# TTP Detail – T1563

## TTP Information

Name: Remote Service Session Hijacking

Description: Adversaries may take control of preexisting sessions with remote services to move laterally in an environment. Users may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and RDP. When a user logs into a service, a session will be established that will allow them to maintain a continuous interaction with that service.

Adversaries may commandeer these sessions to carry out actions on remote systems. [Remote Service Session Hijacking](https://attack.mitre.org/techniques/T1563) differs from use of [Remote Services](https://attack.mitre.org/techniques/T1021) because it hijacks an existing session rather than creating a new session using [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: RDP Hijacking Medium)(Citation: Breach Post-mortem SSH Hijack)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: lateral-movement