Detect abuse of Windows BITS Jobs for download, execution and persistence, Detection Strategy DET0098

Archived: 2026-04-05 16:44:07 UTC

AN0274

Behavioral chain: (1) An actor creates or modifies a BITS job via bitsadmin.exe, PowerShell BITS cmdlets, or COM; (2) the job performs HTTP(S)/SMB network transfers while the owning user is logged on; (3) upon job completion/error, BITS launches a notify command (SetNotifyCmdLine) from svchost.exe -k netsvcs -s BITS, often establishing persistence by keeping long-lived jobs. The strategy correlates process creation, command/script telemetry, BITS-Client operational events, and network connections initiated by BITS.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window linking job creation, transfer, and notify execution (e.g., 30m–24h depending on environment and BITS retry behavior).
ExpectedUpdateHosts	Allow-list of corporate update/CDN endpoints that legitimately use BITS (WSUS, MEMCM, vendor updaters).
SuspiciousCliSwitches	BITSAdmin flags of interest (/transfer, /addfile, /SetNotifyCmdLine, /resume, /setcustomheaders, /setminretrydelay).
NotifyCmdBlockList	Known risky binaries or folders (e.g., %TEMP%*.exe, powershell.exe, cmd.exe) used as BITS notify commands.
UserContext	Scope by interactive users, service accounts, or high-value targets (admins/servers) to reduce benign noise.
ExternalNetCIDRs	Definition of external/non-corp destinations for network correlation.
JobLifetimeThreshold	Maximum age or retry count for benign jobs before flagging persistence (e.g., >3 days or retry>20).