CIRT Playbook Battle Card: **GSPBC-1019 - Persistence - BITS Jobs**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on systems
4. Ensure that servers and workstations are logging to a central location
5. Log network traffic

(I) Identification

1. Monitor for:
    a. Unusual DNS activity
    b. Antivirus/Endpoint alerts
    c. IDS alerts
    d. The creation of new BITS jobs
2. Investigate and clear ALL alerts associated with the impacted assets

(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. Review the suspicious BITS job
6. Lock any potentially compromised accounts
7. Systems believed to have malware on them should be removed from the network

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform Endpoint/AV scans on affected systems
4. Review logs to determine if any other systems are affected
5. Check for and remove other persistence mechanisms in place

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine how the BITS job was created
4. Resolve any related security incidents

(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