CIRT Playbook Battle Card: GSPBC-1039 - Lateral Movement - Use Alternate Authentication Material

(P) Preparation

1. Patch asset vulnerabilities
2. Ensure antivirus/endpoint protection software is installed on workstations and laptops
3. Confirm that servers and workstations are logging to a central location
4. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
5. Restrict access to critical assets as needed
6. Conduct employee security awareness training
7. Restrict users to the least privileges required
8. Implement file encryption for all email communications containing sensitive information
9. Use application control to whitelist approved password storage applications[1]
10. Configure strong Audit Policies[2]

(I) Identification

1. Monitor for:
   a. Abnormal access token activity[3]
   b. Unusual or suspicious API calls
   c. Abnormal logins or credential use, including any remote logins
   d. Abnormal Kerberos authentication and credential use
   e. Anomalous access of websites and cloud-based applications by the same user in different locations[4]
2. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess) environment technologies
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Archive scanning related artifacts such as IP addresses, user agents, and requests
5. Determine the source and pathway of the attack
6. Issue a perimeter enforcement for known threat actor locations

(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

References:

1. MITRE ATT&CK Mitigation M1038: https://attack.mitre.org/mitigations/M1038/
2. MITRE ATT&CK Technique T1550: https://attack.mitre.org/techniques/T1550/
3. MITRE ATT&CK Technique T1550 - 001: https://attack.mitre.org/techniques/T1550/001/
4. MITRE ATT&CK Technique T1550 - 001: https://attack.mitre.org/techniques/T1550/004/

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