# TTP Detail – T1134.003

## TTP Information

Name: Make and Impersonate Token

Description: Adversaries may make new tokens and impersonate users to escalate privileges and bypass access controls. For example, if an adversary has a username and password but the user is not logged onto the system the adversary can then create a logon session for the user using the `LogonUser` function.(Citation: LogonUserW function) The function will return a copy of the new session's access token and the adversary can use `SetThreadToken` to assign the token to a thread.

This behavior is distinct from [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) in that this refers to creating a new user token instead of stealing or duplicating an existing one.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

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

## Malware

* Cobalt Strike
* Mafalda

## Tools

* SILENTTRINITY

## APTs (Intrusion Sets)

* BlackByte
* FIN13