# TTP Detail – T1093

## TTP Information

Name: Process Hollowing

Description: Process hollowing occurs when a process is created in a suspended state then its memory is unmapped and replaced with malicious code. Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), execution of the malicious code is masked under a legitimate process and may evade defenses and detection analysis. (Citation: Leitch Hollowing) (Citation: Elastic Process Injection July 2017)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion