張貼日期：2019/04/12

[資安漏洞預警通知] 北韓駭客組織HIDDEN COBRA所利用的惡意程式HOPLIGHT請各單位注意防範

主旨：[資安漏洞預警通知] 北韓駭客組織HIDDEN COBRA所利用的惡意程式HOPLIGHT請各單位注意防範

- 內容說明:
  - 美國國土安全部與聯邦調查局公布最新北韓駭客組織HIDDEN COBRA所利用的惡意程式HOPLIGHT透過加密連線進行惡意活動。
  - 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，也可透過已知惡意連線IP與惡意檔案存在路徑確認感染與否。
- 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HIDDEN COBRA IP黑名單如下：
     - 112.175.92.57
     - 113.114.117.122
     - 128.200.115.228
     - 137.139.135.151
     - 181.39.135.126
     - 186.169.2.237
     - 197.211.212.59
     - 21.252.107.198
     - 26.165.218.44
     - 47.206.4.145
     - 70.224.36.194&
     - 81.94.192.10&
     - 81.94.192.147
     - 84.49.242.125
     - 97.90.44.200
  2. 檢查系統是否存在下列檔案：
     1. %System32%\rdpproto.dll
        - MD5: dc268b166fe4c1d1c8595dccf857c476
        - SHA-1: 8264556c8a6e460760dc6bb72ecc6f0f966a16b8
     2. C:\WINDOWS\udbcgiut.dat 或 %AppData%\Local\Temp\udbcgiut.dat
        - MD5: ae829f55db0198a0a36b227addcdeeff
        - SHA-1: 04833210fa57ea70a209520f4f2a99d049e537f2
     3. C:\WINDOWS\MSDFMAPI.INI 或%UserProfile%\AppData\Local\VirtualStore\Windows\MSDFMAPI.INI
        - MD5: c4103f122d27677c9db144cae1394a66
        - SHA-1: 1489f923c4dca729178b3e3233458550d8dddf29

        4. %System32%\UDPTrcSvc.dll
            - MD5: 0893e206274cb98189d51a284c2a8c83
            - SHA-1: d1f4cf4250e7ba186c1d0c6d8876f5a644f457a4
    3. 若確認資訊設備已遭入侵，建議處理措施：
        1. 重新安裝作業系統，並更新作業系統及相關安裝軟體。
        2. 更換系統使用者密碼。
        3. 安裝及啟用防毒軟體防護。
        4. 安裝及啟用防火牆防護。
    4. 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。
- 參考資料:
    - https://www.us-cert.gov/ncas/analysis-reports/AR19-100A

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:20190412_01

Last update: **2019/11/04 09:14**