資通安全網路月報（111年10月）

資通安全網路月報（111年10月）

<近期政策重點>

近來各機關接獲資安預警警訊(EWA)或入侵事件警訊(INT)簡訊時，對於後續通報應處混淆一事，再次重申其警訊定義及應處作為如下：

EWA：機關收到此類警訊時，請機關依警訊內容，先進行檢視，若發現入侵事實(機密性、完整性或可用性受影響)，應依資通安全管理法執行資安事件通報作業。

INT：機關收到此類警訊時，表示機關已遭受資安事件影響，須循機關內部通報程序陳報外，並應依資通安全管理法執行資安通報作業。

前揭2類警訊差異在確認是否遭駭侵，EWA警訊係請機關先確認有無遭駭事實，若屬實，應即通報資安事件；INT警訊表示機關被發現已有駭侵事實，請機關儘速通報資安事件。

<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80,510件，統計近1年情資數量分布詳圖1。經分析前揭情資，可明確辨識的威脅種類，第1名為入侵攻擊類(39%)，主要是SQL資料隱碼攻擊；其次為掃描刺探類(36%)，係外部主機執行掃描探測攻擊；以及政策規則類(12%)，主要為單一帳號持續登入失敗。

經進一步分析聯防情資彙整資訊，發現近期駭客多次以「業務諮詢」相關主旨與郵件內容，將內含惡意壓縮檔的社交工程電子郵件寄予政府機關人員，誘騙目標收件人開啟惡意郵件附檔，並對多個政府機關發動魚叉式社交工程電子郵件攻擊，技服中心已透過聯防監控月報，提供防護建議供政府機關參考。

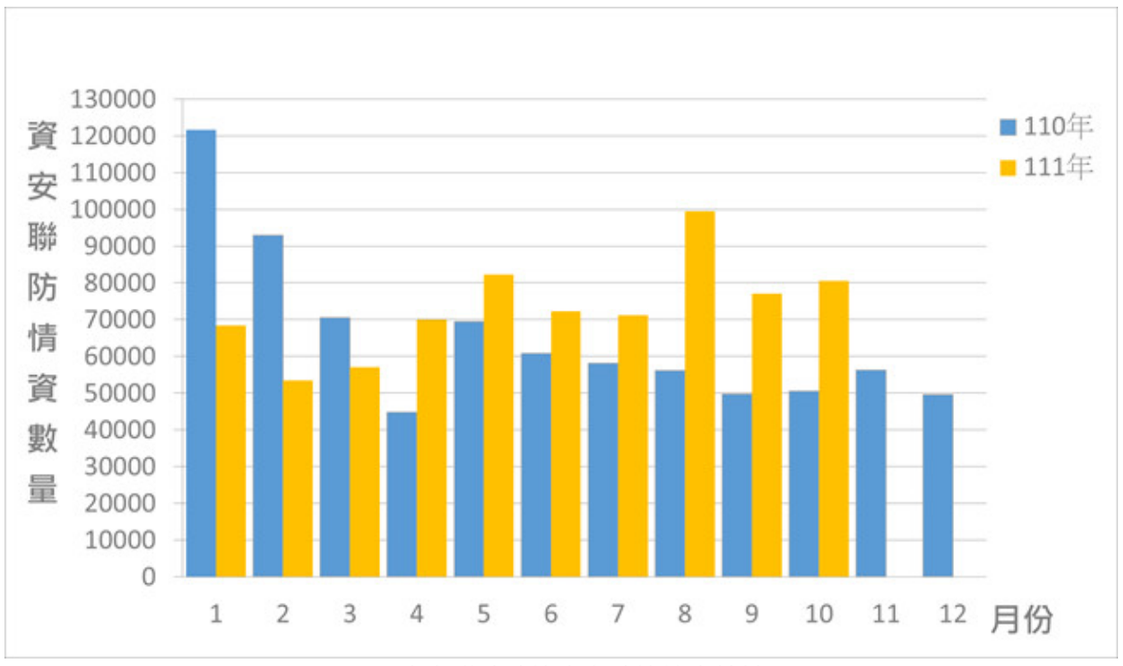

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共101件，近1年資安事件通報統計詳圖2。本月通報事件較去年同期增加69.29%，主要是技服中心偵測發現多個機關資訊設備下載疑似殭屍網路(Botnet)相關惡意程式，占總通報數量20.79%，部分機關調查發現其連網監視器遭駭。

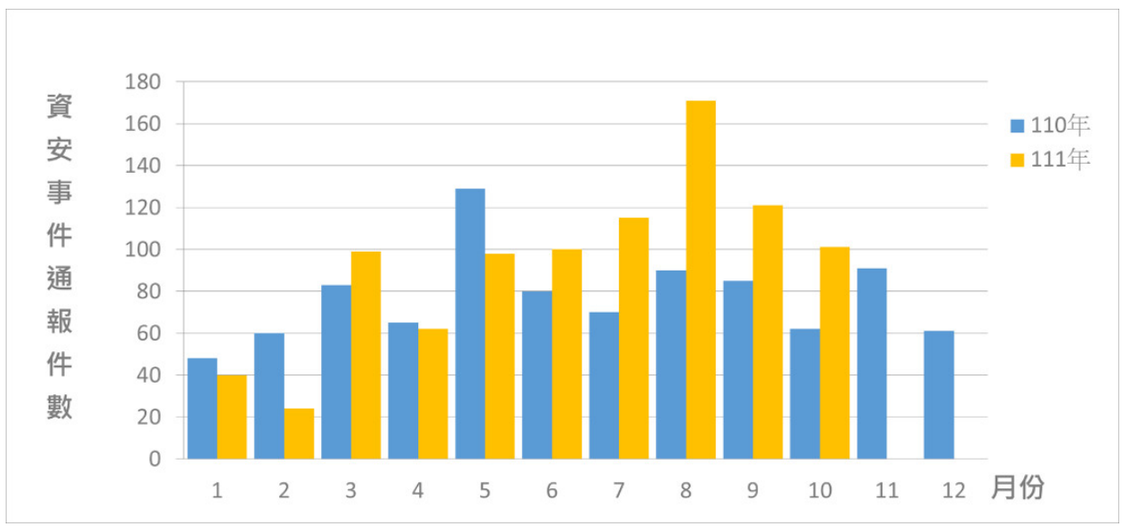

圖2 資安事件通報統計

事後資訊分享

本月偵測發現某機關資訊設備查詢惡意域名行為，經查其受駭主機是透過系統維護廠商的特權帳號登入並被植入惡意程式，檢視該惡意程式建立時間與來源IP，係該廠商申請之遠端登入執行版本更新作業，故研判入侵來源為系統維護廠商，後續已禁止該廠商遠端維護系統，並要求其檢測內部資訊設備確保無資安疑慮。

足資借鏡：鑑於近年駭客透過供應鏈攻擊事件頻傳，數位發展部資通安全署(前行政院資通安全處)以110年3月2日院臺護字第1100165761號函請各機關加強遠端存取控制機制，依「原則禁止、例外允許」方式辦理，若有必要允許外部遠端維護，應加強防護措施，如採多因子驗證方式，強化遠端登入身分驗證；稽核帳號登入時間與執行紀錄，確認時間與作業項目均與實際情形相符；結束遠端維運作業後，應確實關閉遠端網路連線服務，並更換遠端維護管理登入密碼等。此外，機關可依資通安全管理法第9條規定，監督委外廠商資通安全維護情形，降低委外廠商資訊設備遭利用做為入侵管道之風險。

<國內外重點資安新聞>

一、臉書公布逾四百多個Android和iOS惡意APP竊取用戶登入帳號憑證

Meta臉書團隊在10月7日公告位於Google Play Store和蘋果App Store 2平臺的APP安全研究結果，指出超過四百多個Android和iOS APP透過「Log-in with Facebook」功能，竊取個人臉書登入資訊與帳號。

Google和蘋果接獲Meta通知後已進行資料外洩調查，並將四百多個惡意程式APP從官方平臺移除。Meta呼籲，在下載APP前應審慎瞭解應用程式資訊與使用者評價。

(資料來源：Meta、iThome)

二、台灣獲歐盟邀請正式加入「隱私及個人資料保護聯合宣言」

國家發展委員會於10月12日表示，台灣獲歐盟邀請於10月8日加入「隱私及個人資料保護聯合宣言」(Joint Declaration on privacy and the protection of personal data)，共同宣示推動印太、歐洲等地區可信賴的資料流通。

該宣言旨在提升個人資料安全保護及隱私標準，並以促進國際間合作為目標，要項包含：完整規範私部門及公部門的法律框架及政策、落實個資保護核心原則以及個人可行使權利、強化國際資料傳輸的保障措施，以及獨立監督機關之監督和有效救濟等。

(資料來源：An official EU website、國家發展委員會)

三、衛福部舉辦111年度醫院資安長資安管理共識營

為加強醫院資安防護實務經驗，並促進台灣醫療單位之交流學習，衛生福利部於10月28日舉辦第4屆醫院資安長資安管理共識營。

討論議題涵蓋供應鏈資安稽核、醫療儀器資安防護政策、資安攻防演練實戰分享，以及未來醫院聯防機制等，藉由政策、管理與執行等構面綜合性探討，持續提升醫療資安領域的防護能量與韌性。

(資料來源：衛福部、HiNet生活誌)

<近期重要資安會議及活動>

「111年第2次政府資通安全防護巡迴研討會」訂於111年11月21日至12月7日分別於北、中、南、東區辦理8場次，請鼓勵資安專職(責)人員報名參加。

<資通安全長及資訊主管異動情形>

外交部資通安全長自111年10月28日起，原由曾厚仁次長兼任，現由蔡明彥次長兼任。

發布單位：資通安全署　　建立日期：2022-11-15　　更新日期：2022-11-15