BITS Jobs, Technique T1197 - Enterprise

Archived: 2026-04-05 12:34:47 UTC

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM).[1][2] BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

The interface to create and manage BITS jobs is accessible through PowerShell and the BITSAdmin tool.[2][3]

Adversaries may abuse BITS to download (e.g. Ingress Tool Transfer), execute, and even clean up after running malicious code (e.g. Indicator Removal). BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls.[4][5][6] BITS enabled execution may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots).[7][4]

BITS upload functionalities can also be used to perform Exfiltration Over Alternative Protocol.[4]
