Catch me if you can!
「勒索軟體」危機

本文轉自法務部調查局清流雙月刊 106 年 9 月號　　文 / 吳旻純

惡意軟體之演進

今年 5 月出現大規模電腦病毒 Wanna cry 攻擊，全球 150 國的政府部門、企業及醫院等超過 30 萬台電腦受影響，資訊安全維護岌岌可危。攻擊模式是將電腦使用者常用的文件檔（如 word、pdf）、照片圖檔等加密，再以支付一定金額比特幣（Bitcoin）方式換取金鑰解密。此種控制使用者檔案，並要求支付贖金的電腦病毒攻擊即所謂勒索軟體（ransomware）。最初開始的惡意軟體（malware）攻擊模式，以植入木馬程式的方式，竊取使用者個資來獲利，惟現行模式已從竊取個資轉向加密使用者檔案，若使用者不支付贖金，將無法取得金鑰來解密檔案。

鑑於惡意軟體攻擊愈趨猖獗，攻擊模式不斷演進，政府機關、企業等單位必須正視資安監控與維護，避免因系統漏洞而受到損失。

勒索軟體之內涵

一、何謂勒索軟體？

勒索軟體（ransomware）係一種阻斷存取式攻擊（denial-of-access attack），透過以釣魚網站或下載檔案的方式，讓使用者個資外洩或自動安裝病毒程式，用戶電腦如果有系統上漏洞，如使用盜版軟體、未定期更新系統等，病毒軟體就會產生匿名資料夾，取代原本電腦用戶的資料夾，然後自動執行病毒程式，以 RSA 不對稱式加密演算法加密檔案，即只有駭客才有私鑰（private key）解密，使用者唯有支付定額的比特幣或黑幣，方有可能回復檔案。

二、勒索軟體攻擊手法

基本上勒索軟體攻擊主要有三個階段，如圖 1 所示，駭客會先設置惡意陷阱以潛入用戶電腦，俟偵測出用戶系統漏洞，匿名資料夾即自動執行取代原資料夾，將所有檔案加密，並出現要求支付贖金的通知訊息，用戶支付後才能取回檔案。■

勒索軟體攻擊三階段，設下陷阱、控制電腦、要求贖金。