CIRT Playbook Battle Card: **GSPBC-1027 - Impact - Disk Wipe**

(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. Regularly update virus definitions and signatures
5. Take regular backups of critical systems and ensure the hardened storage is off-site or offline
6. Develop an IT disaster recovery plan
7. Utilize threat intelligence to make informed decisions about defensive priorities
8. Ensure that servers are logging to a central location
9. Conduct employee security awareness training
10. Be aware of any laws or contractual obligations that require notification of data loss

(I) Identification

1. Monitor for:
   a. Attempts to write to the MBR or partition table
   b. Unusual kernel driver activity
   c. Direct access to drives using the “\\.\” notation
   d. IDS/IPS alerts
   e. Antivirus alerts
   f. Unusual error messages in logs
   g. Unusual web traffic patterns
2. Investigate and clear ALL alerts

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Utilize EDR hunter/killer agents to terminate offending processes
5. Remove the affected system from the network
6. Determine the source and pathway of the attack
7. Issue a perimeter enforcement for known threat actor locations
8. Determine what data was stored on the device

(E) Eradication

1. Close the attack vector
2. Create forensic backups of affected systems
3. Perform endpoint/AV scans on affected systems
4. Reset any compromised passwords
5. Inspect ALL assets and user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
7. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Restore affected systems to their last clean backup
3. Assess and Address collateral damage
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
3. Implement policy changes to reduce future risk
4. Utilize newly obtained threat signatures

References:

1. MITRE ATT&CK Technique T1561: https://attack.mitre.org/techniques/T1561/

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