CIRT Playbook Battle Card: **GSPBC-1031 - Persistence - Hijack Execution Flow**

(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. Conduct employee security awareness training
5. Ensure all software is kept up to date
6. Restrict the loading of remote DLLs[1]
7. Restrict users to the least privileges required
8. Ensure that servers and workstations are logging to a central location

(I) Identification

1. Monitor for:
    a. Moving, renaming, replacing, or modifying of DLLs
    b. Applications loading DLLs not consistent with past behavior
    c. DLLs that have the same file name but abnormal paths
    d. Changes to environment variables
    e. Unusual process activity
    f. Suspicious modification or creation of .manifest and .local redirection files[2]
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

(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. MITRE ATT&CK Technique M1044: https://attack.mitre.org/mitigations/M1044/
2. Dynamic-Link Library Redirection: https://docs.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-redirection?redirectedfrom=MSDN
3. MITRE ATT&CK Technique T1574: https://attack.mitre.org/techniques/T1574/

Resources:

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

GUARDSIGHT

© GuardSight, Inc.® | https://www.guardsight.com