CIRT Playbook Battle Card: **GSPBC-1016 - Defense Evasion - Install Root Certificate**

(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. Ensure that servers and workstations are logging to a central location
5. Maintain a list of known good root certificates
6. Check pre-installed root certificates on new devices

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Antivirus/Endpoint alerts
   c. IDS/IPS alerts
   d. An unusual absence of logs from security software
2. Periodically enumerate root certificates on devices and check for changes
3. 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. Remove the affected system from the network
5. Check for the presence of the root certificate on other systems

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Identify the origin of the potentially malicious root certificate
4. Perform Endpoint/AV scans on affected systems

(R) Recovery

1. Restore to the RPO within the RTO
2. Address collateral damage
3. Determine the root cause of the incident
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

References:

1. MITRE ATT&CK Technique T1553 Sub-technique 004: https://attack.mitre.org/techniques/T1553/004/

Resources:

- ➔ GuardSight GSVSOC Incident Response Plan: https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan
- ➔ IT Disaster Recovery Planning: https://www.ready.gov/it-disaster-recovery-plan
- ➔ Report Cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT