Masquerading: Break Process Trees, Sub-technique T1036.009 - Enterprise

Archived: 2026-04-02 12:35:08 UTC

An adversary may attempt to evade process tree-based analysis by modifying executed malware's parent process ID (PPID). If endpoint protection software leverages the "parent-child" relationship for detection, breaking this relationship could result in the adversary’s behavior not being associated with previous process tree activity. On Unix-based systems breaking this process tree is common practice for administrators to execute software using scripts and programs.[1]

On Linux systems, adversaries may execute a series of Native API calls to alter malware's process tree. For example, adversaries can execute their payload without any arguments, call the `fork()` API call twice, then have the parent process exit. This creates a grandchild process with no parent process that is immediately adopted by the `init` system process (PID 1), which successfully disconnects the execution of the adversary's payload from its previous process tree.

Another example is using the "daemon" syscall to detach from the current parent process and run in the background.[2][3]

Source: https://attack.mitre.org/techniques/T1036/009