CIRT Playbook Battle Card: **GSPBC-1026 - Defense Evasion - Obfuscated Files or Information**

(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. Employ a multifaceted approach to malware detection, that includes, but is not limited to:
   a. File-based detection
   b. Heuristic-based detection
   c. Network-based detection
   d. Behavior-based detection
   e. Reputation-based detection
5. Regularly update virus definitions and signatures
6. Ensure that servers and workstations are logging to a central location
7. Conduct employee security awareness training

(I) Identification

1. Flag and analyze commands that contain indicators of obfuscation or suspicious syntax
2. Use network intrusion detection systems (NIDS) and email gateway filtering to identify compressed/encrypted attachments and scripts
3. Utilize file scanning to look for known software packers and software packing techniques
4. Search system artifacts for steganography-related strings and signatures
5. Look for non-native binary formats, cross-platform compilers, and execution frameworks
6. Investigate and clear ALL alerts associated with impacted assets

(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

(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. Review the logs of all impacted assets
6. Patch asset vulnerabilities

(R) Recovery

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

References:

1. MITRE ATT&CK Technique T1027: https://attack.mitre.org/techniques/T1027/

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