# TTP Detail – T1560.002

## TTP Information

Name: Archive via Library

Description: 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](https://attack.mitre.org/techniques/T1059/006) rarfile (Citation: PyPI RAR), libzip (Citation: libzip), and zlib (Citation: Zlib Github). 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.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* BADFLICK
* BBSRAT
* Cardinal RAT
* Denis
* Epic
* FoggyWeb
* FunnyDream
* InvisiMole
* LunarWeb
* OSX\_OCEANLOTUS.D
* SeaDuke
* TajMahal
* ZLib

## APTs (Intrusion Sets)

* Lazarus Group
* Threat Group-3390