Archive Collected Data: Archive via Library, Sub-technique T1560.002 - Enterprise

Archived: 2026-04-05 15:06:52 UTC

An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party libraries. Many libraries exist that can archive data, including Python rarfile [1], libzip [2], and zlib [3]. Most libraries include functionality to encrypt and/or compress data.

Some archival libraries are preinstalled on systems, such as bzip2 on macOS and Linux, and zip on Windows. Note that the libraries are different from the utilities. The libraries can be linked against when compiling, while the utilities require spawning a subshell, or a similar execution mechanism.

Source: https://attack.mitre.org/techniques/T1560/002