

CIRT Playbook Battle Card: GSPBC-1032 - Resource Development - Compromise Accounts

(P) Preparation	(I) Identification	(C) Containment
<ol style="list-style-type: none"> 1. Patch asset vulnerabilities 2. Enforce strong password policies <ol style="list-style-type: none"> a. Don't allow the usage of old passwords b. Cycle passwords according to the organization's best practices c. Enforce alpha-numeric passwords, with symbols, and longer than 8 characters 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 RDP, SSH, and similar protocols 7. Conduct employee security awareness training 8. Restrict users to the least privileges required 	<ol style="list-style-type: none"> 1. Monitor: <ol style="list-style-type: none"> a. Social media activity related to your organization^[1] b. Suspicious emails and attachments coming into your organization^[2] 2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior^[3] 3. Analyze web application metadata for suspicious user-agent strings and other artifacts 4. Investigate and clear ALL alerts 	<ol style="list-style-type: none"> 1. Inventory (enumerate & assess) environment technologies 2. Detect Deny Disrupt Degrade Deceive Destroy 3. Observe -> Orient -> Decide -> Act 4. Archive scanning related artifacts such as IP addresses, user agents, and requests 5. Determine the source and pathway of the attack 6. Issue a perimeter enforcement for known threat actor locations
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 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 <div data-bbox="1392 967 2043 1268"> <p>References:</p> <ol style="list-style-type: none"> 1. MITRE ATT&CK Technique T1586: https://attack.mitre.org/techniques/T1586/ 2. Compromise Account Sub-technique T1586.002: https://attack.mitre.org/techniques/T1586/002/ 3. Compromise Account Sub-technique T1586.001: https://attack.mitre.org/techniques/T1586/001/ </div>

Resources:

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