CIRT Playbook Battle Card: **GSPBC-1056 - Reconnaissance - Gather Victim Host Information**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Maintain Antivirus/EDR application updates
4. Create network segmentation
5. Log traffic between network segments
6. Incorporate threat intelligence
7. Perform routine inspections of asset backups
8. Conduct phishing simulations
9. Conduct user security awareness training
10. Conduct response training (this PBC)
11. Focus on minimizing the amount and sensitivity of data available to external parties [1]

(I) Identification

1. Monitor for:
   a. Logged network traffic in response to a scan showing both protocol header and body values that may buy and/or steal SSL/TLS certificates that can be used during targeting [2]
   b. Contextual data about an Internet-facing resource gathered from a scan, such as running services or ports that may buy, lease, rent, or compromise infrastructure that could be used during targeting [2]
2. Investigate and clear ALL alerts associated with the impacted assets or accounts
3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity

(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. Archive scanning related artifacts such as IP addresses, user agents, and requests
6. Determine the source and pathway of the attack
7. Fortify non-impacted critical assets

(E) Eradication

1. Close the attack vector by applying the Preparation steps listed above
2. Perform endpoint/AV scans on targeted systems
3. Reset any compromised passwords
4. Inspect ALL assets and user activity for IOC consistent with the attack profile
5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)
2. Address any collateral damage by assessing exposed technologies
3. Resolve any related security incidents
4. 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. Utilize newly obtained threat signatures
5. Avoid opening email and attachments from unfamiliar senders
6. Avoid opening email attachments from senders that do not normally include attachments
7. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities

References:

1. MITRE ATT&CK Mitigation M1056: https://attack.mitre.org/mitigations/M1056/
2. MITRE ATT&CK Datasource DS0035: https://attack.mitre.org/datasources/DS0035/
3. MITRE ATT&CK Technique T1592: https://attack.mitre.org/techniques/T1592/

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