# TTP Detail – T1134.004

## TTP Information

Name: Parent PID Spoofing

Description: Adversaries may spoof the parent process identifier (PPID) of a new process to evade process-monitoring defenses or to elevate privileges. New processes are typically spawned directly from their parent, or calling, process unless explicitly specified. One way of explicitly assigning the PPID of a new process is via the <code>CreateProcess</code> API call, which supports a parameter that defines the PPID to use.(Citation: DidierStevens SelectMyParent Nov 2009) This functionality is used by Windows features such as User Account Control (UAC) to correctly set the PPID after a requested elevated process is spawned by SYSTEM (typically via <code>svchost.exe</code> or <code>consent.exe</code>) rather than the current user context.(Citation: Microsoft UAC Nov 2018)  
  
Adversaries may abuse these mechanisms to evade defenses, such as those blocking processes spawning directly from Office documents, and analysis targeting unusual/potentially malicious parent-child process relationships, such as spoofing the PPID of [PowerShell](https://attack.mitre.org/techniques/T1059/001)/[Rundll32](https://attack.mitre.org/techniques/T1218/011) to be <code>explorer.exe</code> rather than an Office document delivered as part of [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001).(Citation: CounterCept PPID Spoofing Dec 2018) This spoofing could be executed via [Visual Basic](https://attack.mitre.org/techniques/T1059/005) within a malicious Office document or any code that can perform [Native API](https://attack.mitre.org/techniques/T1106).(Citation: CTD PPID Spoofing Macro Mar 2019)(Citation: CounterCept PPID Spoofing Dec 2018)  
  
Explicitly assigning the PPID may also enable elevated privileges given appropriate access rights to the parent process. For example, an adversary in a privileged user context (i.e. administrator) may spawn a new process and assign the parent as a process running as SYSTEM (such as <code>lsass.exe</code>), causing the new process to be elevated via the inherited access token.(Citation: XPNSec PPID Nov 2017)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

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

## Malware

* Cobalt Strike
* DarkGate
* KONNI
* PipeMon