CIRT Playbook Battle Card: **GSPBC-1083 - Initial Access - Content Injection**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation
5. Log traffic between network segments
6. Incorporate threat intelligence
7. Perform routine inspections of asset backups
8. Conduct user security awareness training
9. Conduct response training (this PBC)
10. Where possible, ensure that online traffic is appropriately encrypted through services such as trusted VPNs[2]
11. Consider blocking download/transfer and execution of potentially uncommon file types known to be used in adversary campaigns[3]

(I) Identification

1. Monitor for:
    a. unexpected and abnormal file creations that may indicate malicious content injected through online network communications[4]
    b. other unusual network traffic that may indicate additional malicious content transferred to the system. Use network intrusion detection systems, sometimes with SSL/TLS inspection, to look for known malicious payloads, content obfuscation, and exploit code[5]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity
4. Look for behaviors on the endpoint system that might indicate successful compromise, such as abnormal behaviors of browser processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution, or evidence of Discovery[6]

(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. Fortify non-impacted critical assets

(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 (Recovery Point Objective) within the RTO (Recovery Time Objective)
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. https://attack.mitre.org/techniques/T1659/
2. https://attack.mitre.org/mitigations/M1041/
3. https://attack.mitre.org/mitigations/M1021/
4. https://attack.mitre.org/datasources/DS0022/
5. https://attack.mitre.org/datasources/DS0029/
6. https://attack.mitre.org/datasources/DS0009/