SOC Use Case Report

UC-027: BITS Job Persistence

Author	Abishek V
Date	6 feb 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Logs / BITS Telemetry
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-027
Use Case Name	BITS Job Persistence
Category	Persistence / Living-off-the-Land
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	High

BITS jobs can persist across reboots and user logouts. Attackers abuse this capability to maintain persistence or repeatedly retrieve payloads.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User: `clair`
- Utility observed: `bitsadmin.exe`
- Activity: Persistent BITS job configured

SOC risk point: Persistent BITS jobs may execute repeatedly without user interaction.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs
- BITS operational logs
- Process creation events (4688)

Key Indicators

BITS Job Creation	Background transfer job observed
Persistence Flags	Job set to resume automatically
External Source	Repeated contact with remote server

4. Detection Logic

Trigger when:

- BITS jobs are created with persistence attributes
- jobs point to external or suspicious URLs

5. SOC L1 Playbook

Phase A: Triage

1. Identify BITS job owner and creation time
2. Review job parameters and persistence settings
3. Confirm associated process and user

Phase B: Investigation

1. Determine purpose of BITS job
2. Review destination URL and downloaded content
3. Check for job execution across reboots
4. Correlate with other persistence mechanisms

6. Evidence Timeline

Time	Event ID	Source	Observation
11:04:12	4688	bitsadmin.exe	Persistent job created
11:04:30	–	BITS	Job scheduled for retry
11:15:42	–	BITS	Job resumed automatically

Outcome: Unauthorized persistent BITS job detected. Classified as persistence technique.

7. False Positive Checks

- enterprise update mechanisms
- patch management tools
- approved software installers

8. Verdict Criteria

True Positive if:

- job persists without business justification
- external or suspicious source involved
- correlated with other malicious indicators

9. SOC Response Actions

- cancel and remove BITS job
- block remote destination
- scan endpoint for malware
- escalate to incident response

10. Ticket Notes

Ticket: UC-027 BITS Job Persistence Detected
Severity: High
Verdict: True Positive