SOC Use Case Report

UC-026: BITSAdmin Download File

Author	Abishek V
Date	5 Feb 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Logs / Process Telemetry
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-026
Use Case Name	BITSAdmin Download File
Category	Living-off-the-Land / Defense Evasion
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium → High

BITSAdmin is a legitimate Windows utility that can be abused by attackers to download payloads while blending into normal background network activity.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User: `clair`
- Process observed: `bitsadmin.exe`
- Activity: File downloaded from external URL

SOC risk point: BITSAdmin is commonly abused to retrieve malware payloads due to its trusted behavior and low visibility.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs
- Process creation logs (4688)
- Network telemetry

Key Indicators

bitsadmin.exe Execution	LOLBAS usage detected
External URL	Download from non-corporate source
Suspicious File Path	Payload saved to temp or user directory

4. Detection Logic

Trigger when:

- `bitsadmin.exe` executes with download arguments
- destination URL is external or low-reputation

5. SOC L1 Playbook

Phase A: Triage

1. Identify command-line arguments
2. Identify destination URL and file path
3. Confirm user and endpoint context

Phase B: Investigation

1. Validate whether BITSAdmin usage is authorized
2. Review downloaded file type and hash
3. Correlate with follow-on execution activity
4. Scope similar activity across environment

6. Evidence Timeline

Time	Event ID	Process	Observation
10:12:31	4688	bitsadmin.exe	Download job created
10:12:45	–	network	External file retrieved
10:13:02	4688	cmd.exe	Post-download execution attempt

Outcome: Unauthorized BITSAdmin file download detected. Escalation required.

7. False Positive Checks

- approved patching or update tasks
- legacy application installers
- admin-approved scripts

8. Verdict Criteria

True Positive if:

- download source is untrusted
- file is executable or suspicious
- follow-on execution observed

9. SOC Response Actions

- quarantine downloaded file
- block source URL or IP
- isolate endpoint if execution occurred
- escalate to incident response

10. Ticket Notes

Ticket: UC-026 BITSAdmin Download Detected
Severity: High
Verdict: True Positive