# TTP Detail – T1055.008

## TTP Information

Name: Ptrace System Calls

Description: Adversaries may inject malicious code into processes via ptrace (process trace) system calls in order to evade process-based defenses as well as possibly elevate privileges. Ptrace system call injection is a method of executing arbitrary code in the address space of a separate live process.

Ptrace system call injection involves attaching to and modifying a running process. The ptrace system call enables a debugging process to observe and control another process (and each individual thread), including changing memory and register values.(Citation: PTRACE man) Ptrace system call injection is commonly performed by writing arbitrary code into a running process (ex: <code>malloc</code>) then invoking that memory with <code>PTRACE\_SETREGS</code> to set the register containing the next instruction to execute. Ptrace system call injection can also be done with <code>PTRACE\_POKETEXT</code>/<code>PTRACE\_POKEDATA</code>, which copy data to a specific address in the target processes’ memory (ex: the current address of the next instruction). (Citation: PTRACE man)(Citation: Medium Ptrace JUL 2018)

Ptrace system call injection may not be possible targeting processes that are non-child processes and/or have higher-privileges.(Citation: BH Linux Inject)

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 ptrace system call 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

* PACEMAKER