CIRT Playbook Battle Card: GSPBC-1022 - Defense Evasion - Process Injection

(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. Secure local administrator accounts
5. Ensure that servers and workstations are logging to a central location
6. Configure endpoint security solutions to detect and block process injection behaviors
7. On Unix-based operating systems, restrict the use of **ptrace** to privileged users
8. Utilize Yama or other Linux security modules to configure advanced access control and process restrictions

(I) Identification

1. Monitor for the following Windows API calls:
    a. **CreateRemoteThread**
    b. **SuspendThread**
    c. **SetThreadContext**
    d. **ResumeThread**
    e. **QueueUserAPC**
    f. **NtQueueApcThread**
    g. **VirtualAllocEx**
    h. **WriteProcessMemory**
2. On Linux systems, monitor the **ptrace** system call
3. Detect named pipe creation and connection events
4. Collect DLL/PE file events
5. Analyze process behavior and compare to expected activity
6. Investigate and clear ALL alerts associated with impacted assets

(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. Review the logs of all impacted assets
6. Patch asset vulnerabilities

(R) Recovery

1. Restore to the RPO within the RTO
2. Assess and address collateral damage
3. Determine the root cause of the incident
4. Resolve any related security incidents
5. 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. Conduct employee security awareness training

Resources:

1. Yama security module guide: https://www.kernel.org/doc/html/latest/admin-guide/LSM/Yama.html
2. Report cybercrime: https://www.ic3.gov/Home/FAQ