資通安全網路月報（112年6月）

資通安全網路月報（112年6月）

<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72,090件，分析可辨識的威脅種類，第1名為資訊蒐集類(42%)，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(27%)，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(21%)，主要係嘗試入侵未經授權的主機。另統計近1年情資數量分布詳見圖1。

進一步彙整分析聯防情資資訊，發現近期駭客發起的社交攻擊活動，是利用URL混淆手法規避資安防護機制，提高入侵機關成功率。駭客利用訂單確認與收據文件等主旨，引誘使用者點擊惡意附檔，並在該惡意附檔內含經混淆的URL，該URL將連線至中繼站下載惡意程式，進而達到竊取機敏資料的目的。相關情資已提供各機關聯合監控防護建議。

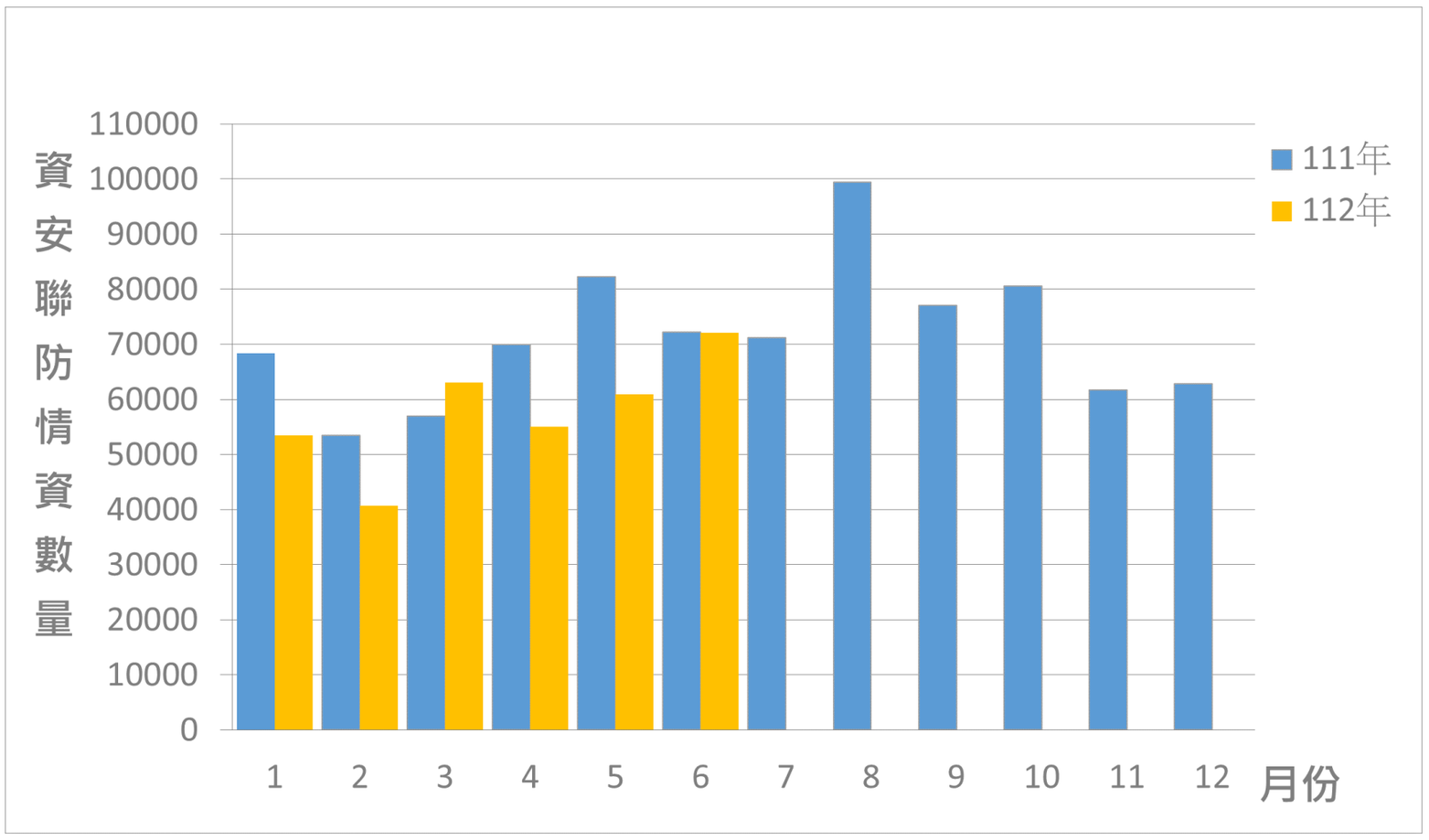

圖1 資安聯防監控資安監控情資統計

事中通報應變

本月資安事件通報數量共119件，較去年同月增加19%，國家資通安全研究院偵測發現多個機關的資訊設備，嘗試下載木馬程式HiatusRAT，占總通報數量11.77%，經機關調查後發現，受駭設備多為N牌路由器或防火牆等網通設備，後續已藉由重置與更新韌體版本進行應處，降低整體資安風險。另近1年資安事件通報統計詳見圖2。

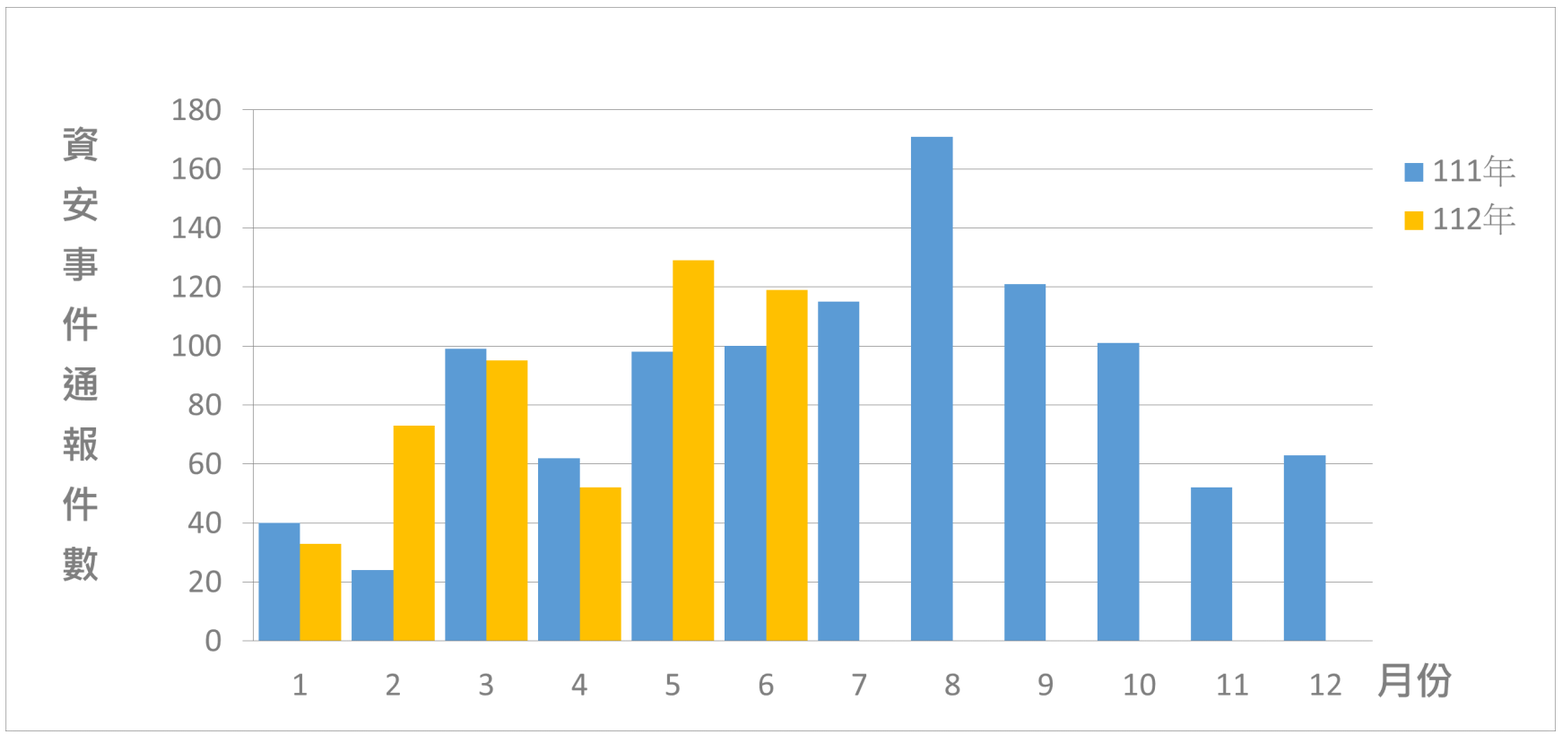

圖2 資安事件通報統計

事後資訊分享

本月國家資通安全研究院偵測發現多個機關設備對外下載木馬程式HiatusRAT，部分機關調查後發現該連線設備為網通設備(路由器或防火牆)，因設備紀錄保存不足導致難以進行根因調查，又進一步檢視設備更新情形，發現受駭設備久未更新韌體與軟體，推測可能是舊版本存在漏洞遭利用所致，目前受駭機關均已重置其受駭的網通設備或完成版本更新作業，國家資通安全研究院目前未再發現觸發類此異常連線行為之機關設備。

足資借鏡：

網通設備(如路由器、防火牆及物聯網設備等)軟體或韌體更新訊息常遭忽略而存在資安風險，且囿於設備本身容量限制，難以保存相關紀錄。建議機關應定期盤點設備，檢視韌體與軟體更新紀錄，同時留意所採購產品之支援版本更新情形，若產品已釋出停止支援更新訊息，應儘早評估汰換或採取相關因應措施。此外，應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、歐洲議會通過全球首部AI監管法

歐洲議會表決通過採納「歐盟人工智慧法案」(E.U. AI Act)，讓歐盟實施全球首套AI(人工智慧)監管措施、樹立世界AI標準，惟該法案還需與歐洲理事會進行協商。

該法案禁用「風險水準不可接受」的AI系統，例如在公共場所禁用人臉辨識技術等預測性工具；並對「高風險AI」設新限制，如禁用可能在選舉中影響選民、或傷害民眾健康的系統。

(資料來源：自由時報)

二、勒索軟體Lockbit之威脅與應處

多國網路安全機構警告Lockbit是近年最活躍的勒索軟體即服務(RaaS)，並針對勒索軟體Lockbit發布1份聯合安全公告，揭露Lockbit從2019年迄今之進化，列出了Lockbit的攻擊滲透步驟，並提供在各階段預防相關攻擊的緩解措施，是資安防護上相當具價值的參考。

(資料來源：iThome)

<近期重要資安會議及活動>

112年第1次政府資通安全巡迴研討會於112年6月28日至7月13日分別於北、中、南、東區辦理8場次，宣導最新資安防護重點與訊息，協助各機關提升資通安全管理與技術認知。

<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：2023-07-15　　更新日期：2023-07-18