# TTP Detail – T1134.001

## TTP Information

Name: Token Impersonation/Theft

Description: Adversaries may duplicate then impersonate another user's existing token to escalate privileges and bypass access controls. For example, an adversary can duplicate an existing token using `DuplicateToken` or `DuplicateTokenEx`.(Citation: DuplicateToken function) The token can then be used with `ImpersonateLoggedOnUser` to allow the calling thread to impersonate a logged on user's security context, or with `SetThreadToken` to assign the impersonated token to a thread.

An adversary may perform [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) when they have a specific, existing process they want to assign the duplicated token to. For example, this may be useful for when the target user has a non-network logon session on the system.

When an adversary would instead use a duplicated token to create a new process rather than attaching to an existing process, they can additionally [Create Process with Token](https://attack.mitre.org/techniques/T1134/002) using `CreateProcessWithTokenW` or `CreateProcessAsUserW`. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) is also distinct from [Make and Impersonate Token](https://attack.mitre.org/techniques/T1134/003) in that it refers to duplicating an existing token, rather than creating a new one.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

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

## Malware

* Aria-body
* BADHATCH
* BitPaymer
* Cobalt Strike
* Emotet
* FinFisher
* Okrum
* REvil
* Shamoon
* Siloscape
* Stuxnet
* Tarrask

## Tools

* Pupy
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT28
* FIN8