張貼日期：2020/06/03

【資安攻擊預警】近期利用PORT 445加密勒索軟體活動頻繁，請加強系統/應用程式更新與資料備份作業

主旨：【資安攻擊預警】近期利用PORT 445加密勒索軟體活動頻繁，請加強系統/應用程式更新與資料備份作業

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202006-0095□
  - 近期勒索軟體攻擊活動情資顯示，此波勒索軟體攻擊是利用微軟伺服器訊息區塊(SMB,PORT 445)協定進行攻擊，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。
  - 建議請各級政府機關除加強組織資安監控防護外，持續確認相關應用程式更新情況，定期備份重要檔案，加強資訊安全宣導，避免開啟來路不明郵件或連結。
- 影響平台:
  全
- 建議措施:
  1. 建議機關儘速進行作業系統更新，如無特殊需求，建議關閉Port 445服務。
  2. 清查重要資料，並參考下列做法定期進行備份作業：
     - 定期執行重要的資料備份。
     - 備份資料應有適當的實體及環境保護。
     - 應定期測試備份資料，以確保備份資料之可用性。
     - 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。
     - 重要機密的資料備份，應使用加密方式來保護。
  3. 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。
  4. 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。
  5. 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。
  6. 若疑似遭受感染時，可參考下列做法：
     - 應立即關閉電腦並切斷網路，避免災情擴大。
     - 通知機關資訊人員或廠商協助搶救還沒被加密的檔案。
     - 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。
     - 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。
  7. 加強教育訓練，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。

計算機與通訊中心
網路系統組 敬啟