

資安月報：政府機關 6 月遭 Emotet 殭屍網路攻擊增加

根據行政院最新一期資安月報，6 月針對政府機關的 Emotet 殭屍網路攻擊活動持續增加，透過竊取受駭電腦的電子郵件資訊，偽造惡意郵件夾帶惡意程式，寄送給其他政府機關人員。

最新一期資安月報顯示，6 月政府機關的資安聯防情資共 7 萬 2185 件，其中可明確辨識的威脅種類，主要是外部主機執行掃描探測攻擊及外對內連線大量阻擋事件，占 48%。

月報分析上述情資發現，Emotet 殭屍網路攻擊活動持續增加，主要是透過竊取受駭電腦的電子郵件資訊，偽造惡意郵件，如以電子郵件或政府機關人員姓名填入郵件內文或主旨，再以附加檔案夾帶惡意程式寄送給政府機關人員，藉以擴散 Emotet 殭屍網路。

月報指出，行政院國家資通安全會報技術服務中心，已對此提供相關防護建議給各機關參考。月報並指出，偵測到某機關資訊設備對外產生異常連線，經調查發現，內部人員使用個人外接式行動硬碟傳遞資料，導致行動硬碟中的惡意程式，透過公務電腦對外連線，但清除惡意程式後，未發現有其他受駭情事。

月報建議，機關規範私人資訊設備或外接式儲存設備使用原則，如設置管制區限定使用範圍，或以防毒軟體掃描無異常後再使用，降低遭外部資訊設備惡意程式感染風險。

月報也提醒，資安責任等級 A、B、C 級納管機關，依法應導入資通安全弱點通報系統 (VANS)，其中 A、B 級機關應於 8 月 23 日前完成。根據資通安全責任等級分級辦法，公務機關及特定非公務機關的資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級；業務涉及國家機密、屬關鍵基礎設施提供者、公立醫學中心等機關列為 A 級。

(資料來源：蘋果新聞網 111 年 06 月 24 日報導)

多一分保密警覺，少一分洩密風險

廉政檢舉專線 0800-286-586

法務部矯正署雲林監獄政風室關心您