張貼日期:2019/10/24

## 【資安漏洞預警】惡意 IP 對企業 Office 365 帳號 進行暴力破解攻擊,請各單位注意防範

主旨:惡意 IP 對企業 Office 365 帳號進行暴力破解攻擊,請各單位注意防範

## 說明:

- 內容說明
  - 台灣電腦網路危機處理暨協調中心接獲國際情資,企業 Office 365 帳號遭到暴力破解攻擊, 駭客能夠利用破解的帳號,來監控企業流量、產生其他帳號或是潛入組織內部網路。
  - 目前已知會對企業 Office 365 帳號進行攻擊的 IP 如下所列:
    - **112.179.242.181**
    - **113.204.147.26**
    - 118.163.143.170
    - **120.209.20.16**
    - **175.230.213.33**
    - **201.184.241.243**
    - **218.107.49.71**
    - **218.206.132.194**
    - **218.28.50.51**
    - **218.64.165.194**
    - **220.164.2.61**
    - **220.164.2.87**
    - **221.3.236.94**
    - **222.218.17.189**
    - **222.223.56.116**
    - **42.243.154.6**
    - **58.213.46.110**
    - **59.48.82.14**
    - **60.13.154.174**
    - 61.136.104.131
    - **61.160.95.126**
    - **•** 61.163.231.150
    - **61.163.36.24**
    - **•** 61.182.82.34
    - **91.233.156.93**
    - **9**4.156.119.230
- 影響平台: Office 365
- 建議措施:
  - 1. 阻擋攻擊IP列表內的IP
  - 2. 使用多重認證
  - 3. 開啟網路日誌並保留相關資訊至少90天
  - 4. 啟用登入錯誤鎖定機制
  - 5. 使用高強度密碼

Last update: 2019/10/24 15:55

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:20191024\_01

Last update: 2019/10/24 15:55

