CIRT Playbook Battle Card: GSPBC-1012 - Initial Access - External Remote Services - Unauthorized VPN and VDI Access

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations and laptops
4. Prohibit non-employees from accessing company devices
5. Ensure that all remotely accessible services are logging to a central location
6. Provide security awareness training to employees
7. Use multifactor authentication where possible
8. Ensure proper network segmentation/firewall rules are in place for remote users
9. Routinely audit remote system access

(I) Identification

1. Monitor for:
   a. Remote access during unusual hours/days
   b. Remote access from unusual sources (i.e. geographic locations, IPs, etc.)
   c. Excessive failed login attempts
   d. IPS/IDS alerts
   e. Antivirus/Endpoint alerts
2. Investigate and clear ALL alerts associated with the impacted assets
3. Contact the user out of band to determine the legitimacy of the detected 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 user
6. Lock accounts associated with the compromised user
7. Inspect all potentially compromised systems for IOCs

(E) Eradication

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

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. 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