# TTP Detail – T1560.001

## TTP Information

Name: Archive via Utility

Description: Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration. Many utilities include functionalities to compress, encrypt, or otherwise package data into a format that is easier/more secure to transport.

Adversaries may abuse various utilities to compress or encrypt data before exfiltration. Some third party utilities may be preinstalled, such as <code>tar</code> on Linux and macOS or <code>zip</code> on Windows systems.

On Windows, <code>diantz</code> or <code> makecab</code> may be used to package collected files into a cabinet (.cab) file. <code>diantz</code> may also be used to download and compress files from remote locations (i.e. [Remote Data Staging](https://attack.mitre.org/techniques/T1074/002)).(Citation: diantz.exe\_lolbas) <code>xcopy</code> on Windows can copy files and directories with a variety of options. Additionally, adversaries may use [certutil](https://attack.mitre.org/software/S0160) to Base64 encode collected data before exfiltration.

Adversaries may use also third party utilities, such as 7-Zip, WinRAR, and WinZip, to perform similar activities.(Citation: 7zip Homepage)(Citation: WinRAR Homepage)(Citation: WinZip Homepage)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* AppleSeed
* CORALDECK
* Calisto
* Crutch
* Daserf
* DustySky
* IceApple
* InvisiMole
* LunarWeb
* Micropsia
* Octopus
* Okrum
* OopsIE
* PUNCHBUGGY
* PoetRAT
* PowerShower
* Ramsay
* Sagerunex
* SampleCheck5000
* Turian
* WindTail
* ccf32
* iKitten

## Tools

* PoshC2
* Pupy
* Rclone
* certutil

## APTs (Intrusion Sets)

* APT1
* APT28
* APT3
* APT33
* APT39
* APT41
* APT5
* Agrius
* Akira
* Aquatic Panda
* BRONZE BUTLER
* Chimera
* CopyKittens
* Earth Lusca
* FIN13
* FIN8
* Fox Kitten
* GALLIUM
* Gallmaker
* HAFNIUM
* INC Ransom
* Ke3chang
* Kimsuky
* Lotus Blossom
* Magic Hound
* MuddyWater
* Mustang Panda
* Play
* RedCurl
* Sea Turtle
* Sowbug
* ToddyCat
* Turla
* Volt Typhoon
* Wizard Spider
* menuPass