CIRT Playbook Battle Card: GSPBC-1011 - Initial Access - Drive By Compromise

(P) Preparation

1. Patch browsers and other software regularly
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Ensure that workstations are logging to a central location
5. Log network traffic
6. Set up a proxy for web traffic
7. Use Group Policy to manage security related browser settings
8. Make use of Windows Defender Exploit Guard or other exploit mitigation tools

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alerts
   c. IDS/IPS alerts
   d. User reports of unexpected behavior
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. Systems believed to have been compromised should be removed from the network

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform an antivirus scan on the affected system
4. Review logs and network traffic to identify any related malicious activity

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Reset the passwords of any accounts in use on the compromised system
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