張貼日期：2019/11/04

【資安漏洞預警】更新北韓駭客組織HIDDEN COBRA利用之惡意程式HOPLIGHT變種資訊

主旨：更新北韓駭客組織HIDDEN COBRA利用之惡意程式HOPLIGHT變種資訊，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發布惡意程式分析報告AR19-304更新北韓駭客組織HIDDEN COBRA利用之惡意程式HOPLIGHT變種資訊，該惡意程式會透過與中繼站建立加密連線，隱匿惡意活動。
  - 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
- 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，本次新增HIDDEN COBRA IP黑名單如下：
     - 117.239.241.2
     - 119.18.230.253
     - 14.140.116.172
     - 195.158.234.60
     - 210.137.6.37
     - 218.255.24.226
     - 221.138.17.152
  2. 各單位可依參考資料連結，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。
- 參考資料:
  1. https://www.us-cert.gov/ncas/analysis-reports/ar19-304a
  2. 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