POSTING DATE: 2025/12/16

[ATTACK WARNING] Social Engineering Attack Advisory: Enhance Defenses Against Social Engineering Emails Posing as Administrative Litigation

- Subject: [ATTACK WARNING] Social Engineering Attack Advisory: Enhance Defenses Against Social Engineering Emails Posing as Administrative Litigation

- Content Description:
  - Forwarded from National Information Security Information Sharing and Analysis Center Security Alert NISAC-400-202512-00000018
  - Our organization recently received external intelligence that attackers are launching a social engineering email campaign, posing as administrative litigation, to trick recipients into opening, downloading, and executing malicious attachments.
  - It is recommended that your unit strengthen defenses and notify all departments to remain highly vigilant, avoiding clicking on email attachments and links to prevent compromise. The known characteristics of the attack emails are as follows; please refer to the attachment for related indicators of compromise (IOCs).
  1. Subject sent by attacker: [Agency Name]
  2. Related malicious relay stations: giugh9ygiuhljbgh-1328314126[.]cos[.]ap-tokyo[.]myqcloud[.]com, 202[.]79[.]168[.]155
  3. SHA1 hashes of malicious attachments: 770e64e02d2cf2cac30d6074c201d44279996cbc, e69b347f9608abaf31cab02f0a34b3dfa1d7c872
     - Note: Related domain names are separated by “[.]” to prevent accidental clicking and triggering of connection.
- Affected Platforms:
  - N/A
- Recommended Actions:
  1. Network administrators should refer to the indicators of compromise (IOCs), update firewalls promptly, and block malicious relay stations.
  2. It is recommended to pay attention to suspicious emails, verify the correctness of the sender's address, and avoid opening emails and attachments from unknown sources.
  3. Install antivirus software and update to the latest virus definitions. Before opening a file, use antivirus software to scan the email attachment, and verify the file type. Remain vigilant if unusual characters are found in the file name (such as the reverse sorting of executable file extensions like lnk, rcs, exe, moc).
  4. Strengthen internal awareness campaigns to enhance personnel's cybersecurity awareness and prevent hackers from using email for social engineering attacks.
- Reference Material:
  - Attachment - Social Engineering Attack_IOC: https://cert.tanet.edu.tw/pdf/report_IoC_1210.csv

Computer and Communication Center
Network Systems Division, Respectfully

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251216_01

Last update: **2025/12/16 09:35**