# TTP Detail – T1055.005

## TTP Information

Name: Thread Local Storage

Description: Adversaries may inject malicious code into processes via thread local storage (TLS) callbacks in order to evade process-based defenses as well as possibly elevate privileges. TLS callback injection is a method of executing arbitrary code in the address space of a separate live process.

TLS callback injection involves manipulating pointers inside a portable executable (PE) to redirect a process to malicious code before reaching the code's legitimate entry point. TLS callbacks are normally used by the OS to setup and/or cleanup data used by threads. Manipulating TLS callbacks may be performed by allocating and writing to specific offsets within a process’ memory space using other [Process Injection](https://attack.mitre.org/techniques/T1055) techniques such as [Process Hollowing](https://attack.mitre.org/techniques/T1055/012).(Citation: FireEye TLS Nov 2017)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via TLS callback injection may also evade detection from security products since the execution is masked under a legitimate process.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

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

## Malware

* Ursnif