CIRT Playbook Battle Card: **GSPBC-1014 - Impact - Inhibit System Recovery - Disabling Volume Shadow Service**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that servers are logging to a central location
4. Ensure Antivirus/Endpoint Protection software is installed on workstations
5. Verify that important data is backed up regularly
6. Ensure that accounts with administrative privileges are only used when necessary

(I) Identification

1. Monitor for:
   a. Antivirus/endpoint alerts
   b. Log messages related to system recovery services being altered or disabled
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. Temporarily remove the affected system from the network

(E) Eradication

1. Perform Endpoint/AV scans on affected systems
2. Review logs to determine the cause of the detected activity
3. Determine if any other systems or user accounts have been compromised
4. Check for altered or deleted files on the system and network shares
5. Reset any potentially compromised passwords
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the breach
4. Resolve any related security incidents

(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 T1490: https://attack.mitre.org/techniques/T1490/

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