CIRT Playbook Battle Card: **GSPBC-1007 - Persistence - Browser Extensions - Malicious Browser Extensions**

(P) Preparation

1. Patch asset vulnerabilities
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. Use Group Policy to whitelist approved browser extensions

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alerts
   c. IDS/IPS alerts
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. Identify the malicious extension
5. Issue perimeter enforcement for known threat actor locations
6. Remove the affected system from the network if necessary

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Check the system for other malicious/unapproved extensions
4. Remove the malicious extension from the system
5. Perform an antivirus scan on the affected system

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine how and why the extension was installed
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

GUARDSIGHT