張貼日期：2022/08/08

【資安攻擊預警】社交工程攻擊通告：請加強防範駭客以紓困福利為由之社交工程郵件攻擊

主旨：【資安攻擊預警】社交工程攻擊通告：請加強防範駭客以紓困福利為由之社交工程郵件攻擊

- 內容說明：
  - 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202208-0307
  - 技服中心近期發現駭客大量註冊偽冒衛福部與相關政府機關的域名(如www[.]vgov[.]tw、www[.]mohwgov[.]tw等)，目前已偵測駭客利用該域名架設偽冒衛福部之釣魚網站，並寄送以提供紓困福利為由之網路釣魚電子郵件。當收件者點擊釣魚連結，將連線至前述之釣魚網站，並誘導輸入個人機敏資訊，導致個資外洩與身分遭偽冒之風險，請各機關加強防範社交工程郵件，相關受駭偵測指標請參考附件。
  - 註：相關網域名稱為避免誤點觸發連線故以「[.]」區隔
- 影響平台:
  N/A
- 建議措施:
  1. 機關網路管理人員請參考附件受駭偵測指標，確實更新防火牆，阻擋可疑釣魚域名與惡意中繼站。
  2. 建議留意可疑電子郵件，注意郵件來源正確性，勿開啟不明來源之郵件與相關連結。
  3. 開啟任何網頁時請留意網頁域名，確認域名正確性，勿隨意提供機敏資訊，如：公務用電子郵件帳號、密碼、信用卡號碼等，以防個人資料與公務機敏資訊外洩。
  4. 加強內部宣導，提升人員資安意識，以防範駭客利用電子郵件進行社交工程攻擊。
- 參考資料:
  1. 附件-社交工程IoC https://cert.tanet.edu.tw/pdf/IoC_0805.rar

—- 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:20220808_01

Last update: **2022/08/08 10:02**