張貼日期：2020/06/22

【資安攻擊預警】澳洲網路安全中心分享網路攻擊相關威脅指標，請注意防範！

主旨：【資安攻擊預警】澳洲網路安全中心分享網路攻擊相關威脅指標，請注意防範！

- 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-202006-05897
  - 近期澳洲遭受大規模網路攻擊，駭客針對政府機關、民間企業、教育、醫療及關鍵基礎設施服務提供者等領域進行攻擊，澳洲網路安全中心(ACSC)發布本次攻擊事件之威脅指標與防護建議，技服中心分享相關情資提供會員加強資安防護，注意防範。
- 影響平台:
  微軟作業系統
- 建議措施:
  1. 部署黑名單於防護設備進行偵測，監控是否有資訊設備已遭入侵，網路位址與網域名稱黑名單如附件。(威脅指標下載連結：https://cert.tanet.edu.tw/images/nisac-ana-202006-0589-ioc.csv)
  2. 依附件惡意程式特徵如雜湊值與偵測規則，用以偵測系統是否存在相關惡意程式，若確認資訊設備已遭入侵，建議立即進行必要處理措施：
     1. 針對受害電腦進行資安事件應變處理。
     2. 重新安裝作業系統，並更新作業系統及相關應用軟體。
     3. 更換系統使用者密碼。
  3. 日常資訊設備資安防護建議：
     1. 持續更新作業系統及辦公室文書處理軟體等安全性修補程式。若所使用的作業系統已不再提供更新程式，建議升級至較新版本作業系統。
     2. 系統上所有帳號需設定強健的密碼，非必要使用的帳號請將其刪除或停用。系統上非必要的服務程式亦建議移除或關閉。
     3. 安裝及啟用防毒軟體防護，並持續更新病毒碼及掃毒引擎。
     4. 安裝及啟用防火牆防護，並設定防火牆規則僅開放所需之通訊埠。
     5. 不要開啟可疑的郵件與檔案，在開啟下載資料之前先進行資安防護掃描檢查。
- 參考資料:
  https://www.cyber.gov.au/threats/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks

---

計算機與通訊中心
網路系統組 敬啟