

115 年 3 月公務機密維護宣導

公務機關近半年常見攻擊態樣及防範強化作為

國家資通安全研究院近半年總計接獲 723 件公務機關資安通報案件，常見攻擊態樣說明如下：

1. 冒牌軟體散播惡意程式

攻擊者假冒合法或常用軟體，誘使使用者下載或安裝，進而植入惡意程式或門，於背景建立異常對外連線，作為後續控制或資料外傳之管道。

2. 可攜式媒體設備（USB）感染蠕蟲

利用 USB 等可攜式媒體作為傳播媒介，當設備插入機關電腦時即自動執行惡意程式，造成端點遭入侵並產生異常行為，進一步衍生橫向擴散或對外通訊風險。

3. 假借「行政訴訟」主題之社交工程郵件攻擊

攻擊者以政府機關高度關注之業務主題（如行政訴訟、公文往返等）製作釣魚郵件，誘使人員開啟附件或點擊連結，藉此植入惡意程式或竊取資訊。

4. 水坑式攻擊（Watering Hole Attack）

攻擊者入侵公務人員或特定族群常瀏覽之合法網站，植入惡

意指令，使使用者於正常瀏覽過程中觸發惡意程式下載，導致端點受害並產生異常連線行為。

國家資通安全研究院建議，在管理面上，宜持續強化人員對社交工程、水坑式攻擊及冒牌軟體等常見手法之風險意識，並建立可攜式媒體使用、軟體來源及外部網站存取之管理原則，將使用情境納入資安治理與教育訓練範疇。

資料來源：摘錄自「國家資通安全研究院 資安週報-第 30 期」

