# TTP Detail – T1570

## TTP Information

Name: Lateral Tool Transfer

Description: Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e., [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation.

Adversaries may copy files between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) to connected network shares or with authenticated connections via [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001).(Citation: Unit42 LockerGoga 2019)

Files can also be transferred using native or otherwise present tools on the victim system, such as scp, rsync, curl, sftp, and [ftp](https://attack.mitre.org/software/S0095). In some cases, adversaries may be able to leverage [Web Service](https://attack.mitre.org/techniques/T1102)s such as Dropbox or OneDrive to copy files from one machine to another via shared, automatically synced folders.(Citation: Dropbox Malware Sync)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: lateral-movement

## Malware

* BlackByte Ransomware
* BlackCat
* DustySky
* Emotet
* HermeticWizard
* INC Ransomware
* IPsec Helper
* LockerGoga
* Lucifer
* Netwalker
* Olympic Destroyer
* OutSteel
* Shamoon
* Stuxnet
* WannaCry

## Tools

* BITSAdmin
* Expand
* Impacket
* PsExec
* cmd
* esentutl
* ftp

## APTs (Intrusion Sets)

* APT32
* APT41
* Agrius
* Aoqin Dragon
* BlackByte
* Chimera
* Ember Bear
* FIN10
* GALLIUM
* INC Ransom
* Magic Hound
* Sandworm Team
* Storm-1811
* Turla
* Velvet Ant
* Volt Typhoon
* Wizard Spider