張貼日期：2018/06/05

[資安漏洞預警通知] 北韓駭客組織HIDDEN COBRA所利用的惡意程式Joanap及Brambul□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Joanap及Brambul□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□Joanap遠端存取後門程式與Brambul網路檔案分享系統蠕蟲。
  - 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。
  - 建議除使用防毒軟體檢查資訊設備是否受惡意程式感染，也可透過下列方式檢查感染與否：
    1. 路徑□%WINDIR%\system32\□下存在檔案□mssscardprv.ax□□
    2. 嘗試寄信至redhat@gmail.com□
    3. 嘗試寄信至misswang8107@gmail.com□
    4. 嘗試連線至HIDDEN COBRA-IP黑名單。
  - 下載連結：http://140.117.101.5/pdf/HIDDENCOBRA-IP.rar (學校骨幹網路已做阻擋)
- 影響平臺：微軟作業系統
- 建議措施：
  - 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。
  - 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:
  1. https://www.us-cert.gov/ncas/alerts/TA18-149A
  2. https://www.us-cert.gov/ncas/analysis-reports/AR18-149A

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:20180605_01

Last update: **2018/06/05 15:14**