CIRT Playbook Battle Card: **GSPBC-1005 - Persistence - Create Account - Backdoor User Accounts**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Ensure that servers and workstations are logging to a central location
5. Verify that security software generates alerts when privileged accounts are created
6. Remove inactive/unused accounts

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Privileged account creation
   c. Unexpected permissions changes for accounts
2. Investigate and clear ALL alerts associated with the impacted assets
3. Review log activity of the newly created account and the account that was used to create it
4. Contact users out of band to inquire about new account

(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 suspicious accounts
6. Lock any compromised accounts
7. Review the activity of newly created and compromised accounts
8. Systems believed to have malware on them should be removed from the network

(E) Eradication

1. Identify and close the initial attack vector
2. Patch asset vulnerabilities
3. Perform Endpoint/AV scans on the systems of affected users
4. Verify that any additional persistence mechanisms have been removed

(R) Recovery

1. Restore to the RPO within the RTO for affected systems
2. Address collateral damage
3. If the attacker gained Domain Admin access, reset the krbtgt user account's password

(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 T1136: https://attack.mitre.org/techniques/T1136/

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