# CIRT Playbook Battle Card: **GSPBC-1028 - Persistence - Office Application Startup**

## (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. Disable add-ins and prevent Office VBA macros from executing
   a. If add-ins are necessary, follow best practices for securing them, such as requiring them to be signed
   b. NOTE: disabling add-ins in the Office Trust Center does not disable WLL nor does it prevent VBA code
6. Ensure that servers and workstations are logging to a central location
7. Create the registry key for the Office Test [2] method and set the permissions to "Read Control"

## (I) Identification

1. Monitor for:
   a. Abnormal chains of activity resulting from Office processes
   b. Events related to Registry key creation and modification
   c. Office processes performing anomalous DLL loads
   d. Changes to Office macro security settings or base templates
2. Check for the creation of the Office Test key
   a. TIP: Sysinternals Autoruns [3] can detect tasks set up using the Office Test Registry key
3. Audit Registry entries that are relevant to enabling add-ins
4. Validate Office trusted locations
5. 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 T1137: https://attack.mitre.org/techniques/T1137/
2. Office Test Sub-technique T1137.002: https://attack.mitre.org/techniques/T1137/002/
3. Sysinternals Autoruns: https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

**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