

【政風宣導-公務機密宣導】「勒索軟體」危機

廉政檢舉專線：0800-286-586

(本文引自「清流」雙月刊)

※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。

※勒索軟體攻擊手法

基本上勒索軟體攻擊主要有三個階段，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。

第一階段 設下陷阱

當勒索軟體要採取攻擊時，常見的有透過釣魚網站 (phishing) 來騙取個資，或以垃圾郵件 (spam email) 夾帶 zip 壓縮檔，誘騙使用者開啟安裝；另外駭客還會利用知名部落格等點閱率高的網頁，嵌入惡意廣告頁面，當使用者不小心點開或網站自動執行播放 java script 或 flash 廣告時，勒索軟體即搜尋其漏洞駭入用戶系統。

第二階段 控制電腦

當用戶電腦被植入勒索軟體後，其會先修改系統內部相關設定，當開機時就自動執行安裝。安裝完成後，用戶電腦會與外部伺服器連線進行公開金鑰 (public key) 加密，將電腦系統內的檔案加密後進行勒索。

第三階段 要求贖金

當勒索軟體完成檔案加密後，使用者登入系統或開啟檔案時，就會跳出勒索通知，要求期限內支付相當金額的比特幣，如果超過期限贖金則加倍，唯有支付贖金以取得私鑰（private key）回復檔案。

※勒索軟體之預防

電腦使用者搭乘網路安全公車（BUS）必經三大站以通往資訊安全的目的地：

第一站：定期備份（Backup）

為了避免重要資料被駭而無法回復的情形，電腦使用者應隨時將重要資料備份至異地，免於遭受勒索軟體威脅。

第二站：系統軟體定期更新（Update）

電腦使用者須定期更新作業軟體及防毒軟體，以修補系統漏洞，降低遭到勒索軟體攻擊機率。若防毒軟體偵測出系統已感染，在顯示出勒索訊息前，先切斷主機網路連結，以避免完成加密程序，並重新安裝系統軟體，確保系統及資料安全。

第三站：不隨意開啟不明郵件及注意瀏覽網頁安全（Safety）

不管是公務機關、公司團體或個人使用者，除了倚靠資訊單位防禦管理外，都必須養成良好的網路使用習慣。不隨意開啟來源不明的電子郵件、附件及自非信任來源下載安裝程式，另瀏覽網頁時，不要開啟網頁上嵌入的廣告連結，避免落入勒索病毒的陷阱，造成個資外洩或更大損害。

面對惡意攻擊不斷演進的網路環境，電腦使用者必須隨時保持警戒，養成良好的網路安全習慣，避免因為疏忽而造成個人資料被駭及其他相關損害，在浩瀚未知的網路世界，唯有搭乘網路安全公車（BUS）方能通往資訊安全的境界。