張貼日期：2020/05/07

【資安攻擊預警】加密勒索軟體猖獗，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】加密勒索軟體猖獗，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-202005-0115
  - 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。 依近期攻擊活動研究報告顯示，駭客透過進階持續性滲透攻擊(Advanced Persistent Threat, APT)方式成功入侵目標組織，並取得網域管理者權限後，以群組原則方式散布勒索軟體，達到大範圍資料加密目的，建議各會員應提高警覺，定期檢視例行性排程設定與派送機制，如於相關日誌發現異常連線或警示，應深入釐清事件原因，避免錯失調查時機。 此外，傳統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，建議請各會員除加強組織資安監控防護外，仍應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. 定期檢視資通訊系統日誌紀錄，同時檢視資通訊系統排程設定與派送機制，如發現異常連線或新增排程情形，應立即深入了解事件原因。
  2. 不定期檢視資通訊系統帳號使用情況，並定期變更帳號密碼，確保密碼設定符合複雜性原則，避免字符轉換情況發生。
  3. 清查重要資料，並參考下列做法定期進行備份作業：
     1. 定期執行重要的資料備份。
     2. 備份資料應有適當的實體及環境保護。
     3. 應定期測試備份資料，以確保備份資料之可用性。
     4. 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。
     5. 重要機密的資料備份，應使用加密方式來保護。
  4. 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。
  5. 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。
  6. 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。
  7. 若疑似遭受感染時，可參考下列做法：
     1. 應立即關閉電腦並切斷網路，避免災情擴大。
     2. 通知機關資訊人員或廠商協助搶救還沒被加密的檔案。
     3. 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。
     4. 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。
  8. 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

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20200507_01

Last update: **2020/05/07 08:56**