# TTP Detail – T1036.011

## TTP Information

Name: Overwrite Process Arguments

Description: Adversaries may modify a process's in-memory arguments to change its name in order to appear as a legitimate or benign process. On Linux, the operating system stores command-line arguments in the process’s stack and passes them to the `main()` function as the `argv` array. The first element, `argv[0]`, typically contains the process name or path - by default, the command used to actually start the process (e.g., `cat /etc/passwd`). By default, the Linux `/proc` filesystem uses this value to represent the process name. The `/proc/<PID>/cmdline` file reflects the contents of this memory, and tools like `ps` use it to display process information. Since arguments are stored in user-space memory at launch, this modification can be performed without elevated privileges.

During runtime, adversaries can erase the memory used by all command-line arguments for a process, overwriting each argument string with null bytes. This removes evidence of how the process was originally launched. They can then write a spoofed string into the memory region previously occupied by `argv[0]` to mimic a benign command, such as `cat resolv.conf`. The new command-line string is reflected in `/proc/<PID>/cmdline` and displayed by tools like `ps`.(Citation: Sandfly BPFDoor 2022)(Citation: Microsoft XorDdos Linux Stealth 2022)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BPFDoor