CIRT Playbook Battle Card: **GSPBC-1013 - Impact - Defacement**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that servers are logging to a central location
4. Verify that servers are backed up on a regular basis

(I) Identification

1. Monitor for:
   a. Unplanned changes to any websites
   b. Unusual error messages in logs
   c. Unusual web traffic patterns
   d. IDS/IPS alerts
   e. Antivirus alerts
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 take down the defaced website
5. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Review logs to determine the cause of the breach
2. Perform antivirus scans on affected systems
3. Review web servers and other systems for evidence of backdoors or lateral movement
4. Verify the integrity of any data the attackers had access to
5. Reset any potentially compromised passwords
6. Patch asset vulnerabilities

(R) Recovery

1. Restore the defaced content
2. Address collateral damage
3. 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 T1491:
   https://attack.mitre.org/techniques/T1491/

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