CIRT Playbook Battle Card: **GSPBC-1002 - Credential Access - Spearphishing - Phishing**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Perform routine phishing education
4. Conduct phishing simulations
5. Log network traffic
6. Log incoming and outgoing emails
7. Establish a method for users to report suspicious emails
8. Incorporate threat intelligence

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Emails with suspicious attachments
   c. Multiple identical emails sent from unknown sources
   d. Emails sent from typo domains
   e. 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. Lock or reset the password of affected users if credentials were disclosed

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Inspect any attachments included in the emails
4. Perform Endpoint/AV scans on the systems of affected users
5. Review logs to identify other affected users

(R) Recovery

1. Verify any compromised credentials have been changed
2. Restore/re-image any systems with malware present
3. Blacklist sources of phishing emails
   a. Individual sending email addresses
   b. Entire sending domain, if appropriate
4. Address collateral damage

(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