

# CIRT Playbook Battle Card: GSPBC-1038 - Credential Access - Steal Web Session Cookies

(P) Preparation	(I) Identification	(C) Containment
<ol style="list-style-type: none"> <li>1. Patch asset vulnerabilities</li> <li>2. Ensure antivirus/endpoint protection software is installed on workstations and laptops</li> <li>3. Confirm that servers and workstations are logging to a central location</li> <li>4. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment</li> <li>5. Restrict access to critical assets as needed</li> <li>6. Conduct employee security awareness training</li> <li>7. Restrict users to the least privileges required</li> <li>8. Configure browsers or tasks to delete persistent cookies regularly<sup>[1]</sup></li> <li>9. Consider setting up a physical second-factor key that uses the target login domain as part of the negotiation protocol<sup>[1]</sup></li> </ol>	<ol style="list-style-type: none"> <li>1. Monitor for:               <ol style="list-style-type: none"> <li>a. Attempts to access files and repositories on a local system that are used to store browser session cookies<sup>[1]</sup></li> <li>b. Attempts by programs to inject into or dump browser process memory<sup>[1]</sup></li> </ol> </li> <li>2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior</li> <li>3. Analyze web application metadata for suspicious user-agent strings and other artifacts</li> <li>4. Investigate and clear ALL alerts</li> </ol>	<ol style="list-style-type: none"> <li>1. Inventory (enumerate &amp; assess) environment technologies</li> <li>2. Detect   Deny   Disrupt   Degrade   Deceive   Destroy</li> <li>3. Observe -&gt; Orient -&gt; Decide -&gt; Act</li> <li>4. Archive scanning related artifacts such as IP addresses, user agents, and requests</li> <li>5. Determine the source and pathway of the attack</li> <li>6. Issue a perimeter enforcement for known threat actor locations</li> </ol>
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<ol style="list-style-type: none"> <li>1. Close the attack vector by applying the Preparation steps listed above</li> <li>2. Perform endpoint/AV scans on targeted systems</li> <li>3. Reset any compromised passwords</li> <li>4. Inspect ALL assets and user activity for IOC consistent with the attack profile</li> <li>5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery</li> <li>6. Patch asset vulnerabilities</li> </ol>	<ol style="list-style-type: none"> <li>1. Restore to the RPO within the RTO</li> <li>2. Address any collateral damage by assessing exposed technologies</li> <li>3. Resolve any related security incidents</li> <li>4. Restore affected systems to their last clean backup</li> </ol>	<ol style="list-style-type: none"> <li>1. Perform routine cyber hygiene due diligence</li> <li>2. Engage external cybersecurity-as-a-service providers and response professionals</li> <li>3. Implement policy changes to reduce future risk</li> <li>4. Utilize newly obtained threat signatures</li> <li>5. Train users to identify aspects of phishing attempts where they're asked to enter credentials into a site that has the incorrect domain for the application they are logging into<sup>[1]</sup></li> </ol> <div data-bbox="1392 1094 2045 1214"> <p>References:</p> <ol style="list-style-type: none"> <li>1. MITRE ATT&amp;CK Technique T1539: <a href="https://attack.mitre.org/techniques/T1539/">https://attack.mitre.org/techniques/T1539/</a></li> </ol> </div>

## Resources:

- GuardSight GSVSOC Incident Response Plan: [https://github.com/guardsight/gsvsoc\\_cybersecurity-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>