# TTP Detail – T1074.001

## TTP Information

Name: Local Data Staging

Description: Adversaries may stage collected data in a central location or directory on the local 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.  
  
Adversaries may also stage collected data in various available formats/locations of a system, including local storage databases/repositories or the Windows Registry.(Citation: Prevailion DarkWatchman 2021)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* ADVSTORESHELL
* AppleSeed
* Astaroth
* Attor
* AuTo Stealer
* BADNEWS
* BadPatch
* BoxCaon
* CHIMNEYSWEEP
* Calisto
* Carbon
* Catchamas
* Chrommme
* Crutch
* Cuckoo Stealer
* DarkWatchman
* Dtrack
* Duqu
* DustySky
* Dyre
* ECCENTRICBANDWAGON
* Elise
* Exaramel for Windows
* FLASHFLOOD
* FrameworkPOS
* FunnyDream
* Gold Dragon
* Helminth
* InvisiMole
* KGH\_SPY
* KOPILUWAK
* Kazuar
* LightNeuron
* LoFiSe
* Lumma Stealer
* LunarMail
* MESSAGETAP
* MacMa
* Machete
* Mafalda
* MarkiRAT
* Milan
* Mis-Type
* MoonWind
* NETWIRE
* NOKKI
* NavRAT
* NightClub
* ObliqueRAT
* Octopus
* OilBooster
* OopsIE
* PACEMAKER
* PUNCHBUGGY
* PUNCHTRACK
* PoisonIvy
* PowerLess
* Prikormka
* Pteranodon
* QakBot
* RainyDay
* Ramsay
* RawPOS
* Rover
* SLIGHTPULSE
* SLOWPULSE
* SPACESHIP
* STARWHALE
* SUGARDUMP
* Sagerunex
* SampleCheck5000
* SocGholish
* SombRAT
* Trojan.Karagany
* Troll Stealer
* Turian
* USBStealer
* Ursnif
* VersaMem
* Zebrocy
* ccf32
* metaMain

## APTs (Intrusion Sets)

* APT28
* APT3
* APT39
* APT5
* Agrius
* BackdoorDiplomacy
* Chimera
* Dragonfly
* FIN13
* FIN5
* GALLIUM
* Indrik Spider
* Kimsuky
* Lazarus Group
* Leviathan
* Lotus Blossom
* MuddyWater
* Mustang Panda
* Patchwork
* Sidewinder
* Storm-1811
* TeamTNT
* Threat Group-3390
* Volt Typhoon
* Wizard Spider
* menuPass