CIRT Playbook Battle Card: **GSPBC-1003 - Exfiltration - Automated Exfiltration - Data Theft**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure Antivirus/Endpoint Protection software is installed on workstations
4. Provide security awareness training to employees

(I) Identification

1. Monitor for:
   a. Unusual DNS activity
   b. Unusual file system activity
   c. Unusual network activity
   d. Antivirus/endpoint 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. Issue perimeter enforcement for known threat actor locations
5. Temporarily remove affected systems from the network

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Perform Endpoint/AV scans on the systems of affected users

(R) Recovery

1. Identify the malware strain used
2. Determine what data may have been uploaded
3. Verify any compromised credentials have been changed
4. Restore/re-image any systems with malware present
5. Scan other systems and logs for known Indicators of Compromise
6. Block IP addresses associated with the malware on perimeter firewalls

(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 T1020: https://attack.mitre.org/techniques/T1020/

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