# TTP Detail – T1563.002

## TTP Information

Name: RDP Hijacking

Description: Adversaries may hijack a legitimate user’s remote desktop session to move laterally within an environment. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services)

Adversaries may perform RDP session hijacking which involves stealing a legitimate user's remote session. Typically, a user is notified when someone else is trying to steal their session. With System permissions and using Terminal Services Console, `c:\windows\system32\tscon.exe [session number to be stolen]`, an adversary can hijack a session without the need for credentials or prompts to the user.(Citation: RDP Hijacking Korznikov) This can be done remotely or locally and with active or disconnected sessions.(Citation: RDP Hijacking Medium) It can also lead to [Remote System Discovery](https://attack.mitre.org/techniques/T1018) and Privilege Escalation by stealing a Domain Admin or higher privileged account session. All of this can be done by using native Windows commands, but it has also been added as a feature in red teaming tools.(Citation: Kali Redsnarf)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: lateral-movement

## Malware

* WannaCry

## APTs (Intrusion Sets)

* Axiom