CIRT Playbook Battle Card: **GSPBC-1008 - Money Mule Scams - CEO Fraud**

(P) Preparation

1. Perform routine inspections of controls/weapons
2. Perform routine phishing education
3. Conduct phishing simulations
4. Establish procedures for verifying requested financial transactions out of band
5. Log incoming and outgoing emails
6. Establish a method for users to report suspicious emails

(I) Identification

1. Monitor for:
   a. Emails with suspicious attachments
   b. Multiple identical emails sent from unknown sources
   c. Emails sent from typo domains
   d. Emails that fail SPF and/or DKIM
2. Investigate and clear ALL alerts associated with the impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Issue perimeter enforcement for known threat actor locations
5. Review email logs to identify other affected users
6. Review relevant financial transactions

(E) Eradication

1. Contact financial institutions to halt/reverse transactions

(R) Recovery

1. Blacklist sources of phishing emails
   a. Individual sending email addresses
   b. Entire sending domain, if appropriate
2. Report the incident to the appropriate law enforcement agency

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

References:

1. MITRE ATT&CK Technique T1566: https://attack.mitre.org/techniques/T1566/

Resources:

- ➔ GuardSight GSVSOC Incident Response Plan: https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan
- ➔ IT Disaster Recovery Planning: https://www.ready.gov/it-disaster-recovery-plan
- ➔ Report Cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT