# TTP Detail – T1074.002

## TTP Information

Name: Remote Data Staging

Description: Adversaries may stage data collected from multiple systems in a central location or directory on one system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.

In cloud environments, adversaries may stage data within a particular instance or virtual machine before exfiltration. An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and stage data in that instance.(Citation: Mandiant M-Trends 2020)

By staging data on one system prior to Exfiltration, adversaries can minimize the number of connections made to their C2 server and better evade detection.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* ccf32

## APTs (Intrusion Sets)

* APT28
* Chimera
* FIN6
* FIN8
* Leviathan
* MoustachedBouncer
* Sea Turtle
* Threat Group-3390
* ToddyCat
* menuPass