# TTP Detail – T1055.003

## TTP Information

Name: Thread Execution Hijacking

Description: Adversaries may inject malicious code into hijacked processes in order to evade process-based defenses as well as possibly elevate privileges. Thread Execution Hijacking is a method of executing arbitrary code in the address space of a separate live process.

Thread Execution Hijacking is commonly performed by suspending an existing process then unmapping/hollowing its memory, which can then be replaced with malicious code or the path to a DLL. A handle to an existing victim process is first created with native Windows API calls such as <code>OpenThread</code>. At this point the process can be suspended then written to, realigned to the injected code, and resumed via <code>SuspendThread </code>, <code>VirtualAllocEx</code>, <code>WriteProcessMemory</code>, <code>SetThreadContext</code>, then <code>ResumeThread</code> respectively.(Citation: Elastic Process Injection July 2017)

This is very similar to [Process Hollowing](https://attack.mitre.org/techniques/T1055/012) but targets an existing process rather than creating a process in a suspended state.

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 Thread Execution Hijacking 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

* Gazer
* Pikabot
* Trojan.Karagany
* Waterbear