CIRT Playbook Battle Card: **GSPBC-1029 - Execution - User Execution**

(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. Utilize threat intelligence to make informed decisions about defensive priorities
5. Conduct employee security awareness training
6. Consider restricting web-based content[1] that could be malicious such as:
   a. Javascript
   b. Downloads from untrusted websites
   c. Browser extensions
7. Use application control to whitelist approved applications[2]
8. Reference CIRT Playbook Battle Card: GSPBC-1002 - Credential Access - Spearphishing - Phishing[3]
9. Ensure that servers and workstations are logging to a central location

(I) Identification

1. Monitor for:
   a. Abnormal network activity
   b. Unauthorized downloads
   c. Emails with suspicious attachments
   d. IDS/IPS alerts
   e. Antivirus alerts
   f. Unusual executable files with the following file types: .exe, .doc, .pdf, .xls, .rtf, .scr, .lnk, .pif, and .cpl.[4]
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 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. 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. Assess and address collateral damage
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

References:

1. https://attack.mitre.org/mitigations/M1021/
2. https://attack.mitre.org/mitigations/M1038/
3. https://github.com/guardsight/gsvsoc_cirt-playbook-battle-cards
4. https://attack.mitre.org/techniques/T1204/002/

Resources:

- ➔ IT Disaster Recovery Planning: https://www.ready.gov/it-disaster-recovery-plan
- ➔ Report Cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT