# TTP Detail – T1005

## TTP Information

Name: Data from Local System

Description: Adversaries may search local system sources, such as file systems, configuration files, local databases, or virtual machine files, to find files of interest and sensitive data prior to Exfiltration.

Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show\_run\_config\_cmd\_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* Action RAT
* Amadey
* AppleSeed
* AuTo Stealer
* BADFLICK
* BADNEWS
* BLINDINGCAN
* BadPatch
* Bandook
* Bankshot
* Bazar
* Bisonal
* BlackMould
* BoxCaon
* Bumblebee
* CHIMNEYSWEEP
* Calisto
* Caterpillar WebShell
* CharmPower
* China Chopper
* Chrommme
* Clambling
* Cobalt Strike
* CookieMiner
* CosmicDuke
* CreepyDrive
* Crimson
* Crutch
* Cryptoistic
* Cyclops Blink
* DRATzarus
* DUSTTRAP
* DanBot
* DarkGate
* DarkWatchman
* DnsSystem
* Drovorub
* Dtrack
* EnvyScout
* FLASHFLOOD
* FatDuke
* Flagpro
* FlawedAmmyy
* FoggyWeb
* FrameworkPOS
* FunnyDream
* Gelsemium
* Goopy
* GravityRAT
* Green Lambert
* GrimAgent
* Hikit
* Hydraq
* IPsec Helper
* IceApple
* InvisiMole
* Ixeshe
* KGH\_SPY
* KONNI
* KOPILUWAK
* Kazuar
* Kevin
* Latrodectus
* LightNeuron
* Linfo
* LoFiSe
* MacMa
* Machete
* Mafalda
* MarkiRAT
* MgBot
* Milan
* Mis-Type
* Misdat
* MobileOrder
* Mongall
* Nebulae
* Neoichor
* NightClub
* OSX\_OCEANLOTUS.D
* Octopus
* OutSteel
* P.A.S. Webshell
* POWERSTATS
* PUNCHTRACK
* Pasam
* Pcexter
* Pillowmint
* PinchDuke
* PingPull
* PoisonIvy
* PowerLess
* Proxysvc
* QakBot
* QuietSieve
* RAPIDPULSE
* RCSession
* ROKRAT
* Raccoon Stealer
* RainyDay
* Ramsay
* RawPOS
* Rising Sun
* Rover
* SDBbot
* SLIGHTPULSE
* SLOTHFULMEDIA
* STARWHALE
* SUNBURST
* SVCReady
* Saint Bot
* Samurai
* Sardonic
* Shark
* SharpDisco
* ShimRat
* SideTwist
* SombRAT
* SpicyOmelette
* StealBit
* StrifeWater
* SysUpdate
* Taidoor
* TajMahal
* ThreatNeedle
* TinyTurla
* Tomiris
* TrickBot
* Troll Stealer
* USBferry
* Uroburos
* Ursnif
* WarzoneRAT
* WellMail
* WellMess
* Woody RAT
* XCSSET
* Zox
* ZxShell
* ZxxZ
* ccf32
* metaMain
* njRAT
* xCaon
* yty

## Tools

* Brute Ratel C4
* Forfiles
* Koadic
* MCMD
* NPPSPY
* Out1
* PcShare
* PowerSploit
* QuasarRAT
* Wevtutil
* esentutl

## APTs (Intrusion Sets)

* APT1
* APT28
* APT29
* APT3
* APT37
* APT38
* APT39
* APT41
* Agrius
* Andariel
* Aquatic Panda
* Axiom
* BRONZE BUTLER
* CURIUM
* Dark Caracal
* Dragonfly
* Ember Bear
* FIN13
* FIN6
* FIN7
* Fox Kitten
* GALLIUM
* Gamaredon Group
* HAFNIUM
* Inception
* Ke3chang
* Kimsuky
* LAPSUS$
* Lazarus Group
* LuminousMoth
* Magic Hound
* OilRig
* Patchwork
* RedCurl
* Sandworm Team
* Stealth Falcon
* Threat Group-3390
* ToddyCat
* Turla
* Volt Typhoon
* Windigo
* Wizard Spider
* menuPass