CIRT Playbook Battle Card: **GSPBC-1024 - Credential Access - OS Credential Dumping**

(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. Limit credential overlap across accounts and systems
5. Ensure that servers and workstations are logging to a central location
6. Confirm that Domain Controller backups are properly secured
7. Avoid placing domain accounts in local administrator groups across systems
8. Add users to the "Protected Users" AD security group to limit the caching of plaintext credentials
9. Consider disabling WDigest authentication and disabling or restricting NTLM

(I) Identification

1. Monitor processes and command-line arguments for indicators of credential dumping
2. Identify unexpected processes interacting with **lsass.exe**
3. Detect **Security Accounts Manager (SAM)** access on the local file system
4. Monitor domain controller logs for replication requests and unscheduled activity
5. On Windows 8.1 and Windows Server 2012 R2, monitor Windows Logs for **lsass.exe** and verify that it starts as a protected process
6. Investigate and clear ALL alerts associated with impacted assets

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Review the logs of all impacted assets
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and address collateral damage
3. Determine the root cause of the incident
4. Resolve any related security incidents
5. 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. Conduct employee security awareness training

Resources:

1. Report cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT