CIRT Playbook Battle Card: **GSPBC-1073 - Privilege Escalation - Access Token Manipulation**

(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. Limit permissions so that users and user groups cannot create tokens [2]
11. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command runas [2]
12. An adversary must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require [3]

(I) Identification

1. Monitor for:
    a. changes made to AD settings that may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls [4]
    b. executed commands and arguments for token manipulation by auditing command-line activity. Specifically, analysts should look for use of the runas command. Detailed command-line logging is not enabled by default in Windows [5]
    c. API calls, loaded by a payload, for token manipulation only through careful analysis of user network activity, examination of running processes, and correlation with other endpoint and network behavior. There are many Windows API calls a payload can take advantage of to manipulate access tokens [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. Query systems for process and thread token information and look for inconsistencies such as user owns processes impersonating the local SYSTEM account [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/T1134/
2. https://attack.mitre.org/mitigations/M1026/
3. https://attack.mitre.org/mitigations/M1018/
4. https://attack.mitre.org/datasources/DS0026/
5. https://attack.mitre.org/datasources/DS0017/
6. https://attack.mitre.org/datasources/DS0009/