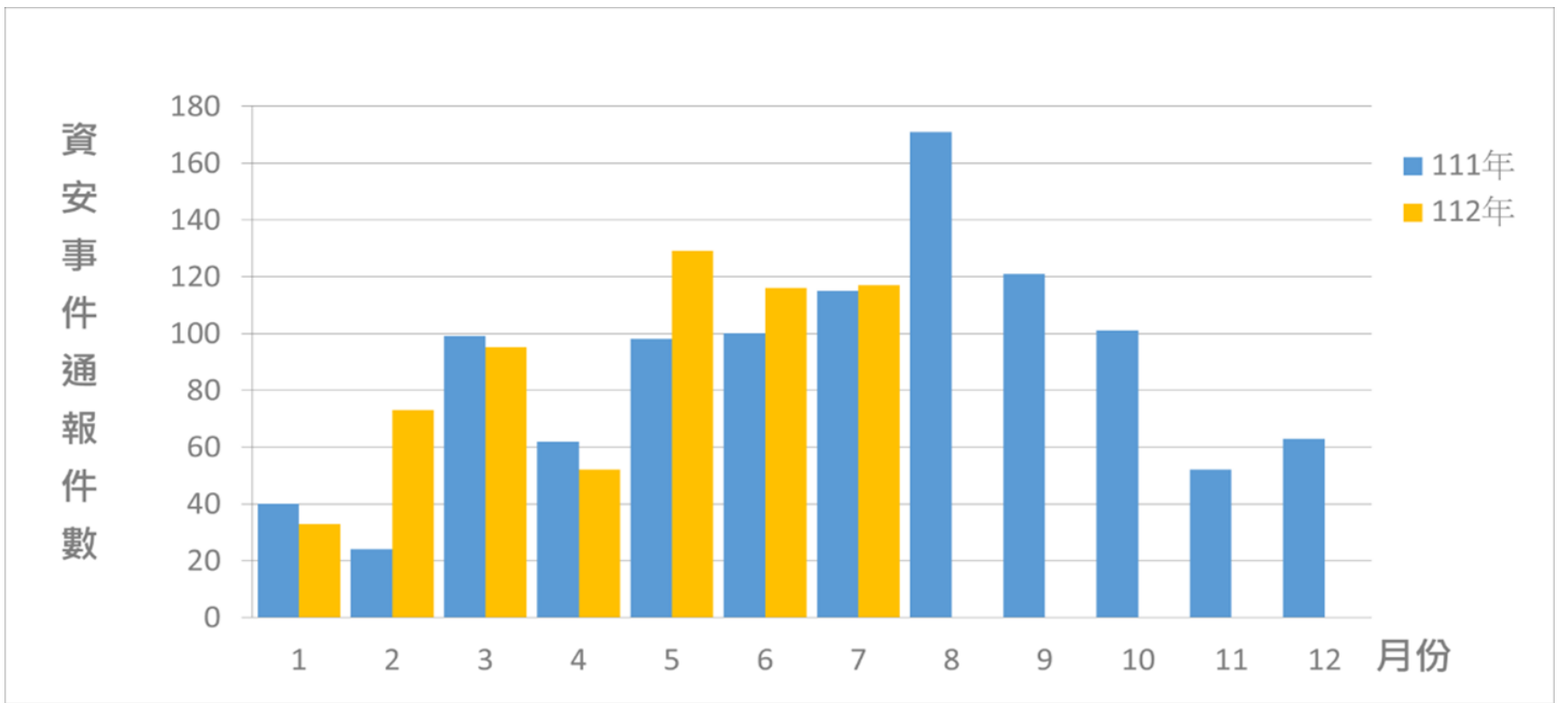

圖2 資安事件通報統計

事後資訊分享

本月接獲某機關通報其多部觀測站主機遭勒索軟體攻擊，經調查後發現攻擊來源為觀測站維護商電腦，駭客成功登入維護商電腦，並以該設備做為跳板，陸續透過遠端桌面連線多台觀測站主機進行攻擊，進一步分析該機關部分觀測站主機設置於偏遠地區，較難實地維護，爰開放維護商連線維護。該機關已變更受駭設備帳號密碼，同時限制維護廠商電腦存取，並將觀測站主機之設備集中設置於機關內進行管控，降低遭入侵風險。

足資借鏡：

機關開放委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理，若有執行需求，應依資通安全管理法施行細則第4條及資通安全責任等級分級辦法附表十有關遠端存取規定辦理，並建立及落實管理機制。此外，不同資訊設備應避免設置相同帳號密碼，以降低資安風險。

<國內外重點資安新聞>

一、公司遭冒名發送用戶簡訊，數位發展部打造政府專屬短碼簡訊平臺供民眾識別

簡訊詐騙議題頻傳，近日發現某公司遭假冒名義傳送用戶詐騙簡訊。遭冒名公司在官網指出，有假借該公司名義發送「提醒用戶未繳費、通知停止服務等訊息，並提供假網址、假檔案連結等」之簡訊及電子郵件，誘使用戶提供信用卡個資及下載檔案，呼籲民眾勿相信此類詐騙簡訊，應前往其官網查詢。

由於此類事件仍持續不斷且零星發生，數位發展部表示，將從簡訊源頭號碼端做管理，打造政府專屬短碼簡訊平臺，希望讓民眾識別簡訊是否來自政府機關。

(資料來源：iThome 、某公司官網 1、某公司官網2 、中央社)

二、日本最大港「名古屋港」遭勒索軟體攻擊，物流癱瘓2天

貿易量占日本總貿易量10%、每年處理超過200萬個貨櫃及1.65億噸貨物的名古屋港貨櫃碼頭，在當地時間112年7月4日上午6時半左右，主管貨櫃上下貨及港口運作的系統無法作業，負責營運的名古屋港運協會發現系統遭勒索軟體攻擊。

這次事件，名古屋港運協會電腦感染勒索病毒被加密，約100台印表機遭劫持列印系統感染勒索軟體的通知，並要求贖金。名古屋港當局未支付贖金，並自行掃毒修復系統，至112年7月6日確認系統已無病毒，恢復裝卸工作。歷經這次駭客攻擊，當局決定加強系統資安防護，避免類似情形再次發生。

(資料來源：資安人 、iThome 、yahoo新聞)

<近期重要資安會議及活動>

數位發展部資通安全署擬具資通安全管理法修正草案，為廣蒐各界意見，將於112年8月底進行草案預告，並於112年8月17日、24日、28日及9月8日分別在北、中、南、東區辦理4場次工作坊，已函邀產官學界專家進行意見交流，彙整相關意見及凝聚共識，俾完善本次修法作業。

<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：2023-08-15　　更新日期：2023-08-15