張貼日期：2019/05/14

[資安漏洞預警通知] 北韓駭客組織HIDDEN COBRA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

主旨：[資安漏洞預警通知] 北韓駭客組織HIDDEN COBRA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

- 內容說明:
  - 美國國土安全部與聯邦調查局近期公布北韓駭客組織HIDDEN COBRA所利用的惡意程式「ELECTRICFISH」該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. 檢查系統是否存在下列檔案：
     1. a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb
        - MD5: 8d9123cd2648020292b5c35edc9ae22e
        - SHA-1: 0939363ff55d914e92635e5f693099fb28047602
     2. hs.exe
        - MD5: df934e2d23507a7f413580eae11bb7dc
        - SHA-1: 5ce51e3882c40961caf2317a3209831ed77c9c40
  2. 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。
  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.us-cert.gov/ncas/analysis-reports/AR19-129A

計算機與通訊中心
網路系統組 敬啟