張貼日期：2019/09/11

【資安漏洞預警】北韓駭客組織HIDDEN COBRA利用惡意程式BADCALL運用知名網站憑證進行fake TLS連線，以及利用惡意程式ELECTRICFISH建立隱密通道進行通訊

主旨：北韓駭客組織HIDDEN COBRA利用惡意程式BADCALL運用知名網站憑證進行fake TLS連線，以及利用惡意程式ELECTRICFISH建立隱密通道進行通訊，請各單位注意防範

說明：

- 內容說明:
  - 美國國土安全部、聯邦調查局及美國國防部近期更新北韓駭客組織HIDDEN COBRA所利用的BADCALL與ELECTRICFISH惡意程式相關資訊。
  - BADCALL工具會利用知名網站憑證，如Apple, Facebook, Google, Microsoft等，以進行fake TLS連線並將所取得資料回傳至駭客所控制的主機□ELECTRICFISH工具可用於在受害電腦與駭客電腦之間建立隱密通道(Tunnel)□規避資安設備之偵測；該工具亦可指定外部代理伺服器(Proxy Server)作為中間跳板，以隱藏駭客真實網路位址(IP Address)□
  - 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，也可透過檢查連線紀錄與惡意程式資訊確認感染與否。
- 影響平台:
  微軟作業系統□Android系統
- 建議措施:
  1. 檢查資安防護設備紀錄，確認是否有不正常的8000、60000埠連線。
  2. 檢查個人電腦上的防火牆是否被不正常停用或是防火牆設定被修改成允許外部連線到該電腦的443埠。
  3. 檢查系統是否存在下列檔案(BADCALL惡意程式)：
     1. 本次報告更新□22082079AB45CCC256E73B3A7FD54791
        - MD5: 22082079ab45ccc256e73b3a7fd54791
        - SHA1: 029bb15a2ba0bea98934aa2b181e4e76c83282ce
     2. 本次報告更新：
        - MD5: 2733a9069f0b0a57bf9831fe582e35d9
        - SHA1: f06f9d015c2f445ee0f13da5708f93c381f4442d
     3. 本次報告更新□hc.zip
        - MD5: eb7da5f1e86679405aa255aa4761977d
        - SHA1: 880cb39fee291aa93eb43d92f7af6b500f6d57dc
     4. C01DC42F65ACAF1C917C0CC29BA63ADC
        - MD5: c01dc42f65acaf1c917c0cc29ba63adc
        - SHA1: d288766fa268bc2534f85fd06a5d52264e646c47
     5. C6F78AD187C365D117CACBEE140F6230
        - MD5: c6f78ad187c365d117cacbee140f6230

        - SHA1: 5116f281c61639b48fd58caaed60018bafdefe7a
    6. Android惡意程式D93B6A5C04D392FC8ED30375BE17BEB4
        - MD5: d93b6a5c04d392fc8ed30375be17beb4
        - SHA1: f862c2899c41a4d1120a7739cdaff561d2490360
4. 檢查系統是否存在下列檔案(ELECTRICFISH惡意程式)：
    1. 本次報告更新0BA6BB2AD05D86207B5303657E3F6874
        - MD5: 0ba6bb2ad05d86207b5303657e3f6874
        - SHA1: ad44567c8709df4889d381a0a64cc4b49e5004c3
    2. 8d9123cd2648020292b5c35edc9ae22e
        - MD5: 8d9123cd2648020292b5c35edc9ae22e
        - SHA1: 0939363ff55d914e92635e5f693099fb28047602
5. 若確認資訊設備已遭入侵，建議處理措施：
    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。
6. 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:
    - ADCALL報告
        1. https://www.us-cert.gov/ncas/analysis-reports/ar19-252a
        2. https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-G.PDF
    - ELECTRICFISH報告
        1. https://www.us-cert.gov/ncas/analysis-reports/ar19-252b
        2. https://www.us-cert.gov/ncas/analysis-reports/AR19-129A

計算機與通訊中心
網路系統組 敬啟