CIRT Playbook Battle Card: **GSPBC-1017 - Credential Access - Password Spraying**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that workstations and servers are logging to a central location
4. Verify that authentication attempts to systems and applications are being logged
5. Set up network segmentation and firewalls to limit access to systems and services
6. Make use of multi-factor authentication
7. Establish and enforce a secure password policy

(I) Identification

1. Monitor for:
    a. Failed login attempts for default and common account names
    b. Failed login attempts for the same account across multiple systems
    c. Failed login attempts to multiple systems from the same source
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 logs to determine if the attacker successfully logged in to any accounts
5. Lock any compromised accounts
6. Issue perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Reset the credentials of any compromised accounts
3. Inspect any potentially compromised assets

(R) Recovery

1. Restore to the RPO within the RTO
2. Resolve any related security incidents
3. Address collateral damage

(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 T1110 Sub-technique 003: https://attack.mitre.org/techniques/T1110/003/
2. NIST Digital Identity Guidelines: https://pages.nist.gov/800-63-3/sp800-63-3.html
3. Microsoft Password Guidance: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

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