Date：2019/10/24

【Security Vulnerability Warning】 Brute-force attacks on Microsoft Office 365 for enterprise accounts from Malicious IPs, please be alerted

Subject: Brute-force attacks on Microsoft Office 365 for enterprise accounts from Malicious IPs, please be alerted

- Description:
  - TWCERT received cyber intelligence; Microsoft Office 365 suffered brute-force attacks. Hackers can monitoring the company traffic, generate additional accounts, or sneak into internal network by using the cracked account.
  - Currently known IPs that will attack Microsoft Office 365 are listed below:
    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
    94.156.119.230
- Impact platform: Microsoft Office 365
- Recommended practices:
  1. Block those listed IPs listed above.
  2. Apply multi-factor authentication.

3. Enable network events log and keep relevant information for at least 90 days.
4. Enable “account disable” mechanism when login error.
5. Use strong passwords.

Network System Division
Computer and Communication Center