CIRT Playbook Battle Card: **GSPBC-1009 - Persistence - Web Shells**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that servers are logging to a central location
4. Disable script execution in directories where it is not required
5. Verify that web applications do not run with excessive privileges on the server
6. Use AppArmor, SELinux, or other mitigations where appropriate

(I) Identification

1. Monitor for:
   a. Unusual error messages in logs
   b. Unusual web traffic patterns
   c. Unexpected changes in websites' document roots
   d. IPS/IDS 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. Review web logs to identify instances of the web shell being accessed
5. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Scan web servers for other instances of web shells
4. Determine how the web shell was placed on the system
5. Reset any potentially compromised passwords
6. Review logs of any system the attacker may have accessed
7. Scan affected systems with antivirus/endpoint software

(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 T1505 Sub-technique 003: https://attack.mitre.org/techniques/T1505/003/

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