**POSTING DATE: 2026/01/30**

# [ATTACK ALERT] Social Engineering Attack Notice: Please strengthen precautions against social engineering email attacks impersonating the Legal Affairs Committee of the Executive Yuan under the pretext of amending the "Regulations for the Receipt, Disbursement, Custody and Utilization of the Employment Stability Fund"

- Subject: [ATTACK ALERT] Social Engineering Attack Notice: Please strengthen precautions against social engineering email attacks impersonating the Legal Affairs Committee of the Executive Yuan under the pretext of amending the “Regulations for the Receipt, Disbursement, Custody and Utilization of the Employment Stability Fund”

- Content Description:
  - Forwarded from National Information Sharing and Analysis Center (NISAC) Security Alert NISAC-400-202601-00000012
  - The National Institute of Cyber Security (NICS) recently received external intelligence that attackers, using the “amendment of Article 5 of the Regulations for the Receipt, Disbursement, Custody and Utilization of the Employment Stability Fund” as a pretext, sent social engineering phishing emails containing malicious download links, inducing recipients to click on the links and download malicious files.
  - It is recommended that your unit strengthen precautions and notify all departments to increase vigilance, avoiding clicking on emails, phishing links, and attachments sent from these email accounts to prevent compromise.
  - Known characteristics of the attack-related emails are as follows:

1. Sender accounts used by hackers: “executive_yuan@boitedebijou.com.tw”, “executive-yuan@boitedebijou.com.tw”
2. Subject: “Amending Article 5 of the 'Regulations for the Receipt, Disbursement, Custody and Utilization of the Employment Stability Fund'”
3. Related malicious links: hxxps:*www[.]boitedebijou[.]com[.]tw/Mns/populace/EYG/e_detail[.]do?metaid=162736&accesskey_c=3447 - Malicious file names: “1140202422A.rar”, “1140202422A.chm” - Related malicious command and control (C2) stations: 79[.]108[.]224[.]222 - Malicious file SHA1 hashes: 73281aa5a69f2d39aa5f6e08868073a24020d677, 599217201b4db537db681a21d6115d33289eb965 * Note: Domain names are separated by “[.]” to avoid accidental clicks triggering connections. * Affected Platforms: * N/A * Recommended Actions: - Network administrators should refer to the Indicators of*

*Compromise (IoC), ensure firewalls are updated, and block malicious C2 stations. - Be alert for suspicious emails, verify the authenticity of the email source, and do not open emails or related attachments from unknown sources. - Install antivirus software and update to the latest virus signatures. Use antivirus software to scan email attachments before opening and verify the file types. If unusual characters (e.g., lnk, rcs, exe, moc, which are reverse orderings of executable file extensions) are found in file names, please be highly vigilant. - Strengthen internal training to enhance personnel cybersecurity awareness and prevent hackers from using emails for social engineering attacks. * Reference Material: * Attachment - Social Engineering Attack_IOC: https://cert.tanet.edu.tw/pdf/social_ioc_0128.csv —- Computer and Communication Center Network Systems Division, Respectfully*