# TTP Detail – T1055.012

## TTP Information

Name: Process Hollowing

Description: Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Process hollowing is a method of executing arbitrary code in the address space of a separate live process.

Process hollowing is commonly performed by creating a process in a suspended state then unmapping/hollowing its memory, which can then be replaced with malicious code. A victim process can be created with native Windows API calls such as <code>CreateProcess</code>, which includes a flag to suspend the processes primary thread. At this point the process can be unmapped using APIs calls such as <code>ZwUnmapViewOfSection</code> or <code>NtUnmapViewOfSection</code> before being written to, realigned to the injected code, and resumed via <code>VirtualAllocEx</code>, <code>WriteProcessMemory</code>, <code>SetThreadContext</code>, then <code>ResumeThread</code> respectively.(Citation: Leitch Hollowing)(Citation: Elastic Process Injection July 2017)

This is very similar to [Thread Local Storage](https://attack.mitre.org/techniques/T1055/005) but creates a new process rather than targeting an existing process. This behavior will likely not result in elevated privileges since the injected process was spawned from (and thus inherits the security context) of the injecting process. However, execution via process hollowing may also evade detection from security products since the execution is masked under a legitimate process.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

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

## Malware

* Agent Tesla
* Astaroth
* Azorult
* BADNEWS
* BBSRAT
* Bandook
* Bazar
* Clambling
* Cobalt Strike
* DarkGate
* Denis
* Dtrack
* Duqu
* Emotet
* Gootloader
* ISMInjector
* IcedID
* Lokibot
* Lumma Stealer
* NETWIRE
* Orz
* QakBot
* RCSession
* Raspberry Robin
* Saint Bot
* Smoke Loader
* Snip3
* TrickBot
* Ursnif
* WhisperGate
* Woody RAT
* XLoader

## APTs (Intrusion Sets)

* BlackByte
* Gorgon Group
* Kimsuky
* Patchwork
* TA2541
* Threat Group-3390
* menuPass