# TTP Detail – T1134.002

## TTP Information

Name: Create Process with Token

Description: Adversaries may create a new process with an existing token to escalate privileges and bypass access controls. Processes can be created with the token and resulting security context of another user using features such as <code>CreateProcessWithTokenW</code> and <code>runas</code>.(Citation: Microsoft RunAs)

Creating processes with a token not associated with the current user may require the credentials of the target user, specific privileges to impersonate that user, or access to the token to be used. For example, the token could be duplicated via [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) or created via [Make and Impersonate Token](https://attack.mitre.org/techniques/T1134/003) before being used to create a process.

While this technique is distinct from [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001), the techniques can be used in conjunction where a token is duplicated and then used to create a new process.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

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

## Malware

* Aria-body
* Azorult
* Bankshot
* KONNI
* PipeMon
* REvil
* WhisperGate
* ZxShell

## Tools

* Empire
* PoshC2

## APTs (Intrusion Sets)

* Lazarus Group
* Turla