# TTP Detail – T1104

## TTP Information

Name: Multi-Stage Channels

Description: Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult.

Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features.

The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* BACKSPACE
* BLACKCOFFEE
* Bazar
* Chaos
* JumbledPath
* Latrodectus
* LunarWeb
* Snip3
* Uroburos
* Valak

## APTs (Intrusion Sets)

* APT3
* APT41
* Lazarus Group
* MuddyWater