# TTP Detail – T1098.007

## TTP Information

Name: Additional Local or Domain Groups

Description: An adversary may add additional local or domain groups to an adversary-controlled account to maintain persistent access to a system or domain.

On Windows, accounts may use the `net localgroup` and `net group` commands to add existing users to local and domain groups.(Citation: Microsoft Net Localgroup)(Citation: Microsoft Net Group) On Linux, adversaries may use the `usermod` command for the same purpose.(Citation: Linux Usermod)

For example, accounts may be added to the local administrators group on Windows devices to maintain elevated privileges. They may also be added to the Remote Desktop Users group, which allows them to leverage [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) to log into the endpoints in the future.(Citation: Microsoft RDP Logons) On Linux, accounts may be added to the sudoers group, allowing them to persistently leverage [Sudo and Sudo Caching](https://attack.mitre.org/techniques/T1548/003) for elevated privileges.

In Windows environments, machine accounts may also be added to domain groups. This allows the local SYSTEM account to gain privileges on the domain.(Citation: RootDSE AD Detection 2022)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

## Malware

* DarkGate
* SMOKEDHAM
* ServHelper

## Tools

* Net

## APTs (Intrusion Sets)

* APT3
* APT41
* APT5
* Dragonfly
* FIN13
* Kimsuky
* Magic Hound