

(P) Preparation	(I) Identification	(C) Containment
<div>1. Patch asset vulnerabilities</div> <div>2. Perform routine inspections of controls/weapons</div> <div>3. Ensure Antivirus/Endpoint Protection software is installed on workstations</div> <div>4. Ensure that workstations are logging to a central location</div> <div>5. Log network traffic</div> <div>6. Use Group Policy to whitelist approved browser extensions</div>	<div>1. Monitor for:<div>a. Unusual DNS activity</div><div>b. Antivirus/Endpoint alerts</div><div>c. IDS/IPS alerts</div></div> <div>2. Investigate and clear ALL alerts associated with the impacted assets</div>	<div>1. Inventory (enumerate &amp; assess)</div> <div>2. Detect   Deny   Disrupt   Degrade   Deceive   Destroy</div> <div>3. Observe -&gt; Orient -&gt; Decide -&gt; Act</div> <div>4. Identify the malicious extension</div> <div>5. Issue perimeter enforcement for known threat actor locations</div> <div>6. Remove the affected system from the network if necessary</div>
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<div>1. Close the attack vector</div> <div>2. Patch asset vulnerabilities</div> <div>3. Check the system for other malicious/unapproved extensions</div> <div>4. Remove the malicious extension from the system</div> <div>5. Perform an antivirus scan on the affected system</div>	<div>1. Restore to the RPO within the RTO for affected systems</div> <div>2. Address collateral damage</div> <div>3. Determine how and why the extension was installed</div> <div>4. Resolve any related security incidents</div>	<div>1. Perform routine cyber hygiene due diligence</div> <div>2. Engage external cybersecurity-as-a-service providers and response professionals</div> <div><div>References:<div>1. MITRE ATT&amp;CK Technique T1176:<div>https://attack.mitre.org/techniques/T1176/</div></div></div></div>

**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