CIRT Playbook Battle Card: **GSPBC-1085 - Defense Evasion - Template 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. Network/Host intrusion prevention systems, antivirus, and detonation chambers can be employed to prevent documents from fetching and/or executing malicious payloads.[2]
11. Consider disabling Microsoft Office macros/active content to prevent the execution of malicious payloads in documents.[3]
12. Train users to identify social engineering techniques and spearphishing emails that could be used to deliver malicious documents.[4]

(I) Identification

1. Monitor for:
    a. for newly constructed network connections that are sent or received by untrusted hosts.[5]
    b. traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows.[6]
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. Analyze process behavior to determine if an Office application is performing actions, such as opening network connections, reading files, spawning abnormal child processes (ex: PowerShell), or other suspicious actions that could relate to post-compromise behavior.[7]

(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/T1221/
2. https://attack.mitre.org/mitigations/M1049
3. https://attack.mitre.org/mitigations/M1042
4. https://attack.mitre.org/mitigations/M1017
5. https://attack.mitre.org/datasources/DS0029/#Network%20Connection%20Creation
6. https://attack.mitre.org/datasources/DS0029/#Network%20Traffic%20Content
7. https://attack.mitre.org/datasources/DS0009/#Process%20Creation