CIRT Playbook Battle Card: **GSPBC-1021 - Privilege Escalation - Group Policy Modification**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that servers and workstations are logging to a central location
4. Audit Group Policy Object (GPO) permissions periodically
5. Use WMI and Security group filtering to limit which systems and users GPOs will apply to

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alerts
   c. IDS/IPS alerts
   d. GPO creation, deletion, or modification
   e. Creation of scheduled tasks and services
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. Lock compromised user accounts
5. Systems believed to have malware on them should be removed from the network
6. Review system logs to determine what changes the attacker made

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Create forensic backups of affected systems
4. Perform Endpoint/AV scans on affected systems
5. Audit Group Policy Objects and permissions

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the incident
4. Resolve any related security incidents
5. Restore affected systems to their last clean backup

(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 T1484 Sub-technique 001: https://attack.mitre.org/techniques/T1484/001/

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