公務機密維護宣導

摘錄自國家資通安全會報技術服務中心網站

近期勒索軟體攻擊事件頻傳，使用者電腦一旦遭植入該惡意程式，將導致該電腦可存取的檔案(含網路磁碟機、共用資料夾等)全數加密無法開啟讀取，藉以勒索使用者支付贖金換取檔案解密。

依相關研究報告資料顯示，勒索軟體傳染途徑以應用程式漏洞(如 Flash Player)與社交工程為主，且遭加密檔案無法自行解密還原。請確認相關應用程式更新情況，定期備份重要檔案，避免開啟來路不明郵件或連結。

建議措施：

1. 清查重要資料，並參考下列做法定期進行備份作業：

藟霈定期執行重要的資料備份。

藟需備份資料應有適當的實體及環境保護。

藟需應定期測試備份資料，以確保備份資料之可用性。

藟需資料的保存時間與檔案永久保存的需求，應由資料擁有者研提。

藟需重要機密的資料備份，應使用加密方式來保護。

2.檢視網路硬碟與共用資料夾之使用者存取權限，避免非必要使用存取。

3.確認作業系統、防毒軟體，及應用程式(如Adobe Flash Player、Java)更新情況，並定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為。

4.若使用隨身碟傳輸資料，應先檢查隨身碟是否感染病毒或惡意程式。

5.若疑似遭受感染時，可參考下列做法：
藟需應立即關閉電腦並切斷網路，避免災情擴大。

藟需建議重新安裝作業系統與應用程式，且確認已安裝至最新修補程式後，再還原備份的資料。

藟需備份資料在還原至電腦之前，應以防毒軟體檢查，確保沒有殘存的惡意程式。

6.請使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結，以防被植入後門程式。