CIRT Playbook Battle Card: **GSPBC-1006 - Initial Access - Trusted Relationship - Vendor Access to Infrastructure**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain a list of vendors with system or network access
4. Verify that vendors only have access to necessary systems and networks
5. Isolate vendor accessible systems from the rest of the network as much as possible
6. Routinely audit vendor network access and system accounts
7. Force vendor accounts to use multifactor authentication where possible
8. Ensure all systems and network devices log to a central location

(I) Identification

1. Monitor for:
   a. Vendor access during unusual hours/days
   b. Vendor access from unusual sources (i.e. geographic locations, IPs, etc.)
   c. Attempts by vendor accounts to access other systems/networks
2. Investigate and clear ALL alerts associated with the impacted assets
3. Routinely review vendor 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. Block access from the compromised vendor
6. Lock accounts associated with the compromised vendor
7. Inform vendor of detected activity
8. Inspect all potentially compromised systems for IOCs

(E) Eradication

1. Patch asset vulnerabilities
2. Perform Endpoint/AV scans on affected systems
3. Review logs to determine extent of unauthorized activity

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Reset passwords for vendor's accounts
4. Restore necessary vendor access when safe

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals

Notes:

1. Report cybercrime: https://www.ic3.gov/default.aspx

GUARDSIGHT