張貼日期：2020/09/02

【資安訊息】北韓駭客組織利用惡意程式針對金融領域進行攻擊，請注意防範

主旨：【資安訊息】北韓駭客組織HIDDEN COBRA利用惡意程式FASTCash 2.0針對金融領域進行攻擊，請注意防範

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 (NCCST-ANA-G2020-0350)
  - 美國國土安全部、美國財政部、聯邦調查局及美國國防部近期發布惡意程式分析報告，描述北韓駭客組織HIDDEN COBRA利用之FASTCash 2.0遠端存取後門工具程式，用於操控金融設備進行偽冒交易。
    若資訊設備遭受感染會有以下風險：
    1. 個人或單位資料遭竊取。
    2. 個人工作或單位運作被影響而中斷停擺。
    3. 資訊設備資源被利用於對外攻擊。
    4. 單位財務損失。
  - 建議除使用防毒軟體檢查資訊設備是否受惡意程式感染，也可透過檢查惡意程式資訊確認感染與否。
  - 影響平台: 微軟作業系統
- 建議措施:
  1. 檢查系統中是否有惡意程式SHA-256資訊如下：
     129b8825eaf61dcc2321aad7b84632233fa4bbc7e24bdf123b507157353930f0
     39cbad3b2aac6298537a85f0463453d54ab2660c913f4f35ba98fffeb0b15655
     5cb7a352535b447609849e20aec18c84d8b58e377d9c6365eafb45cdb7ef949b
     32a4de070ca005d35a88503717157b0dc3f2e8da76ffd618fca6563aec9c81f8
     9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e
     c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec
     efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e
     70b494b0a8fdf054926829dcb3235fc7bd0346b6a19faf2a57891c71043b3b38
     8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1
     9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852
     a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118
     aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83
     f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de
  2. 各會員可依參考資訊連結，取得詳細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。

計算機與通訊中心
網路系統組 敬啟