資通安全網路月報（112年9月）

資通安全網路月報(112年9月)

<近期政策重點>

資通安全責任等級A、B級公務機關應依「政府領域聯防監控作業規範」辦理，即時回傳資安監控單，並於每月5日前回傳上個月的監控設備狀況單，數位發展部資通安全署近期將清查各機關上傳情形，並函請未依規範辦理之機關提出精進方案。

<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51,086件，分析可辨識的威脅種類，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(25%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(13%)，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，發現近期駭客濫用Cloudflare R2雲端儲存服務設置釣魚網站，寄送社交工程郵件攻擊政府機關與一般民眾。Cloudflare R2提供免費網站代管服務，駭客將釣魚網站託管在Cloudflare R2平台，同時於該釣魚網站網址後插入政府機關網域域名，再偽冒申辦業務資訊，進行社交工程攻擊。相關情資已提供各機關聯防監控防護建議。

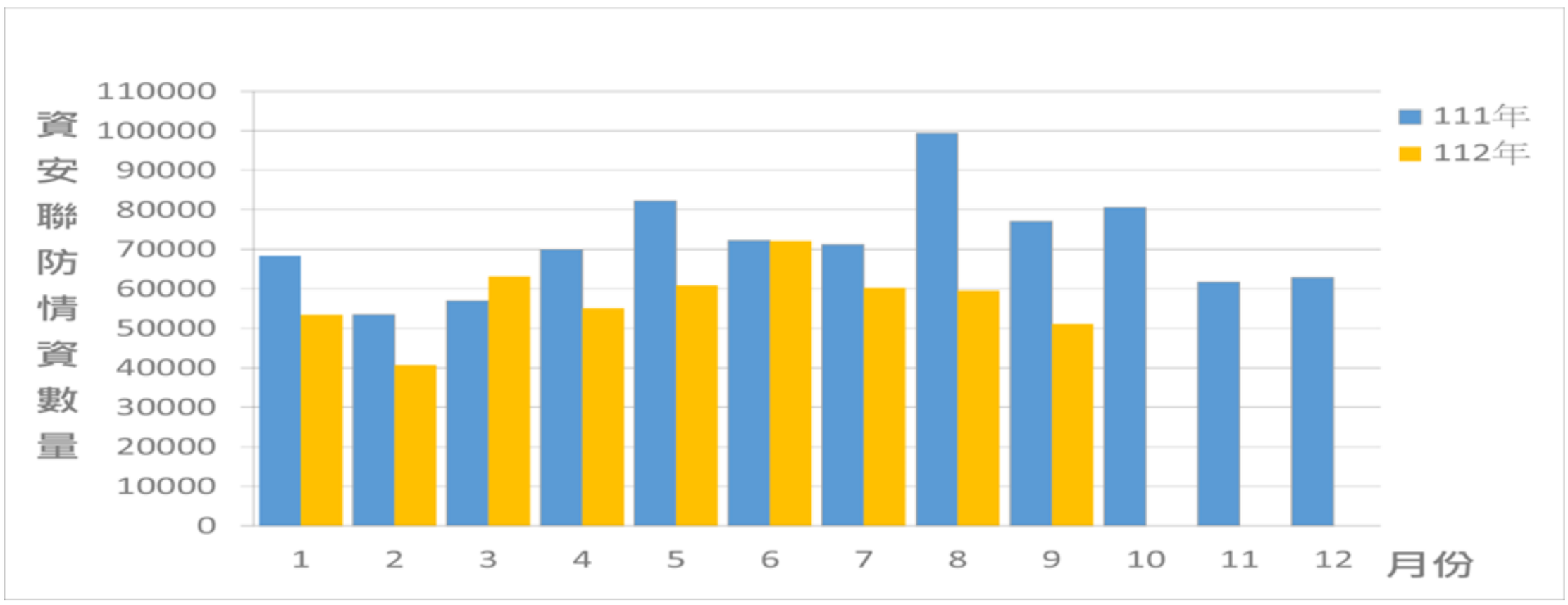

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共94件，本月通報事件較去年同期減少22.31%，主要是實兵演練通報案件數量減少，較去年同期減少約36.07%。另近1年資安事件通報統計詳見圖2。

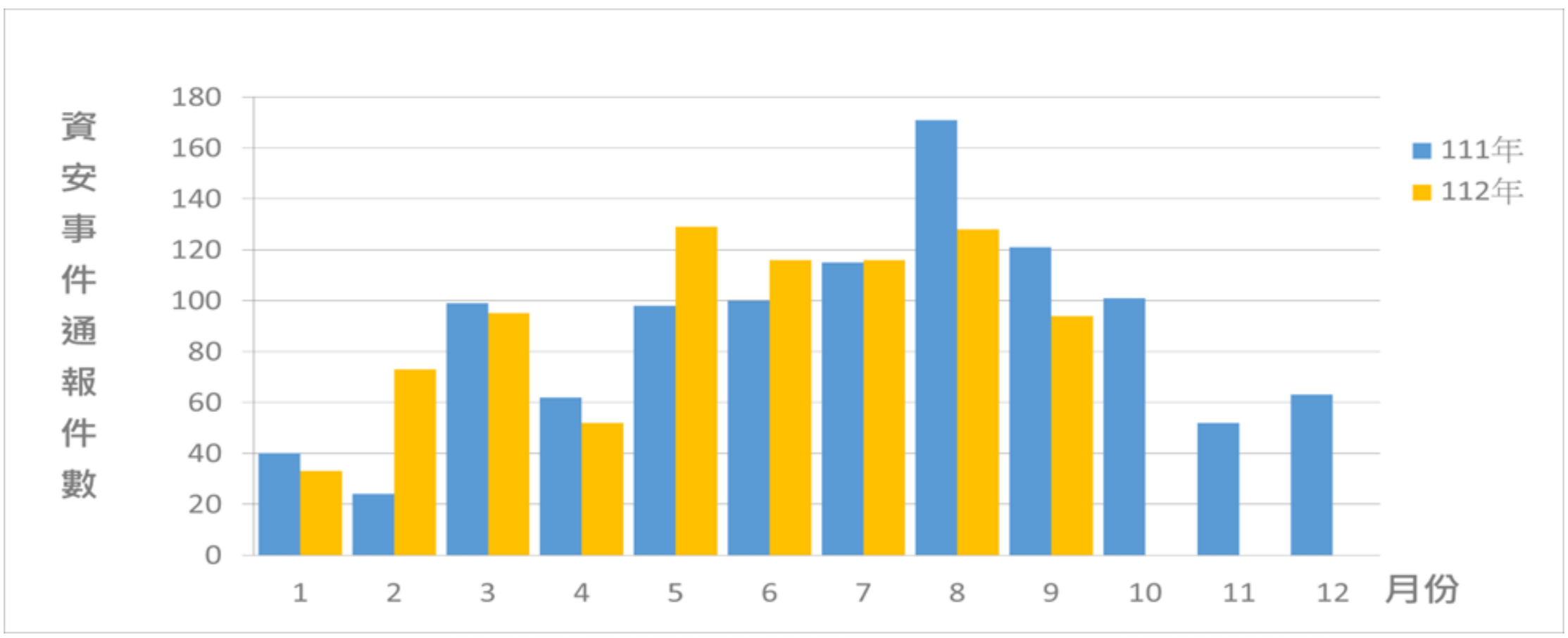

圖2 資安事件通報統計

事後資訊分享

本月國家資通安全研究院偵測到部分機關所使用某廠牌路由器或防火牆在112年6月被偵測發現嘗試下載木馬程式HiatusRAT，本月仍發現符合HiatusRAT網通設備惡意程式連線行為，經瞭解前揭機關網通設備儲存日誌因空間有限致無法確認事件發生原因，雖採重置與更新韌體方式改善，惟因持續監測發現仍有駭侵疑慮，故機關已更換網通設備並擴充可

儲存6個月以上日誌。

足資借鏡：

網通設備常受限於儲存日誌紀錄空間限制，致無法進一步釐清事件發生原因，雖機關採行重置與更新韌體修補安全漏洞等措施，惟仍未能確保更新的韌體能有效防堵攻擊手法。發生資安事件時，應進行事件根因分析，據以完成漏洞修補、強化作為及改善措施，若因設備儲存空間不足而無法確認事件發生原因，除強化設備安全防護措施與偵測機制外，亦建議宜擴增日誌儲存空間(如另建置Log Server)、加強檢視日誌或清查網通設備等防護措施，以利後續調查事件發生原因，降低重複遭入侵的風險。

<國內外重點資安新聞>

一、駭客利用偽造的Booking.com進行網釣攻擊

資安業者近期揭露有關鎖定線上旅遊產業的網釣攻擊，駭客先透過實際訂房，並以此發送夾帶惡意連結的相關詢問信件予訂房網站或飯店客服，倘客服點選信中惡意連結便可植入資訊竊取程式，再以訂房網站或飯店的名義展開第2階段的網釣攻擊，向真正的訂房者騙取信用卡資訊。

(資料來源：iThome)

二、國家級黑客集團藉由特定品牌路由器刺探跨國組織機密資料

美國及日本執法部門聯合發出警告，指某國家級黑客集團BlackTech先攻擊企業分部所使用的路由器，將其所寫惡意功能韌體置換該路由器的韌體，以取得網絡邊緣設備的管理員權限後，利用目標企業內部路由器與分支路由器信任關係，繼而攻擊其他網絡上設備以蒐集機密數據，此類攻擊手法不僅限於特定廠牌路由器，類似的技術也可用於在其他網通設備。

(資料來源：wepro180 、資安人)

三、行政院公共工程委員會公布「資訊服務採購作業指引」

為因應各種網路風險、資安威脅，提升整體資安防護。行政院公共工程委員與數位發展部、資訊、資安業者及公協會等單位，聯手制定「資訊服務採購作業指引」，將「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」納入資安規範參考，並於112年9月25日函知各政府機關。

另為提供資服和資安業者有足夠的調適時間配合及因應，在前揭一覽表普級的資安要求，訂於113年3月1日實施；中、高級的資安要求，則於113年8月1日起適用。

(資料來源：iThome)

<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，為廣蒐各界意見及凝聚共識，自112年8月17日起已辦理6場工作坊。另為擴大蒐集各界意見，資通安全管理法修正草案亦於9月22日預告在公共政策網路參與平臺(眾開講)，預訂10月中旬起辦理修法說明會，詳細報名資訊將另函通知，請有意報名者留意相關訊息。

數位發展部資通安全署為提升關鍵基礎設施資安防護與通報應變能力，探索解決當前重大資安威脅策略議題，2023年「前瞻資安探索會議」(Advanced Cybersecurity Exploration Conference, ACE)訂於112年10月18日至19日假臺大醫院國際會議中心辦理，將討論「關鍵基礎設施安全」及「新興技術風險管理」2大資安議題，規劃邀請國內外深耕資安領域專家學者共同與會，進行專題分享及座談會。

<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：2023-10-15　　更新日期：2023-10-13