CIRT Playbook Battle Card: **GSPBC-1067 - Persistence - Scheduled Task or Job**

(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. Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled[4]
9. Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process. This can be can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority[5]
10. Conduct user security awareness training
11. Conduct response training (this PBC)

(I) Identification

1. Monitor for:
    a. executed commands and arguments and newly constructed containers that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code[1]
    b. newly constructed files and changes made to files that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code[2]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. threat groups, such as Earth Lusca, have been known to establish persistence using the following command: schtasks /Create /SC ONLOgon /TN Windows UpdateCheck /TR "[filepath]" /ru [6]
4. 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
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
6. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges[3]

References:

1. https://attack.mitre.org/datasources/DS0017/
2. https://attack.mitre.org/datasources/DS0032/
3. https://attack.mitre.org/mitigations/M1047/
4. https://attack.mitre.org/mitigations/M1028/
5. https://attack.mitre.org/mitigations/M1026/
6. https://attack.mitre.org/groups/G1006/