CIRT Playbook Battle Card: **GSPBC-1047 - Defense Evasion - Domain Policy Modification**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure antivirus/endpoint protection software is installed on workstations and laptops
4. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required
9. Identify and correct GPO permissions abuse opportunities [1]
10. Consider implementing WMI and security filtering [1]

(I) Identification

1. Monitor for:
   a. Malicious scheduled tasks [2]
   b. Rogue Domain Controllers [2]
   c. Suspicious GPO changes [2]
   d. Commands/cmdlets and command-line arguments that may be leveraged to modify domain policy settings [2]
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(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. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Contain any DLL loaded by processes that are not supposed to be loaded by that process

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. 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
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures
5. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

References:

1. MITRE ATT&CK Mitigation 1047: https://attack.mitre.org/mitigations/M1047/
2. MITRE ATT&CK Technique 1484: https://attack.mitre.org/techniques/T1484/

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