| (P) Preparation | (I) Identification | (C) Containment |
|---|---|---|
| 1. Patch asset vulnerabilities<br>2. Ensure antivirus/endpoint protection software is installed on workstations and laptops<br>3. Confirm that servers and workstations are logging to a central location<br>4. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment<br>5. Restrict access to critical assets as needed<br>6. Conduct employee security awareness training<br>7. Restrict users to the least privileges required | 1. Monitor for:<br>   a. Malicious tasklist commands ran in Windows environment [1]<br>   b. Malicious ps commands ran in Mac and Linux environments [1]<br>   c. Actions that could be taken to gather system and network information [1]<br>   d. Attempts by programs to exfiltrate process memory [1]<br>2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior<br>3. Analyze web application metadata for suspicious user-agent strings and other artifacts<br>4. Investigate and clear ALL alerts<br>5. Investigate information provided by Windows Management Instrumentation and Windows API via PowerShell [1] | 1. Inventory (enumerate & assess) environment technologies<br>2. Detect \| Deny \| Disrupt \| Degrade \| Deceive \| Destroy<br>3. Observe -> Orient -> Decide -> Act<br>4. Archive scanning related artifacts such as IP addresses, user agents, and requests<br>5. Determine the source and pathway of the attack<br>6. Issue a perimeter enforcement for known threat actor locations |
| (E) Eradication | (R) Recovery | (L) Lessons/Opportunities |
| 1. Close the attack vector by applying the Preparation steps listed above<br>2. Perform endpoint/AV scans on targeted systems<br>3. Reset any compromised passwords<br>4. Inspect ALL assets and user activity for IOC consistent with the attack profile<br>5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery<br>6. Patch asset vulnerabilities | 1. Restore to the RPO within the RTO<br>2. Address any collateral damage by assessing exposed technologies<br>3. Resolve any related security incidents<br>4. Restore affected systems to their last clean backup | 1. Perform routine cyber hygiene due diligence<br>2. Engage external cybersecurity-as-a-service providers and response professionals<br>3. Implement policy changes to reduce future risk<br>4. Utilize newly obtained threat signatures<br>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 [1] |

**References:**
1. MITRE ATT&CK Technique 1057: https://attack.mitre.org/techniques/T1057/

**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