# CIRT Playbook Battle Card: **GSPBC-1020 - Persistence - Pre-OS Boot**

## (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. Set a BIOS or UEFI password on applicable assets
6. Use TPM technology and a trusted boot process
7. Secure local administrator accounts
8. Log any changes to boot records, BIOS, and EFI
9. Create backups of the bootloader partition

## (I) Identification

1. Monitor for:
   a. Suspicious changes to boot files
   b. Unusual DNS activity
   c. Antivirus/Endpoint alerts
   d. IDS/IPS alerts
2. Compare boot records, configuration files, and firmware against known good images
3. Perform integrity checks of pre-OS boot mechanisms
4. Utilize disk checks, forensic utilities, and data from device drivers to identify anomalies
5. 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. Remove the affected system from the network
6. Verify the boot integrity of any other at-risk assets
7. Check network logs for suspicious egress traffic

## (E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Create forensic backups of affected systems
4. Replace firmware and boot files from backups or trusted sources
5. 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
5. Restore affected systems to their last clean backup

## (L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Implement policy changes to reduce future risk
4. Conduct employee security awareness training

**References:**

1. MITRE ATT&CK Technique T1542: https://attack.mitre.org/techniques/T1542/

**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