# TTP Detail – T1105

## TTP Information

Name: Ingress Tool Transfer

Description: Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)).

On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as <code>IEX(New-Object Net.WebClient).downloadString()</code> and <code>Invoke-WebRequest</code>. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105\_lolbas) A number of these tools, such as `wget`, `curl`, and `scp`, also exist on ESXi. After downloading a file, a threat actor may attempt to verify its integrity by checking its hash value (e.g., via `certutil -hashfile`).(Citation: Google Cloud Threat Intelligence COSCMICENERGY 2023)

Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://attack.mitre.org/techniques/T1204) (typically after interacting with [Phishing](https://attack.mitre.org/techniques/T1566) lures).(Citation: T1105: Trellix\_search-ms)

Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: command-and-control

## Malware

* ABK
* ANDROMEDA
* Action RAT
* Agent Tesla
* Agent.btz
* Amadey
* Anchor
* Aria-body
* Astaroth
* Attor
* AuditCred
* Avenger
* Azorult
* BADFLICK
* BADHATCH
* BADNEWS
* BBK
* BISCUIT
* BLINDINGCAN
* BLUELIGHT
* BONDUPDATER
* BUSHWALK
* BabyShark
* BackConfig
* Backdoor.Oldrea
* BadPatch
* Bandook
* Bankshot
* Bazar
* BendyBear
* Bisonal
* BlackMould
* Bonadan
* BoomBox
* BoxCaon
* Briba
* Bumblebee
* Bundlore
* CARROTBAT
* CHIMNEYSWEEP
* CHOPSTICK
* CORESHELL
* Calisto
* CallMe
* Cannon
* Carberp
* Cardinal RAT
* Caterpillar WebShell
* ChChes
* Chaes
* CharmPower
* China Chopper
* Chrommme
* CloudDuke
* Cobalt Strike
* CoinTicker
* Conficker
* CookieMiner
* CostaBricks
* CreepyDrive
* Crimson
* Cryptoistic
* Cuba
* Cyclops Blink
* DDKONG
* DEATHRANSOM
* DOGCALL
* DRATzarus
* DUSTTRAP
* Dacls
* DanBot
* DarkComet
* DarkGate
* DarkTortilla
* Daserf
* Denis
* Diavol
* Dipsind
* Disco
* DnsSystem
* Doki
* Downdelph
* DropBook
* Drovorub
* Dtrack
* Dyre
* EVILNUM
* Ecipekac
* Egregor
* Elise
* Emissary
* Emotet
* EvilBunny
* Exaramel for Linux
* Explosive
* FELIXROOT
* FYAnti
* Felismus
* Flagpro
* FlawedAmmyy
* FoggyWeb
* FunnyDream
* Gazer
* Gelsemium
* Gold Dragon
* GoldMax
* GoldenSpy
* Gootloader
* Grandoreiro
* GreyEnergy
* GrimAgent
* GuLoader
* H1N1
* HAPPYWORK
* HOPLIGHT
* HTTPBrowser
* Hancitor
* Hannotog
* Helminth
* Hi-Zor
* HiddenWasp
* Hikit
* Hildegard
* HotCroissant
* Hydraq
* HyperBro
* IMAPLoader
* IcedID
* Industroyer
* InvisiMole
* Ixeshe
* JHUHUGIT
* JPIN
* JSS Loader
* Javali
* KARAE
* KEYMARBLE
* KGH\_SPY
* KOCTOPUS
* KONNI
* Kasidet
* Kazuar
* Kerrdown
* Kessel
* Kevin
* KeyBoy
* Kinsing
* Kivars
* Kwampirs
* LOWBALL
* Latrodectus
* LightNeuron
* LightSpy
* Linfo
* LiteDuke
* LitePower
* Lizar
* Lokibot
* LoudMiner
* Lucifer
* MacMa
* Machete
* Mafalda
* MagicRAT
* MarkiRAT
* MechaFlounder
* Melcoz
* Metamorfo
* Meteor
* Micropsia
* Milan
* MiniDuke
* Mis-Type
* Misdat
* Mivast
* MobileOrder
* MoleNet
* Mongall
* More\_eggs
* Mosquito
* NDiskMonitor
* NETWIRE
* NICECURL
* NOKKI
* NanHaiShu
* NanoCore
* NavRAT
* Nebulae
* Neo-reGeorg
* Neoichor
* Nerex
* Netwalker
* Nidiran
* NightClub
* ODAgent
* OSX/Shlayer
* OSX\_OCEANLOTUS.D
* Octopus
* OilBooster
* OilCheck
* Okrum
* OopsIE
* Orz
* OutSteel
* P.A.S. Webshell
* P8RAT
* PLAINTEE
* PLEAD
* POSHSPY
* POWERSOURCE
* POWERSTATS
* POWRUNER
* PS1
* PUNCHBUGGY
* Pandora
* Pasam
* Penquin
* Peppy
* PipeMon
* Pisloader
* PlugX
* PoetRAT
* PoisonIvy
* PolyglotDuke
* Pony
* PowerDuke
* PowerExchange
* PowerLess
* PowerPunch
* Psylo
* Pteranodon
* QakBot
* QuietSieve
* RARSTONE
* RATANKBA
* RCSession
* RDAT
* REvil
* RGDoor
* ROKRAT
* RTM
* Raccoon Stealer
* RainyDay
* Raspberry Robin
* RedLeaves
* RegDuke
* RemoteCMD
* Remsec
* Revenge RAT
* RogueRobin
* S-Type
* SDBbot
* SEASHARPEE
* SHARPSTATS
* SHUTTERSPEED
* SLIGHTPULSE
* SLOTHFULMEDIA
* SLOWDRIFT
* SMOKEDHAM
* SQLRat
* STEADYPULSE
* SUNBURST
* SVCReady
* Saint Bot
* Sakula
* SampleCheck5000
* Samurai
* Sardonic
* SeaDuke
* Seasalt
* ServHelper
* Seth-Locker
* ShadowPad
* Shamoon
* Shark
* SharpDisco
* SharpStage
* ShimRat
* Sibot
* SideTwist
* Skidmap
* Small Sieve
* Smoke Loader
* Snip3
* SocGholish
* SodaMaster
* Solar
* SombRAT
* SoreFang
* SpeakUp
* Spica
* SpicyOmelette
* Squirrelwaffle
* StoneDrill
* StrelaStealer
* StrifeWater
* StrongPity
* SysUpdate
* TAINTEDSCRIBE
* TAMECAT
* TDTESS
* TSCookie
* TURNEDUP
* TYPEFRAME
* Taidoor
* ThiefQuest
* ThreatNeedle
* TinyTurla
* Tomiris
* TrickBot
* Trojan.Karagany
* Turian
* UBoatRAT
* UPPERCUT
* Unknown Logger
* Uroburos
* Ursnif
* VBShower
* VERMIN
* Valak
* VaporRage
* Vasport
* Volgmer
* WEBC2
* WIREFIRE
* WarzoneRAT
* Waterbear
* WellMail
* WellMess
* WhisperGate
* Wiarp
* Winnti for Linux
* Winnti for Windows
* Woody RAT
* XCSSET
* Xbash
* YAHOYAH
* ZIPLINE
* ZLib
* Zebrocy
* ZeroT
* Zeus Panda
* Zox
* ZxShell
* ZxxZ
* build\_downer
* down\_new
* gh0st RAT
* jRAT
* macOS.OSAMiner
* metaMain
* njRAT
* reGeorg
* xCaon

## Tools

* AsyncRAT
* BITSAdmin
* Brute Ratel C4
* CARROTBALL
* CSPY Downloader
* Donut
* Empire
* Koadic
* MCMD
* Pupy
* QuasarRAT
* Remcos
* RemoteUtilities
* SILENTTRINITY
* ShimRatReporter
* Sliver
* certutil
* cmd
* esentutl
* ftp

## APTs (Intrusion Sets)

* APT-C-36
* APT18
* APT28
* APT29
* APT3
* APT32
* APT33
* APT37
* APT38
* APT39
* APT41
* Ajax Security Team
* Andariel
* Aquatic Panda
* BITTER
* BRONZE BUTLER
* BackdoorDiplomacy
* BlackByte
* Chimera
* Cinnamon Tempest
* Cobalt Group
* Confucius
* Daggerfly
* Darkhotel
* Dragonfly
* Elderwood
* Evilnum
* FIN13
* FIN7
* FIN8
* Fox Kitten
* GALLIUM
* Gamaredon Group
* Gorgon Group
* HAFNIUM
* HEXANE
* INC Ransom
* IndigoZebra
* Indrik Spider
* Ke3chang
* Kimsuky
* Lazarus Group
* LazyScripter
* Leviathan
* LuminousMoth
* Magic Hound
* Metador
* Molerats
* Moonstone Sleet
* Moses Staff
* MuddyWater
* Mustang Panda
* Mustard Tempest
* Nomadic Octopus
* OilRig
* PLATINUM
* Patchwork
* Play
* Rancor
* Rocke
* Sandworm Team
* SideCopy
* Sidewinder
* Silence
* Storm-1811
* TA2541
* TA505
* TA551
* TeamTNT
* Threat Group-3390
* Tonto Team
* Tropic Trooper
* Turla
* Volatile Cedar
* Volt Typhoon
* WIRTE
* Whitefly
* Windshift
* Winnti Group
* Winter Vivern
* Wizard Spider
* ZIRCONIUM
* menuPass