

(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 systems</div> <div>4. Ensure that servers and workstations are logging to a central location</div> <div>5. Log network traffic</div>	<div>1. Monitor for:<div><div>a. Unusual DNS activity</div><div>b. Antivirus/Endpoint alerts</div><div>c. IDS alerts</div><div>d. The creation of new BITS jobs</div></div></div> <div>2. Investigate and clear ALL alerts associated with the impacted assets</div>	<div>1. Inventory (enumerate & assess)</div> <div>2. Detect Deny Disrupt Degrade Deceive Destroy</div> <div>3. Observe -> Orient -> Decide -> Act</div> <div>4. Issue perimeter enforcement for known threat actor locations</div> <div>5. Review the suspicious BITS job</div> <div>6. Lock any potentially compromised accounts</div> <div>7. Systems believed to have malware on them should be removed from the network</div>
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<div>1. Close the attack vector</div> <div>2. Patch asset vulnerabilities</div> <div>3. Perform Endpoint/AV scans on affected systems</div> <div>4. Review logs to determine if any other systems are affected</div> <div>5. Check for and remove other persistence mechanisms in place</div>	<div>1. Restore to the RPO within the RTO</div> <div>2. Address collateral damage</div> <div>3. Determine how the BITS job was created</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&CK Technique T1197: https://attack.mitre.org/techniques/T1197/</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>