CIRT Playbook Battle Card: **GSPBC-1042 - Lateral Movement - Replication Through Removable Media**

(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. Confirm that servers and workstations are logging to a central location
5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment
6. Restrict access to critical assets as needed
7. Conduct employee security awareness training
8. Restrict users to the least privileges required
9. Limit the use of USB devices and removable media within a network
10. Block untrusted executables from running from removable media [1]

(I) Identification

1. Monitor for:
   a. Unusual file access on removable media [1]
   b. Processes that execute from removable media after it is mounted [1]
   c. Network connections to command and control servers [1]
   d. Processes involving unusual system and network information discovery [1]
2. Investigate and clear ALL alerts associated with the impacted assets
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

(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 within the RTO
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. 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 Technique 1091: https://attack.mitre.org/techniques/T1091/
2. Deny All Access to Removable Devices or Media: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc772540(v=ws.10)
3. Disable the Autorun functionality in Windows: https://support.microsoft.com/en-us/topic/how-to-disable-the-autorun-functionality-in-windows-8e5ff0da-c526-7624-c064-ff82aecfd145

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