CIRT Playbook Battle Card: **GSPBC-1044 - Lateral Movement - Taint Shared Content**

(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. Restrict access to shared drives to only employees requiring access [1]

(I) Identification

1. Monitor for:
   a. Suspicious processes writing or overwriting several files on a shared drive [2]
   b. Suspicious processes accessing shared drives without authorization [2]
   c. Network communications to C2 servers [2]
   d. Processes executing from removable media [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

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Temporarily remove access to the shared drive to limit further spread
3. Scan shared drives for malicious files or other files that do not belong in the shared drive [2]
4. Perform endpoint/AV scans on targeted systems
5. Reset any compromised passwords
6. Inspect ALL assets and user activity for IOC consistent with the attack profile
7. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
8. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Restore access to the shared drive to only employees requiring access
3. Address any collateral damage by assessing exposed technologies
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 professionalsImplement policy changes to reduce future risk
3. Utilize newly obtained threat signatures
4. 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 M1022: https://attack.mitre.org/mitigations/M1022/
2. MITRE ATT&CK Technique T1080: https://attack.mitre.org/techniques/T1080/

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