張貼日期：2025/01/24

【攻擊預警】社交工程攻擊通告：請加強防範以偽冒財政部名義並以稅務調查為由之社交工程郵件攻擊

- 主旨說明:【攻擊預警】社交工程攻擊通告：請加強防範以偽冒財政部名義並以稅務調查為由之社交工程郵件攻擊
- 內容說明:
  - 轉發 國家資安資訊分享與分析中心 NISAC-400-202501-00000016
  - 國家資通安全研究院近期發現，攻擊者偽冒財政部名義並以稅務調查為由，發動社交工程郵件攻擊，誘導收件者開啟並下載與執行惡意附檔。 建議貴單位加強防範與通知各單位提高警覺，避免點擊郵件附檔與連結，以免受駭。 已知攻擊郵件特徵如下，相關受駭偵測指標請參考附件。
    1. 駭客寄送之主旨：
       「稅稽徵機關調查通知」、
       「稅務抽查涉稅企業名單」
    2. 惡意附檔名稱：
       「稅務涉稅企業.pdf
       「查閱1140120.zip
       「稅務抽查涉稅企業名單.pdf
       「涉稅企業名單.zip
    3. 相關惡意中繼站:
       206[.]238[.]221[.]240
       9010[.]360sdgg[.]com
       rgghrt1140120-1336065333[.]cos[.]ap-guangzhou[.]myqcloud[.]com
       fuued5-1329400280[.]cos[.]ap-guangzhou[.]myqcloud[.]com
       6-1321729461[.]cos[.]ap-guangzhou[.]myqcloud[.]com
       00-1321729461[.]cos[.]ap-guangzhou[.]myqcloud[.]com
    4. 惡意附檔SHA1雜湊值：
       4dd2a6de2c37e63d3bc239ae50068aaecbd611e3
       5e43b6d336a98344c2429b0073899844b17332c2
       e45cd29f904ab54e0d7f831982c7a78b4a370e9d
       7629f699f10f6230d7778b4800df12d3a557f1a4
       - 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. 網路管理人員請參考受駭偵測指標，確實更新防火牆，阻擋惡意中繼站。
  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附檔。
  3. 安裝防毒軟體並更新至最新病毒碼，開啟檔案前使用防毒軟體掃描郵件附檔，並確認附檔檔案類型，若發現檔案名稱中存在異常字元(如lnk, rcs, exe, moc等可執行檔案附檔名的逆排序)，請提高警覺。
  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: 附件-社交工程攻擊_IOC https://cert.tanet.edu.tw/pdf/IoC_20250124.csv

---

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:20250124_01

Last update: **2025/01/24 14:00**